LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Douglas I. Cuthbertson *(pro hac vice pending)*
dcuthbertson@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 *(pro hac vice pending)*
hbates@cbplaw.com
519 West 7th St.
Little Rock, AR 72201
Telephone: 501.312.8500
Facsimile: 501.312.8505

PARSONS BEHLE & LATIMER
Brook B. Bond
BBond@parsonsbehle.com
800 West Main Street, Suite 1300
Boise, ID 83702
Telephone: 208.562.4900
Facsimile: 208.562.4901

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

AMANDA RUSHING, ASHLEY SUPERNAULT, JULIE REMOLD, and TED POON on behalf of themselves, and as parents and guardians of their children, M.S., L.L., N.B., C.B., R.P., and K.P., and on behalf of all others similarly situated,

Plaintiffs,

v.

KOCHAVA, INC.

Defendant.

Case No. 2:21-cv-322

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. This is an action brought by parents to protect the privacy of their children. Defendant acted—and continues to act—in concert with developers of online child-directed games ("apps") to take personal data from children while they play these apps on mobile devices, monitoring their online behavior, and profiling them for commercial gain.

2. Specifically, Defendant Kochava, Inc. ("Kochava") provides its own proprietary computer code—known as a software development kit ("SDK")—to developers of child-directed gaming apps ("Child Apps"), for those developers to embed within the apps. The Kochava SDK is invisible to the child user who is playing a Child App, but beneath the surface of game, the Kochava SDK is secretly collecting and transmitting sensitive, personal data about the child, the device she is using to play the Child App, and numerous other personally-identifying data points. Through the use of "persistent identifiers"—unique data points (typically numbers and letters), akin to a Social Security Number for a device—Kochava can monitor the child as she uses other Internet-enabled devices, apps, and websites.

3. Kochava uses this information that it has surreptitiously acquired to make money for itself and its clients.

4. Numerous Child App developers have placed the Kochava SDK in their apps, including The Walt Disney Company ("Disney"). Disney develops and markets scores of immensely popular apps directed at young children. Among these apps are Princess Palace Pets, Where's My Water?, Where's My Water? Lite, Where's My Water? Free, and Where's My Water? 2[1] (the "Apps"), which collectively have been downloaded onto hundreds of millions of mobile devices, worldwide.

[1] For Android devices, the app is called Where's My Water? Free. For Apple devices, the same app is called Where's My Water? Lite.

5. Including the Apps, Kochava's SDK is embedded in many thousands of Child Apps, within which its SDK functions similarly, permitting Kochava to secretly and invasively track and monitor hundreds of millions of children, worldwide.

6. Kochava's conduct invaded the reasonable expectation of privacy of both parents and their children, violating existing social norms and concomitant legal standards that substantiate those norms. Plaintiffs bring claims under the law of Intrusion Upon Seclusion on behalf of themselves and a class of parents from 35 states (having the same state law claim), as well as state-specific privacy claims on behalf of the California Subclasses, the New York Class, and the Massachusetts Class. Plaintiffs seek to stop Defendant's unlawful practices and sequester their unlawfully obtained information.

II. PARTIES

A. Plaintiffs

7. Plaintiffs are the parents of children who played online gaming apps containing Kochava's embedded SDK.

8. Plaintiffs were also named representatives in another federal lawsuit against Disney, Kochava (until dismissed on personal jurisdiction grounds), and other technology companies whose SDKs are used by Disney in the Northern District of California. *See Rushing v. The Walt Disney Company*, Case No. 3:17-cv-4419-JD (N.D. Cal.) (the "Disney Action").

9. Plaintiff Amanda Rushing, and her child, "L.L," resided in San Francisco, California during the relevant period. Ms. Rushing brings this action on behalf of herself, L.L., and all others similarly situated. L.L. is a minor and played the Disney app Princess Palace Pets on a mobile device. Princess Palace Pets contained the Kochava SDK.

10. Plaintiff Ashley Supernault, and her child, "M.S.," resided in Agawam, Massachusetts during the relevant period. Ms. Supernault brings this action on behalf of herself,

M.S., and all others similarly situated. M.S. is a minor and played the Disney apps Where's My Water? Free and Where's My Water? 2 on mobile devices. Both Where's My Water? Free and Where's My Water? 2 contained or contain the Kochava SDK.

