

1 **LIEFF CABRASER HEIMANN &**
2 **BERNSTEIN, LLP**
3 Michael W. Sobol (SBN 194857)
4 msobol@lchb.com
5 275 Battery Street, 29th Floor
6 San Francisco, CA 94111-3339
7 Telephone: 415.956.1000
8 Facsimile: 415.956.1008

9 **LIEFF CABRASER HEIMANN &**
10 **BERNSTEIN, LLP**
11 Nicholas Diamand
12 ndiamand@lchb.com
13 Douglas I. Cuthbertson
14 dcuthbertson@lchb.com
15 Abbye R. Klamann (SBN 311112)
16 aklamann@lchb.com
17 250 Hudson Street, 8th Floor
18 New York, NY 10013-1413
19 Telephone: 212.355.9500
20 Facsimile: 212.355.9592

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

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

26 AMANDA RUSHING, and her child, L.L.,
27 on behalf of themselves and all others
28 similarly situated,

Plaintiffs,

v.

THE WALT DISNEY COMPANY;
DISNEY ENTERPRISES, INC.; DISNEY
ELECTRONIC CONTENT, INC.;
UPSIGHT, INC.; UNITY
TECHNOLOGIES SF; and KOCHAVA,
INC.,

Defendants.

CARNEY BATES & PULLIAM, PLLC
Hank Bates (SBN 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
519 West 7th St.
Little Rock, AR 72201
Telephone: 501.312.8500
Facsimile: 501.312.8505

Case No. 3:17-cv-4419

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 **I. INTRODUCTION**

2 1. This is an action brought by and on behalf parents of children¹ who, while playing
3 online games via smart phone apps, have had their personally identifying information exfiltrated
4 by The Walt Disney Company and its 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 a parent and her child who used an online gaming app via websites or
11 online services operated by Defendants.

12 3. Plaintiff Amanda Rushing, and her child, “L.L.,” reside in San Francisco,
13 California. Ms. Rushing brings this action on behalf of herself, L.L., and all others similarly
14 situated. L.L. was under the age of 13 while using the gaming app Disney Princess Palace Pets.

15 **Defendants The Walt Disney Company, Disney Enterprises, Inc., and Disney**
16 **Electronic Content, Inc. (together, “Disney”)**

17 4. Defendant The Walt Disney Company is a diversified worldwide entertainment
18 company that (i) runs major media networks; (ii) operates parks and resorts; (iii) produces live
19 and animated films; and (iv) licenses, develops, and publishes consumer products and interactive
20 media, including games for children on mobile platforms through Disney’s “Consumer Products
21 & Interactive Media” segment. This segment generates revenue primarily from – among other
22 things – the sale of online games, in-game purchases, and advertising through online video
23 content. Disney developed and marketed the online gaming app used by Plaintiffs, and apps used
24 by millions of people in the United States. It is headquartered at 500 South Buena Vista Street,
25 Burbank, CA 91521.

26

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

1 5. Defendant Disney Enterprises, Inc. is a wholly-owned subsidiary of The Walt
2 Disney Company that functions as the merchandising and licensing division of The Walt Disney
3 Company, and is the registered owner of Disney-branded trademarks, copyrights and other
4 intellectual property assets. It is headquartered at 500 South Buena Vista Street, Burbank, CA
5 91521.

6 6. Defendant Disney Electronic Content, Inc. is identified as the “Seller” in the Apple
7 App Store and the “Developer” in the Google Play Store, for many of Disney’s Apps. It is
8 headquartered at 500 South Buena Vista Street, Burbank, CA 91521.

9 **The SDK Defendants**

10 7. The “SDK Defendants” – identified in paragraphs 8 through 10 below – are
11 entities which provided their own proprietary computer code to Disney, known as software
12 development kits (“SDK”), for installation and use in Disney’s gaming apps, including Disney
13 Princess Palace Pets. Each of the SDK Defendants named herein embedded their respective
14 SDKs in Disney’s gaming apps, causing the transmittal of app users’ personally identifying
15 information to the SDK Defendants to facilitate subsequent behavioral advertising.

16 8. SDK Defendant Upsight, Inc. (“Upsight”) is an American technology company
17 headquartered at 501 Folsom St., San Francisco, CA 94105.

18 9. SDK Defendant Unity Technologies SF (“Unity”) is an American technology
19 headquartered at 30 3rd Street, San Francisco, CA 94103

20 10. SDK Defendant Kochava, Inc. (“Kochava”) is an American technology company
21 headquartered at 201 Church Street, Sandpoint, ID 83864.

22 **III. JURISDICTION AND VENUE**

23 11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.
24 §§ 1332 and 1367 because this is a class action in which the matter or controversy exceeds the
25 sum of \$5,000,000, exclusive of interest and costs, and in which some members of the proposed
26 Classes are citizens of a state different from some defendants.

27 12. This Court has personal jurisdiction over Defendants because they transact
28 business in the United States, including in this District, have substantial aggregate contacts with

1 the United States, including in this District, engaged and are engaging in conduct that has and had
2 a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons
3 throughout the United States, and purposely availed themselves of the laws of the United States.

4 13. In accordance with 28 U.S.C. § 1391, venue is proper in this district because a
5 substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District,
6 Defendants transact business in this District, and because multiple Defendants reside in this
7 District.

8 **IV. INTRADISTRICT ASSIGNMENT**

9 14. Pursuant to Civil L.R. 3-2(c), assignment to this Division is proper because a
10 substantial part of the conduct which give rise to Plaintiffs' claims occurred in this District.
11 Defendants market their products throughout the United States, including in San Francisco and
12 Alameda counties. In addition, two of the three SDK Defendants are headquartered in San
13 Francisco.

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

15 **A. The Programming of Mobile Online Gaming Apps Enables the Collection of**
16 **Personal Data.**

17 15. The number of Americans using and relying on mobile devices connected to the
18 internet ("smart" phones, tablets, and other devices) had increased to 77% of Americans by
19 November 2016. Consumers increasingly use smart devices to play their favorite online games,
20 or "apps." Many apps are aimed at children, who increasingly use smart devices to play their
21 favorite games.

22 16. Most consumers, including parents of children consumers, do not know that apps
23 created for children are engineered to surreptitiously and unlawfully collect the child-users'
24 personal information, and then exfiltrate that information off the smart device for advertising and
25 other commercial purposes.

26 17. App developers contract with third-parties for the right to embed third-party
27 computer code into the developers' apps, for various purposes. For example, a developer may
28 incorporate Google's "In-App Billing SDK," so that app users may make purchases and payments

1 directly to the developer. In this way, app developers are like vehicle manufacturers, which also
2 incorporate third-party components, such as airbags or brake pads, into their vehicles, rather than
3 developing their own component parts from scratch.

4 18. Advertising-specific SDKs are blocks of computer code which operate to secretly
5 collect an app user's personal information and track online behavior to facilitate behavioral
6 advertising or marketing analysis. In the case of an advertising SDK, the creator of the SDK will
7 embed its SDK code into the underlying code of the app itself, collect personal information to
8 serve behavioral advertisements, and then pay the app developer based on the number of ads
9 shown. This practice is a substantial source of many app developers' revenue, enabling app
10 developers to allow users to download the apps without charging a purchase price.²

11 19. App developers and their SDK-providing partners can track children's behavior
12 while they play online games with their mobile devices by obtaining critical pieces of data from
13 the mobile devices, including "persistent identifiers," typically a unique number linked to a
14 specific mobile device (*e.g.*, an individual's smart phone may be identified as "45 125792 45513
15 7"). SDK providers, such as the SDK Defendants, use their advertising SDKs, embedded into an
16 app in conjunction with an app developer, such as Disney, to capture and collect persistent
17 identifiers associated with a particular child user from her mobile device. These persistent
18 identifiers allow SDK providers to detect a child's activity across multiple apps and platforms on
19 the internet, and across different devices, effectively providing a full chronology of the child's
20 actions across devices and apps. This information is then sold to various third-parties who sell
21 targeted online advertising.

22 20. Key digital privacy and consumer groups described why and how a persistent
23 identifier alone facilitates behavioral advertising:

24 With the increasing use of new tracking and targeting techniques,

25 _____
26 ² "Only 33% of US Mobile Users Will Pay for Apps This Year," eMarketer (Feb. 5, 2015),
27 available at <https://www.emarketer.com/Article/Only-33-of-US-Mobile-Users-Will-Pay-Apps-This-Year/1011965> (last visited August 3, 2017) ("Put a dollar sign in front of an app, and the
28 number of people who are willing to download and install it drops dramatically. According to a 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
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

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

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

21. In other words, the ability to serve behavioral advertisements to a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (email addresses, etc.), but instead on the surreptitious collection of persistent identifiers, which are used in conjunction with other data points to build robust online profiles. Permitting technology companies to obtain persistent identifiers associated with children exposes them to the behavioral advertising (as well as other privacy violations) that COPPA was designed to prevent.

22. When children are tracked over time and across the internet, various activities are linked to a unique and persistent identifier to construct a profile of the user of a given smart device. Viewed in isolation, a persistent identifier is merely a string of numbers uniquely identifying a user, but when linked to other data points about the same user, such as app usage, geographic location (including likely domicile), and internet navigation, it discloses a personal profile that can be exploited in a commercial context. The chain of events typically works as follows: an app developer installs an SDK in an app, which collects persistent identifiers, permitting the SDK entity to sell the child’s persistent identifier to an advertising network or third-party data aggregator (who then further resells the data to additional partners). An “Ad Network” will store the persistent identifiers on its servers. Later, other app or SDK developers sell that same child’s persistent identifier to the Ad Network, bolstering the Ad Network’s profile of the child, increasing the value of the child’s data and, relatedly, the ability to serve a more highly-targeted ad to a specific device. Multiple Ad Networks or other third-parties can then buy and sell data, exchanging databases amongst themselves, creating an increasingly sophisticated

1 and merchantable profile of how, when, and why a child uses her mobile device, along with all of
2 the demographic and psychographic inferences that can be drawn therefrom.