11. Plaintiff Julie Remold, and her children N.B. and C.B. reside in Menlo Park, California. Ms. Remold brings this action on behalf of herself, N.B., C.B., and all other similarly situated. N.B. and C.B. were minors and played Where's My Water? on a mobile device as minors. Where's My Water? contained or contains the Kochava SDK.

12. Plaintiff Ted Poon, and his children R.P. and K.P. reside in New York, New York. Mr. Poon brings this action on behalf of himself, R.P., K.P., and all other similarly situated. R.P. and K.P. were minors and played Where's My Water? Lite on mobile devices. Where's My Water? Lite contained or contains the Kochava SDK.

B. Defendant

13. Defendant Kochava, Inc. is an American technology company headquartered at 201 Church Street, Sandpoint, Idaho 83864. Kochava provided its own proprietary computer code—its SDK—to developers of Child Apps (including but not limited to Disney) for installation and use in those Child Apps (including but not limited to the Apps). Those same developers embedded Kochava's SDK into their Child Apps, causing the transmittal of app users' Personal Data—including in the form of persistent identifiers—to Kochava to facilitate subsequent tracking and profiling. As used herein, "Personal Data" is any data that refers to, is related to, or is associated with an identified or identifiable individual.

14. Kochava was also a Defendant in the Disney Action, but the Court granted Kochava's motion to dismiss for lack of personal jurisdiction in California, agreeing with Kochava that personal jurisdiction exists instead in Idaho. *See* Dkt. 118. Otherwise, the Court largely denied Defendants' (including Kochava's) motions to dismiss, holding that a

substantively identical complaint plausibly alleged an intrusion upon seclusion and violations of the same state consumer protection laws pled here. On April 12, 2021, the Court in the Disney Action granted final approval to class action settlements with all operative Defendants. *See McDonald et al v. Kiloo ApS et. al*, 17-cv-4344, Dkt. 406-9 to 406-13 (final approval orders in the Disney Action; *see also* Dkt. 407-9 to 407-13 (final judgments in the Disney Action).

III. JURISDICTION AND VENUE

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

16. This Court has personal jurisdiction over Kochava because Kochava admits that its principal place of business and headquarters is in Sandpoint, Idaho (which is within this District), it performs work related to the allegations at issue in this Complaint in this District (among other places), and its business records are kept within this District. *See generally Rushing et al. v. Disney et al.*, No. 3:17-cv-04419-JD, Dkt. No. 114 (Kochava motion to dismiss for lack of personal jurisdiction) at 1, 3 (Kochava keeps its business records in Idaho where it "is headquartered in Sandy Point . . . [and] where Kochava performs its work related to the online video game applications or 'apps' at issue in this action.").

17. In accordance with 28 U.S.C. § 1391, venue is proper in this District because Kochava admits that a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, and because Defendant transacts business and is headquartered in this District.

IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

A. Defendant Surreptitiously Exfiltrates Children's Personal Data As They Play Child Apps Containing the Kochava SDK

18. Kochava's SDK is embedded in myriad Child Apps. These apps are specifically designed for—and marketed to—children's use, exclusively.

19. Plaintiff parents or their children installed these Child Apps—including the Apps—onto mobile devices for the children to play.

20. Unbeknownst to parents and their children, Kochava collects and exfiltrates Personal Data as users play the Child Apps. Child App users were not warned that, as they play the games, Kochava surreptitiously collects the Personal Data and tracks online behavior to profile users for commercial purposes. Users of the Child Apps had no reasonable way to know, and Kochava failed to disclose, that when users download the Child Apps onto their mobile devices, that Kochava's data collection and tracking software (*i.e.*, Kochava's SDK) is also simultaneously downloaded. Even while playing the Child Apps, users had no reasonable way to determine that an SDK has been embedded on their mobile devices to secretly monitor them.

21. As users play the Child Apps, Kochava's SDK software collects their Personal Data and, in a continuous stream, exfiltrates the Personal Data back to Kochava, a sophisticated technology company. From there, the data is used to track and profile children for Kochava's financial gain.

22. Online advertising and marketing is driven by users' Personal Data, and the Kochava SDK employs sophisticated algorithms that interpret that Personal Data to make possible the determination of individually-identifying information about individual users, demographic information about individual users, behavioral information about individual users, and the most effective advertising methods for individual users. Once exfiltrated to Kochava, the

Personal Data harvested from Child App users can be combined with other data associated with that same user via persistent identifiers or using other data (*e.g.*, online activity or demographics) which can track and identify the same user. This is often accomplished via an ad network or other data aggregation provider, where additional data may be associated with the user in a similar fashion.

23. The ad networks – supported by and working in concert with Kochava – operate in a virtual marketplace where app developers and advertisers buy and sell advertising space and the ads to fill it. These networks connect advertisers looking to sell data-driven, targeted ads to mobile apps that want to host advertisements. A key function of an ad network is aggregating available ad space from developers and matching it with advertisers' demands.

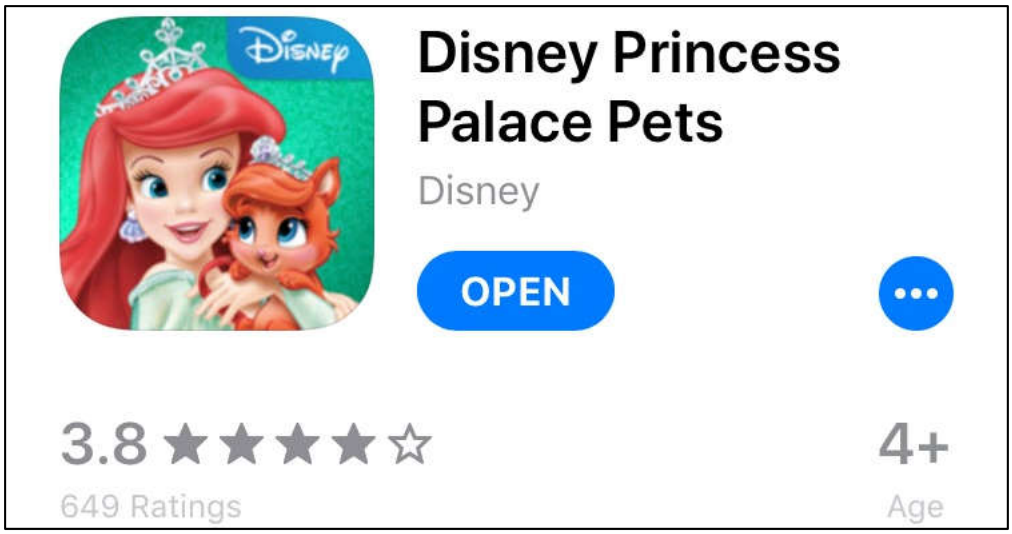
24. Using advanced, custom analytics and network analysis tools, Plaintiffs have been able to: (1) determine that Kochava's software is embedded into Child Apps; (2) record network traffic as it leaves the device, including encrypted data; and (3) detect Personal Data that Kochava accesses in real time and exfiltrates from users' devices. While the following allegations focus on the Apps, Plaintiffs' Counsel's investigation demonstrates that the Kochava SDK behaves similarly in the other Child Apps in which it is embedded.

1. <u>Kochava's SDK Is Embedded in Child Apps</u>

25. Disney is a paradigmatic example: Disney styles and promotes its Apps as fun, kid-friendly games.

a. Princess Palace Pets was available for download as a mobile gaming app in online stores, including Google's "Play Store" and Apple's "App Store," before being retired by Disney in May 2019. Princess Palace Pets has been downloaded millions of times, is still present and active on devices that downloaded Princess Palace Pets before May 2019, and was

marketed as a children's game. The app has an "Everyone" rating in Google's Play Store[2] and "4+" rating in Apple's App Store.[3] Similarly, the Apple age ratings are based on questionnaires completed by the app developer regarding the app's content and reflect its representations about the app's suitability for children,[4] and a 4+ rating indicates that the game is suitable for users ages 9 and older. Additionally, Princess Palace Pets was listed in Google's Designed for Families ("DFF") program, reflecting Disney's proactive efforts to specifically market Princess Palace Pets to children younger than age 13. Historically, apps listed in the DFF program have been featured through Google Play's family-friendly browse and search experiences so that parents could more easily find suitable, trusted, high-quality apps and games, and content must be relevant for children under the age of 13.[5]



[2] Google Play ratings "are intended to help consumers, especially parents, identify potentially objectionable content that exists within an app" and are based on the app developer's responses to questionnaires provided by Google – i.e. the ratings reflect the developer's representations about the appropriate audience for the app. "Play Console Help," Google, *available at* https://support.google.com/googleplay/android-developer/answer/188189?hl=en (accessed on August 6, 2021).