3 23. The Ad Networks, informed by the surreptitious collection of data from children,
4 will assist in the sale of advertising placed within the gaming apps and targeted specifically to
5 children.

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

11 **B. COPPA Outlaws the Collection of Children's Personal Information Without**
12 **Verifiable Parental Consent.**

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

20 26. Recognizing the vulnerability of children in the internet age, in 1999 Congress
21 enacted COPPA. *See* 15 U.S.C. §§ 6501–6506. COPPA's express goal is to protect children's
22 privacy while they are connected to the internet.³ Under COPPA, developers of child-focused
23 apps, and any third-parties working with these app developers, cannot lawfully obtain the
24 personal information of children under 13 years of age without first obtaining verifiable consent
25 from their parents.

26
27 ³ *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 August 3, 2017).

1 27. COPPA applies to any operator of a commercial website or online service
2 (including an app) that is directed to children and that: (a) collects, uses, and/or discloses personal
3 information from children, or (b) on whose behalf such information is collected or maintained.
4 Under COPPA, personal information is “collected or maintained on behalf of an operator when .
5 . . [t]he operator benefits by allowing another person to collect personal information directly
6 from users of” an online service. 16 C.F.R. § 312.2. In addition, COPPA applies to any
7 operator of a commercial website or online service that has actual knowledge that it collects, uses,
8 and/or discloses personal information from children.

9 28. Under COPPA, “personal information” includes more commonly understood
10 information like names, email addresses, and social security numbers, but it also includes
11 “persistent identifier[s] that can be used to recognize a user over time and across different Web
12 sites or online services.” 16 C.F.R. § 312.2. COPPA’s broad definition of “personal
13 information” is as follows:

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

29 29. The FTC regards “persistent identifiers” as “personally identifiable” information
30 that can be reasonably linked to a particular child. The FTC amended COPPA’s definition of
31 “personal information” to clarify the inclusion of persistent identifiers. *See*
32 <https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising->
33 [industry](https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry) (2016 FTC Blog post from Director of the FTC Bureau of Consumer Protection) (last
34 visited August 3, 2017).

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

3 i. Posting a privacy policy on its website or online service providing
4 clear, understandable, and complete notice of its information practices, including what
5 information the website operator collects from children online, how it uses such information, its
6 disclosure practices for such information, and other specific disclosures as set forth in the Rule;

7 ii. Providing clear, understandable, and complete notice of its
8 information practices, including specific disclosures, directly to parents; and

9 iii. Obtaining verifiable parental consent prior to collecting, using,
10 and/or disclosing personal information from children.

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

16 32. The FTC recently clarified acceptable methods for obtaining verifiable parental
17 consent, which include: (i) providing a consent form for parents to sign and return; (ii) requiring
18 the use of a credit card/online payment that provides notification of each transaction; (iii)
19 connecting to trained personnel via video conference; (iv) calling a staffed toll-free number; (v)
20 emailing the parent soliciting a response email plus requesting follow-up information from the
21 parent; (vi) asking knowledge-based questions; or (vii) verifying a photo ID from the parent
22 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)
23 [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)
24 (last visited August 3, 2017).

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

27 33. Disney developed the mobile online gaming app Disney Princess Palace Pets
28 which they have marketed since 2013.

1 34. In 2011, Disney subsidiary Playdom Inc. (“Playdom”) paid a \$3 million civil
2 penalty for violating COPPA when it allegedly collected and disclosed personal information from
3 hundreds of thousands of children without obtaining their parents’ prior verifiable consent. This
4 settlement is the largest civil penalty for a violation of COPPA.⁴ As part of a consent decree
5 governing the settlement, Playdom, and “all persons in active concert or participation with them,”
6 were enjoined from, among other things, not obtaining verifiable parental consent before
7 collecting, using, or disclosing personal information from children from any website or online
8 service directed to children.⁵

9 35. In 2014, privacy watchdog the Center for Digital Democracy (“CDC”) approached
10 the FTC regarding Disney’s MarvelKids.com website, which contained a privacy policy in which
11 Disney (i) acknowledged that it collected personal information from children, including persistent
12 identifiers, for reasons not permissible under COPPA and (ii) indicated that Disney permitted
13 third party advertising SDKs, including SDK Defendants Kochava and Unity, to collect and use
14 children’s persistent identifiers.⁶ The CDC concluded that Disney’s MarvelKids.com website
15 was violating COPPA and the same was likely true “on Disney’s other child-directed websites.”
16 *See id.* at 9.