[3] An "Everyone" rating means the app's content is "generally suitable for all ages." *Id.*

[4] "App Store Review Guidelines," Apple, *available at* https://developer.apple.com/app-store/review/guidelines/ (accessed on August 6, 2021).

[5] "Creating Apps and Games for Children and Families," Google Play, *available at* https://developer.android.com/distribute/google-play/families (accessed on August 6, 2021).

Figure 1[6]

b. The content of the app is clearly focused towards children as well. Disney Princess Palace Pets users read and listen to stories about various Disney princesses' pets, and groom and accessorize the animals. The description encourages children to "[l]earn how the pets met the princesses, find out their unique talents, and treat them to a delightful day at the Royal Pet Salon!"

c. Similarly, the Where's My Water? Apps are styled as child-appropriate games in both the App Store and Play Store. Each is or was rated "4+" in the App Store and "Everyone" in the Play Store. Additionally, Where's My Water? is listed in the Google DFF program and Where's My Water? Free was listed there as well, before Disney retired these apps. The apps are some of the most popular family apps in the App Store Where's My Water? Free/Lite and Where's My Water? 2 are free apps, while Where's My Water? costs $1.99 to download. Together, the Where's My Water? Apps have been downloaded more than 200 million times worldwide.

[6] Figure 1 is a picture of Princess Palace Pets as advertised in the Apple App Store, as of June 4, 2018.

Figure 2[7]

d. Each of the Where's My Water? Apps share the same story line: kids must help an alligator named "Swampy" fill the bathtub with water by navigating puzzle-like challenges. As described in the App Store: "Swampy the Alligator lives in the sewers under the city. He's a little different from the other alligators – he's curious, friendly, and loves taking a nice long shower after a hard day at work. But there's trouble with the pipes and Swampy needs your help getting water to his shower!"[8]

26. Again, the Apps are merely exemplars of the many child-oriented apps in which Kochava has embedded its SDK, which are designed and marketed in a manner similar to the Apps.

2. Kochava Uses Persistent Identifiers to Track Children

27. Kochava takes "persistent identifiers" from children's devices to track and profile children. "Persistent identifiers" are a set of unique data points (typically numbers and letters), akin to a Social Security number, and can link one specific individual to all of the apps on her device and her activity on those apps, allowing her to be tracked over time and across each device she uses (*e.g.*, smart phones, tablets, laptops, desktops, and smart TVs).

28. Apple's common persistent identifiers are the ID for Advertisers ("IDFA") and ID for Vendors ("IDFV"). Both the IDFA and the IDFV are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—in order to track and profile the user, and to serve her with targeted advertising.

[7] Figure 2 is a picture of Where's My Water? as advertised in the Apple App Store, as of June 4, 2018.

[8] "Where's My Water," Apple App Store, *available at* https://itunes.apple.com/us/app/wheres-my-water/id449735650?mt=8 (accessed August 6, 2021).

29. The Android operating system's common persistent identifiers are the Android Advertising ID ("AAID") and the Android ID. The AAID and Android ID are unique, alphanumeric strings assigned to a user's device and used by apps and third parties to track and profile the user, and to serve her targeted advertising.

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

31. Kochava exfiltrates and analyzes persistent identifiers—including a user's IDFA/IDFV (for Apple devices), Android ID/AAID (for Android devices), or Device Fingerprint data[9]—in order to learn more about users, including their behaviors, demographics, and preferences. Defendant also uses persistent identifiers to track the effectiveness of those

[9] There are multiple, additional items of data that are universally recognized as persistent identifiers. For example, a device's Wi-Fi MAC address is a fixed serial number that is used to identify one's phone when transmitting and receiving data using Wi-Fi. Plaintiffs' forensic analysis has principally focused on the exfiltration and use of IDFA/IDFV, Android ID/AAID, and Device Fingerprint data persistent identifiers.

advertisements after the user sees them (to determine, for example, whether the user downloaded the app or bought the product advertised).