17 36. Indeed, in addition to Disney Princess Palace Pets, Disney has developed and
18 marketed other gaming apps which, like Disney Princess Palace Pets, track their users, including:
19 AvengersNet, Beauty and the Beast: Perfect Match, Cars Lightening League, Club Penguin
20 Island, Color by Disney, Disney Color and Play, Disney Crossy Road, Disney Dream Treats,
21 Disney Emoji Blitz, Disney Gif, Disney Jigsaw Puzzle!, Disney LOL, Disney Princess: Story
22 Theater, Disney Store Become, Disney Story Central, Disney’s Magic Timer by Oral-B, Disney
23

24 ⁴ [https://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-](https://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-million-settle-ftc-charges)
25 [million-settle-ftc-charges](https://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-million-settle-ftc-charges) (last visited August 3, 2017).

26 ⁵ *See* <https://www.ftc.gov/sites/default/files/documents/cases/2011/05/110512playdomstip.pdf>.

27 ⁶ Letter from Eric G. Null, *et al.*, to Donald S. Clark, Federal Trade Commission, *Updating the*
28 *Request for Investigation of Disney and Marvel’s Violation of the Children’s Online Privacy*
Protection Act Rule in Connection with Marvelkids.com, (Mar. 20, 2014) (available at
<https://dlbjbjzgnk95t.cloudfront.net/0520000/520581/FTC%20Letter%20FINAL%20SUBMITTE>
[D.pdf](https://dlbjbjzgnk95t.cloudfront.net/0520000/520581/FTC%20Letter%20FINAL%20SUBMITTE) (last visited August 3, 2017).

1 Princess: Charmed Adventures, Dodo Pop, Disney Build It Frozen, DuckTales: Remastered,
2 Frozen Free Fall, Frozen Free Fall: Icy Shot, Good Dinosaur Storybook Deluxe, Inside Out
3 Thought Bubbles, Maleficent Free Fall, Miles from Tomorrowland: Missions, Moana Island Life,
4 Olaf's Adventures, Palace Pets in Whisker Haven, Sofia the First Color and Play, Sofia the First
5 Secret Library, Star Wars: Puzzle Droids™, Star Wars™: Commander, Temple Run: Oz, Temple
6 Run: Brave, The Lion Guard, Toy Story: Story Theater, Where's My Water?, Where's My
7 Mickey?, Where's My Water? 2, Where's My Water? Lite/ Where's My Water? Free, Zootopia
8 Crime Files: Hidden Object (with Disney Princess Palace Pets, these apps are collectively
9 referred to as the "Game Tracking Apps"). Disney offers the Games Tracking Apps for
10 download from Apple's App Store, Google Play Store, and/or Amazon.

11 37. Disney collects and maintains personal information about the users of the Game
12 Tracking Apps, including users under the age of 13, and permits the SDK Defendants to embed
13 their advertising SDKS to collect those users' personal information and use that information to
14 track those users over time and across different websites and online services.

15 38. Disney has control over and responsibility for any advertising and data mining
16 permitted by or undertaken in the Game Tracking Apps. Disney has failed to safeguard
17 children's personal information and ensure that third-parties' collection of data from children is
18 lawful, in part, by allowing the SDK Defendants to embed advertising SDKs in the Game
19 Tracking Apps directed at children.

20 39. Each SDK Defendant has an SDK placed in Disney Princess Palace Pets which
21 collects persistent identifiers to track children app users over time and across the internet. In
22 addition to Disney Princess Palace Pets, the other Game Tracking Apps contain SDKs that
23 surreptitiously track child users for behavioral advertising, analytics, or both. Disney Princess
24 Palace Pets and the other Game Tracking Apps contain multiple SDKs, each operating
25 independently from and in concert with one another.

26 40. Each SDK Defendant facilitates behavioral advertising in the mobile app space by
27 collecting personal information about app users that enables advertisers and other third-parties to
28 reach those users over time and across different websites and online services. Each SDK

1 Defendant does so through its proprietary SDK embedded in Disney’s Apps – including Disney
2 Princess Palace Pets – which collect personal information about children under the age of 13 so
3 that advertisers and other third-parties can target those children over time and across different
4 websites and online services.

5 41. Analytics and network analysis tools have detected the persistent identifiers that
6 each Game Tracking App accessed in real time, determined which SDKs reside in the Game
7 Tracking Apps’ code, and recorded all network traffic, including encrypted data. That
8 documentation contains raw network data, which shows the presence of persistent identifiers and
9 documents (i) when the Game Tracking Apps first attempted to access persistent identifiers, (ii)
10 which persistent identifiers were sent from a users’ device, and (iii) the SDK Defendant to which
11 they were sent.

12 42. Extensive analysis conducted as to each of Disney’s Game Tracking Apps and as
13 to each SDK Defendant, found substantial evidence that each of these child-directed apps collects
14 and uses children’s persistent identifiers.

15 **2. Disney’s Game Tracking Apps Are Directed to Children.**

16 43. COPPA defines “children” as individuals under the age of 13. *See* 16 C.F.R.
17 § 312.2. An app is directed to children if the “subject matter, visual content, use of animated
18 characters or child-oriented activities and incentives, music or other audio content, age of models,
19 presence of child celebrities or celebrities who appeal to children, language or other
20 characteristics of the Web site or online service, as well as whether advertising promoting or
21 appearing on the Web site or online service is directed to children.” *See* 16 C.F.R. § 312.2.

22 44. Disney Princess Palace Pets and the other Game Tracking Apps are directed to
23 children under age 13.⁷ For example, Disney Princess Palace Pets is a game in which users can
24 groom, bathe, accessorize, and play with about with 10 different pets. The app description in the
25 Google Play Store states: “Enter the enchanted world of the Disney Princess Palace Pets. Meet
26 Pumpkin, Teacup, Blondie, Treasure, Berry, Beauty, Lily, Summer, Sultan, and petit! These

27 ⁷ A description of the additional Game Tracking Apps, including screenshots of the games from
28 the Google Play Store, is appended hereto as Exhibit A.

1 adorable pets are all different, but each one loves to be cared for and can't wait to go on new
2 adventures with you. Learn how the pets met the princesses, find out their unique talents, and
3 treat them to a delightful day at the Royal Pet Salon!" Below is a screenshot from the game:



20 45. In the Apple Store, Google Play Store, and Amazon, Disney Princess Palace Pets
21 is rated as a game for children younger than 5, or for "everyone or "all ages."

22 46. Even if the Game Tracking Apps were not directed to children, on information and
23 belief, Defendants have actual knowledge that they collected personal information from children.
24 The Game Tracking Apps contain child-oriented "subject matter, visual content, use of animated
25 characters or child-oriented activities and incentives, music or other audio content, age of models,
26 presence of child celebrities or celebrities who appeal to children, language or other
27 characteristics of the Web site or online service, as well as whether advertising promoting or
28 appearing on the Web site or online service is directed to children." 16 C.F.R. § 312.2.

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

3. The Defendants Are Operators under COPPA.

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

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

16 C.F.R. § 312.2.

48. Both Disney 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 Disney Princess Palace Pets.

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

49. Defendants collected, used, or disclosed the personal information of Plaintiff’s child without notifying her parents. Disney never obtained Plaintiff’s verifiable parental consent to collect, use, or disclose her child’s personal information. The SDK Defendants failed to adequately ensure that when they embedded their advertising SDKs on the Game Tracking Apps or when they collected, used, or disclosed personal information from children via their advertising SDKs on the Game Tracking Apps, that Disney had obtained verifiable parental consent for those children’s use of the Game Tracking Apps.

50. Plaintiff never knew that Defendants collected, disclosed, or used her child’s personal information because Defendants at all times failed to provide Plaintiff any of the required disclosures, never sought verifiable parental consent, and never provided a mechanism by which Plaintiff could provide verifiable consent.

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

5. Each SDK Defendant, in Coordination with Disney, Collects, Uses, or Discloses Children’s Personal Information Within Disney Princess Palace Pets without Verifiable Parental Consent.

51. Disney’s Disney Princess Palace Pets app contains each of the SDK Defendant’s behavioral advertising SDKs.

52. Each SDK Defendant knows or should know that it operates within Disney Princess Palace Pets.

53. Each SDK Defendant knows or should know the age rating or suggested guidance for Disney Princess Palace Pets listed in the Google Play Store, the Apple App Store, or Amazon, within which the SDK Defendant operates.

54. Accordingly, each SDK Defendant knows or should know that its behavioral advertising SDK is contained within Disney Princess Palace Pets, among other child-directed apps.

55. Disney did not inform Plaintiff, her child, or class members that the SDK Defendants’ behavioral advertising SDKs are incorporated into and operate within the Game Tracking Apps, including Disney Princess Palace Pets, to collect Plaintiff’s child’s and class members’ personal information in the form of persistent identifiers.

56. Each SDK Defendant failed to inform the Plaintiff, her child, or class members that its behavioral advertising SDK is incorporated into and operates within Disney Princess Palace Pets to collect Plaintiff’s child’s and class members’ personal information in the form of persistent identifiers.

57. Disney did not obtain verifiable parental consent to track children playing the Game Tracking Apps, including Disney Princess Palace Pets, via persistent identifiers, over time and across different websites and online services.

58. Each SDK Defendant failed to obtain verifiable parental consent to track children playing Disney Princess Palace Pets, via persistent identifiers, over time and across different websites and online services.