3. The Moment Users Launch A Child App Containing the Kochava SDK, The App Sends Children's Personal Data to Kochava

32. As soon as a child opens up one of the Child Apps on her device and it connects to the Internet, the app connects to a server belonging to Kochava and begins sending it data. This activity is invisible to the child playing the app, who simply sees the given app's game interface. However, forensic analysis of the internet communication between the device and server can capture the data exchanged between the two.

33. As the user plays the given Child App, unbeknownst to her, the embedded SDK communicates with Kochava's server. The Kochava SDK sends requests—or "calls"—to the server. With each request from the Kochava SDK, the SDK also sends the child user's Personal Data, including in the form of persistent identifiers. The user may receive a single ad (or even no ads at all, in the case of attribution and analytics gathering), but nonetheless Kochava's SDK has exfiltrated to its server the user's Personal Data. Kochava then stores and analyzes the Personal Data to enable continued tracking of the user, such as what ads she has already seen, what actions she took in response to those ads, other online behavior, and additional demographic data. This way, Kochava (and other entities with whom Kochava contracts, including but not limited to Child App developers) can generally monitor, profile, track her over time, across devices, and across the Internet.

34. Forensic testing demonstrates the exfiltration of this Personal Data, the purposes for which it is used, and the lack of restrictions placed on its exfiltration, retention, and use.

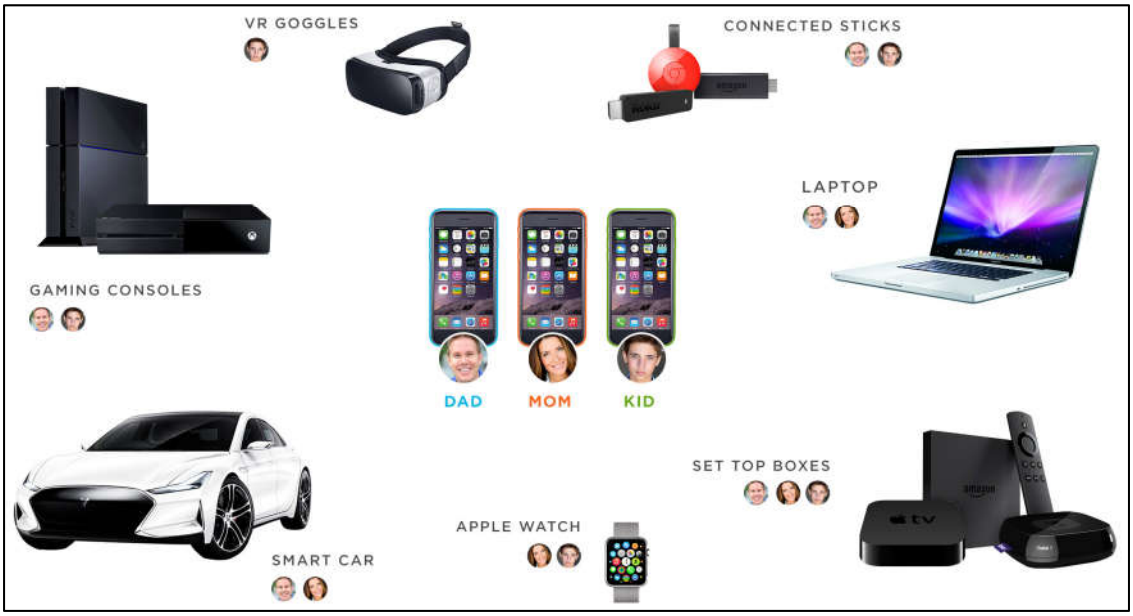
B. Kochava is a Technology Company that Contracts with Numerous Developers that Make Child Apps—Such as Disney—to Use Those Child Apps to Track Children