1 59. Each SDK Defendant systemically tracks each user of Disney Princess Palace
2 Pets, including users under the age of 13, over time and across different websites and online
3 services, through its behavioral advertising SDK.

4 60. Each SDK Defendant does this by operating within Disney Princess Palace Pets to
5 collect, use, and share persistent identifiers from children who play Disney Princess Palace Pets.

6 61. Accordingly, each SDK Defendant, in coordination with Disney, collects, uses,
7 and/or discloses the personal information of Plaintiff's child and class members under the age of
8 13, in the form of persistent identifiers, to track children's activity over time and across different
9 websites and online services.

10 62. By affirmatively incorporating the SDK Defendants' behavioral advertising SDKs
11 into their child-directed apps and permitting them to track children by collecting, using, or
12 disclosing their persistent identifiers without verifiable parental consent, Disney violated COPPA.

13 63. Further, each SDK Defendant knew or should have known that its SDK had been
14 incorporated into Disney Princess Palace Pets and that engaging in the above-described tracking
15 and collection of children's personal information violated COPPA.

16 **6. Disney Engages in Substantially Similar Conduct in Its Other Game**
17 **Tracking Apps by Incorporating the SDK Defendants' Behavioral**
18 **Advertising SDKs into Those Game Tracking Apps.**

19 64. Disney's other Game Tracking Apps also contain the behavioral advertising SDKs,
20 which operate in a substantially similar manner as in Disney Princess Palace Pets.

21 65. Defendant Upsight's Upsight or Fuse Powered SDKs are incorporated into the
22 following additional Game Tracking Apps developed by Disney: Palace Pets in Whisker Haven,
23 Color by Disney, Disney Jigsaw Puzzle!, Disney Princess: Charmed Adventures, and Disney
24 Story Central.

25 66. Defendant Unity's Unity SDK is incorporated into the following additional Game
26 Tracking Apps developed by Disney: Disney Crossy Road, Disney Emoji Blitz, Disney Dream
27 Treats, Inside Out Thought Bubbles, Frozen Free Fall, Where's My Water? 2, Maleficent Free
28 Fall, Temple Run: Brave, Zootopia Crime Files: Hidden Object, Beauty and the Beast: Perfect
Match, Dodo Pop, Club Penguin Island, Frozen Free Fall: Icy Shot, Temple Run: Oz,

1 AvengersNet, Disney Princess: Story Theater, Disney Color and Play, Disney's Magic Timer by
2 Oral-B, Sofia the First Secret Library, Olaf's Adventures, The Lion Guard, Miles from
3 Tomorrowland: Missions, Disney Princess: Charmed Adventures, Toy Story: Story Theater,
4 Good Dinosaur Storybook Deluxe, Sofia the First Color and Play, Cars Lightening League, and
5 Moana Island Life.

6 67. Defendant Kochava's Kochava SDK is incorporated into the following additional
7 Game Tracking App developed by Disney: Disney Crossy Road, Disney Emoji Blitz, Disney
8 Dream Treats, Inside Out Thought Bubbles, Frozen Free Fall, Where's My Mickey?, Where's My
9 Water?, Where's My Water? 2, Where's My Water? Lite/ Where's My Water? Free, Color by
10 Disney, Disney Gif, Disney LOL, Maleficent Free Fall, Temple Run: Brave, Zootopia Crime
11 Files: Hidden Object, DuckTales: Remastered, Beauty and the Beast: Perfect Match, Dodo Pop,
12 Club Penguin Island, Frozen Free Fall: Icy Shot, Star Wars: Puzzle Droids™, Temple Run: Oz,
13 Star Wars™: Commander, Disney Store Become, Disney Princess: Story Theater, Disney Color
14 and Play, Disney Jigsaw Puzzle!, Sofia the First Secret Library, Olaf's Adventures, The Lion
15 Guard, Miles from Tomorrowland: Missions, Disney Princess: Charmed Adventures, Good
16 Dinosaur Storybook Deluxe, Moana Island Life, Disney Story Central, Cars Lightening League,
17 and Disney Build It Frozen.

18 **D. Fraudulent Concealment and Tolling.**

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

23 69. At the time the action was filed, Defendants were under a duty to disclose the true
24 character, quality, and nature of their activities to Plaintiffs and the Class and Subclass.
25 Defendants are therefore estopped from relying on any statute of limitations.

26 70. Defendants' fraudulent concealment is common to the Class and Subclass.
27
28

1 **E. Named Plaintiff Allegations**

2 **Plaintiff Amanda Rushing and Her Child, L.L.**

3 71. On January 14, 2014, Ms. Rushing downloaded Disney’s App Disney Princess
4 Palace Pets onto L.L.’s device in order for her child, L.L., to play the game. L.L. thereafter
5 frequently played Disney Princess Palace Pets on this device on an ongoing and continuous basis.

6 72. On information and belief, during the time L.L. played Disney Princess Palace
7 Pets, one or more of the SDK Defendants had, with the permission of Disney, embedded one or
8 more advertising SDKs which collected, disclosed, or used personal information and persistent
9 identifiers of L.L. Defendants did not collect L.L.’s personal information to provide support for
10 the internal operations of Disney Princess Palace Pets, but instead to profile L.L. for commercial
11 gain.

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

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

20 75. Defendants’ tracking and collection of L.L.’s personal information without her
21 verifiable parental consent is highly offensive to Ms. Rushing and constitutes an invasion of her
22 child’s privacy and of Ms. Rushing’s right to protect her child from this invasion.

23 **VI. CLASS ALLEGATIONS**

24 76. Plaintiffs seek class certification of the Class and Subclass set forth herein
25 pursuant to Federal Rule of Civil Procedure 23.

26 77. Plaintiffs seek class certification of claims for the common law privacy cause of
27 action “Intrusion Upon Seclusion,” on behalf of a multi-state class, with a class defined as
28 follows:

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

The Multi-state Class: all persons residing in the States of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia who are younger than the age of 13, or were younger than the 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.

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

The California Subclass of the Multi-state Class: all persons residing in the State of California who are younger than the age of 13, or were younger than the 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.

79. 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.

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

81. **Ascertainability.** The proposed Class and Subclass are readily ascertainable because they are defined using objective criteria so as to allow class members to determine if they

1 are part of a Class or Subclass. Further, the Class and Subclass can be readily identified through
2 records maintained by Defendants.

3 82. **Numerosity (Rule 23(a)(1)).** The Class and Subclass are so numerous that joinder
4 of individual members herein is impracticable. The exact number of Class or Subclass members,
5 as herein identified and described, is not known, but download figures indicate that the Game
6 Tracking Apps have been downloaded hundreds of millions of times.

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

10 i. Whether Disney engaged in the activities referenced in paragraphs
11 33 to 75 via the Game Tracking Apps;

12 ii. Whether the SDK Defendants engaged in the activities referenced
13 in paragraphs 33 to 75 via the Game Tracking Apps;

14 iii. Whether Defendants provided disclosure of all the activities
15 referenced in paragraphs 33 to 75 on a website as required by COPPA;

16 iv. Whether Defendants directly notified parents of any of the activities
17 referenced in paragraphs 33 to 42, 49-67, 71-75;

18 v. Whether Defendants sought verifiable parental consent prior to
19 engaging in any of the activities referenced in paragraphs 33 to 42, 49-67, 71-75;

20 vi. Whether Defendants provided a process or mechanism for parents
21 to provide verifiable parental consent prior to engaging in any of the activities referenced in
22 paragraphs 33 to 42, 49-67, 71-75;

23 vii. Whether Defendants received verifiable parental consent prior to
24 engaging in any of the activities referenced in paragraphs 33 to 42, 49-67, 71-75;

25 viii. Whether Defendants' acts and practices complained of herein
26 violate COPPA;

27 ix. Whether Defendants' acts and practices complained of herein
28 amount to acts of intrusion upon seclusion under the law of Alabama, Alaska, Arizona, Arkansas,

1 California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas,
2 Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New
3 Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota,
4 Texas, Utah, Vermont, Washington, and West Virginia;

5 x. Whether Defendants' conduct violated Subclass members'
6 California constitutional Right to Privacy;

7 xi. Whether members of the Class and Subclass have sustained
8 damages, and, if so, in what amount; and

9 xii. What is the appropriate injunctive relief to ensure Defendants no
10 longer illegally collect children's personal information to track them over time and across
11 different websites or online services.

12 84. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of members
13 of the proposed Class and Subclass because, among other things, Plaintiffs and members of the
14 Class and Subclass sustained similar injuries as a result of Defendants' uniform wrongful conduct
15 and their legal claims all arise from the same events and wrongful conduct by Defendants.

16 85. **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately protect the
17 interests of the proposed Class and Subclass. Plaintiffs' interests do not conflict with the interests
18 of the Class and Subclass members and Plaintiffs have retained counsel experienced in complex
19 class action and data privacy litigation to prosecute this case on behalf of the Class and Subclass.

20 86. **Predominance & Superiority (Rule 23(b)(3)).** In addition to satisfying the
21 prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under
22 Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only
23 individual Class and Subclass members, and a class action is superior to individual litigation and
24 all other available methods for the fair and efficient adjudication of this controversy. The amount
25 of damages available to individual Plaintiffs is insufficient to make litigation addressing
26 Defendants' conduct economically feasible in the absence of the class action procedure.
27 Individualized litigation also presents a potential for inconsistent or contradictory judgments, and
28 increases the delay and expense presented by the complex legal and factual issues of the case to

1 all parties and the court system. By contrast, the class action device presents far fewer
2 management difficulties and provides the benefits of a single adjudication, economy of scale, and
3 comprehensive supervision by a single court.