35. Kochava is a mobile technology company. Kochava offers, *inter alia*, mobile attribution services, which permit advertisers to track whether a user downloads an app after she is served an ad for that app while playing one of the Child Apps. Kochava calls such attribution "one of the most powerful tools at an advertiser's disposal."[10] In order to track the user – and her subsequent activity online over time and across the Internet – Kochava's "mobile attribution platform identifies a user by device ID, fingerprint, and IP address."[11] Kochava then tracks the user as she navigates the Internet, watching to see whether she responds favorably to the advertisement she was shown (by, for example, downloading the advertised app). Then, "[b]y considering every available data point,"—including persistent identifiers—Kochava determines which ad should get attribution—or credit–for the user's ultimate action (it calls this "determining the winning engagement") and crediting that advertiser.[12] Even where a persistent identifier, such as an AAID or IDFA, is not collected—including when the IDs are not exfiltrated because there are "legal reasons precluding the capture of device id"—Kochava advertises its ability to use the Device Fingerprint data as a workaround to match a user's device to an ad she clicked or viewed.[13]

36. Kochava markets its ability to match individual users to their devices using what it calls "cross-device algorithms."[14] The graphic from Kochava's website below illustrates how

[10] "Configurable Attribution," Kochava, *available at* https://www.kochava.com/configurable-attribution/ (accessed August 6, 2021).
[11] https://media-index.kochava.com/ad_partners/kochava-collective (accessed August 6, 2021).
[12] "Configurable Attribution," *supra* at fn 15.
[13] "Configurable Attribution," *supra* at fn 15.
[14] "Holistic Attribution," Kochava, *available at* https://www.kochava.com/holistic-attribution/ (accessed August 6, 2021).

Kochava uses persistent identifiers to track user behavior and to identify users—including children—at the *individual* level, even where there are multiple users of the same device:[15]



37. In the example above, Kochava purports to be able to use its tracking technology to identify individual members of a household ("Dad," "Mom," and "Kid") and to monitor (and specifically attribute and distinguish) their individual behavior on a variety of household electronics.

38. Kochava claims to have the "the world's largest independent mobile advertising platform offering precise audience targeting capabilities" across multiple platforms and ad networks. Kochava collects and combines mobile users' data on its platform, the Kochava Collective. Kochava gets the data for its Kochava Collective first-hand by exfiltrating it from users—like Plaintiffs' children—through its SDK embedded in mobile apps (Kochava states that its SDK "touches more than 1 billion devices globally") and from acquiring additional data from other third-parties, including ad networks and other third-parties.[16] It uses these third-parties to

[15] *Id.*

[16] "Kochava Collection," Kochava, *available at* https://www.kochava.com/data-marketplace/ (accessed on August 6, 2021).

"to provide unique enrichment" to the data it exfiltrates through its SDK.[17] In other words, Kochava is using all of the data that it can acquire, either directly or through third-parties, to build the most detailed possible profiles of individual users, in order to track them over time and across the Internet. Kochava's efforts lead to collection of large amounts of data on *billions* of users: Kochava states that it has "more than 9 billion+ first-party connected devices making it the largest independent mobile data marketplace."[18]

39. In addition to attribution, Kochava's database of Personal Data facilitates targeted advertising based on users' demographics, interests, and behaviors. Specifically, Kochava states that using its Personal Data and services, advertisers can harness "[d]ata collected from vetted first- and third-party sources [that] are ingested and segmented into various behavioral, demographic, and location audience buckets. These audience data segments can be leveraged to enhance a client's internal database for more detailed audience targeting and analysis."[19] The data stored by Kochava is "mapped against key data sets to help match [latitudes and longitudes] to POIs, user agents to device details, app bundle IDs to app store names, categories, and much more."[20]

40. Partners who make their data available to Kochava are able to not only monetize their own potential customers by profiling them, but in further sharing their data with Kochava (and all of Kochava's other customers) they can "generate incremental revenue when [their] data elements are utilized in custom segment creation and lookalike modeled audiences."[21]

---

[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*

C. Kochava Exfiltrates Children's Personal Data While They Play the Child Apps

41. As discussed, *supra*, the Kochava SDK is in myriad Child Apps, including the Apps. Because the Kochava SDK behaves in a substantially similar way across all apps, Plaintiffs use the following forensic analysis of the Apps as an example of Kochava's uniform conduct.