4 87. **Final Declaratory or Injunctive Relief (Rule 23(b)(2)).** Plaintiffs also satisfy
5 the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or
6 refused to act on grounds that apply generally to the proposed Class and Subclass, making final
7 declaratory or injunctive relief appropriate with respect to the proposed Class and Subclass as a
8 whole.

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

13 **VII. CLAIMS FOR RELIEF**

14 **COUNT I**
15 **Intrusion Upon Seclusion**
16 **(Brought on Behalf of the Multi-state Class)**

17 89. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

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

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

27 92. Defendants intentionally intruded on and into Plaintiffs' and Class members'
28 solitude, seclusion, or private affairs by intentionally designing the Game Tracking Apps (as well
as all SDKs identified in this Complaint) to surreptitiously obtain, improperly gain knowledge of,

1 review, and/or retain Plaintiffs' and Class members' activities through the monitoring
2 technologies and activities described herein.

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

13 94. Plaintiffs and Class members were harmed by the intrusion into their private
14 affairs as detailed throughout this Complaint.

15 95. Defendants' actions and conduct complained of herein were a substantial factor in
16 causing the harm suffered by Plaintiffs and Class members.

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

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

25 **COUNT II**
26 **California Constitutional Right to Privacy**
(Brought on Behalf of the California Subclass of the Multi-state Class)

27 98. Plaintiffs repeat and reallege all preceding paragraphs contained herein.
28

1 99. Plaintiffs and Subclass members have reasonable expectations of privacy in their
2 mobile devices and their online behavior, generally. Plaintiffs’ and Subclass members’ private
3 affairs include their behavior on their mobile devices as well as any other behavior that may be
4 monitored by the surreptitious tracking employed or otherwise enabled by the Game Tracking
5 Apps.

6 100. The reasonableness of such expectations of privacy is supported by Disney’s
7 unique position to monitor Plaintiffs’ and Subclass members’ behavior through their access to
8 Plaintiffs’ and Subclass members’ private mobile devices. It is further supported by the
9 surreptitious, highly-technical, and non-intuitive nature of Defendants’ tracking.

10 101. Defendants intentionally intruded on and into Plaintiffs’ and Subclass members’
11 solitude, seclusion, right of privacy, or private affairs by intentionally designing the Game
12 Tracking Apps (as well as all SDKs identified in this Complaint) to surreptitiously obtain,
13 improperly gain knowledge of, review, and/or retain Plaintiffs’ and Subclass members’ activities
14 through the monitoring technologies and activities described herein.

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

26 103. Plaintiffs and Subclass members were harmed by the intrusion into their private
27 affairs as detailed throughout this Complaint.
28

1 104. Defendants' actions and conduct complained of herein were a substantial factor in
2 causing the harm suffered by Plaintiffs and Subclass members.

3 105. As a result of Defendants' actions, Plaintiffs and Subclass members seek
4 injunctive relief, in the form of Defendants' cessation of tracking practices in violation of
5 COPPA, and destruction of all personal data obtained in violation of COPPA.

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

11 **VIII. PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated,
13 respectfully request that this Court:

- 14 a) Certify this case as a class action, appoint Plaintiff Rushing as Class and Subclass
15 representative, and appoint Plaintiffs' counsel to represent the Class and Subclass;
- 16 b) Find that Defendants' actions, as described herein, constitute: (i) breaches of the
17 common law claim of intrusion upon seclusion in the states of Alabama, Alaska,
18 Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii,
19 Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota,
20 Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina,
21 Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont,
22 Washington, and West Virginia and (2) a violation of the right to privacy under
23 California Constitution, Article I, Section 1;
- 24 c) Enter a declaratory judgment that Defendants' actions of collecting, using, or
25 disclosing personal information of child users without first obtaining verifiable
26 parental consent violates COPPA;
- 27 d) Enter an order permanently enjoining Defendants from collecting, using, or
28 disclosing personal information of child users without first obtaining verifiable

- 1 parental consent;
- 2 e) Award Plaintiffs and Class and Subclass members appropriate relief, including
- 3 actual and statutory damages and punitive damages, in an amount to be determined
- 4 at trial;
- 5 f) Award equitable, injunctive, and declaratory relief as may be appropriate;
- 6 g) Award all costs, including experts' fees, attorneys' fees, and the costs of
- 7 prosecuting this action; and
- 8 h) Grant such other legal and equitable relief as the Court may deem appropriate.

9 Dated: August 3, 2017

Respectfully Submitted,

10 /s/ Michael W. Sobol

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

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

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

27 *Attorneys for Plaintiffs and the proposed Class*

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: August 3, 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. 7th St.
Little Rock, AR 72201
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs and the Proposed Class