Princess Palace Pets

42. To exfiltrate Princess Palace Pets users' Personal Data for tracking and profiling purposes, the Kochava SDK embedded in Princess Palace Pets communicates with or "makes a call" to Kochava's servers (as evidenced by, for example, data being sent to servers affiliated with the address control.kochava.com). This call contains the user's Personal Data, in the form of persistent identifiers including, among others, her IDFA and IDFV (for Apple devices) or AAID (for Android devices).

43. Additionally, Kochava receives the IP address of the child user's device, which enables the identification of the user's location, the identification of the user's device, and cross-device tracking. An IP address is a unique number that identifies a given device, allowing it to communicate with other computers on the Internet (which have their own IP addresses).

44. Kochava's call to its servers also discloses other valuable Personal Data in the form of Device Fingerprint data that can be used to identify and profile specific users. This information can include, *inter alia*:

a. The user's language;

b. The user's device operating system and version;

c. The user's Kochava device ID;[22]

d. The manufacturer, make, and model of the user's device; and

e. The name and developer of the app the user is operating.

Data Point	Exemplar Data Field[23]	Personal Information Derived from Data
IDFA (Apple users)	B3626A74-54CZ-314C-C825-C2A87669D561	Jane Minor's device's unique IDFA
IDFV (Apple users)	A203BB39-0B2C-3B03-C837-93B3CC938E21	Jane Minor's device's unique IDFV
AAID (Android users)	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
User's device's IP address	216.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number.
User's language	Accept-Language: en-US	Jane Minor's Princess Palace Pets app is in American English
Manufacturer and make of the user's device	User-Agent: iPhone	Jane Minor is playing Princess Palace Pets on her Apple iPhone
User's Kochava device ID	"kochava_device_id": KMN7FB4801DD4328V2VFE5931HB3F2272A	Jane Minor's unique device identifier assigned by Kochava
User's device operating system and version	• "platform": "ios" • "os_version": "iPhone OS 7.1"	Jane Minor's phone is running Apple's iOS 7.1
Application name and developer	• "Kochava_app_id": "kodisneyprincesspalacepetsios" • "package_name": "DisneyDigitalBooks.PalacePets"	Jane Minor is a Disney Princess Palace Pets user

[22] According to Kochava's website, the Kochava device ID is a persistent identifier assigned by Kochava. *See* "Query Reference," Kochava, *available at* https://support.kochava.com/advanced-tools/query-reference (accessed August 6, 2021).

[23] The figures in this table are exemplars and, to protect the Plaintiffs' privacy, do not disclose their Personal Data. Except where indicated otherwise, data points are derived from an Apple device.

Where's My Water?

45. To exfiltrate Where's My Water? users' Personal Data for tracking and profiling purposes, the embedded Kochava SDK makes a call to Kochava's servers (as evidenced by, for example, data being sent to servers affiliated with the address control.kochava.com). This call contains the user's Personal Data, in the form of persistent identifiers including, among others, her IDFA (for Apple devices) or AAID (for Android devices).

46. Kochava also receives the IP address of the child user's device and a timestamp.

47. Kochava's call to its servers also discloses other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, track and profile specific users. This information can include, *inter alia*:

a. The user's language;

b. The screen dimensions of the user's device;

c. The user's device operating system and version;

d. The user's Kochava device ID;

e. The manufacturer, make, and model of the user's device; and

f. The name, developer, and version of the app the user is operating.

Data Point	**Exemplar Data Field**[24]	**Personal Information Derived from Data**
IDFA (Apple users)	B3626A74-54CZ-314C-C825-C2A87669D561	Jane Minor's device's unique IDFA
AAID (Android users)	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
User's device's IP address	216.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across

[24] The figures in this table are exemplars and, to protect the Plaintiffs' privacy, do not disclose their Personal Data. Except where indicated otherwise, data points are derived from an Apple device.

Data Point	Exemplar Data Field[24]	Personal Information Derived from Data
		devices via this number.
User's language	Accept-Language: en-US	Jane Minor's Where's My Water? app is in American English
Manufacturer, make, and model of the user's device	"device": "iPhone6,1"	Jane Minor is playing Where's My Water? on her Apple iPhone 6,1
Timestamp	"usertime": "1527608937"	Jane Minor took a specified action in Where's My Water? on May 29, 2018 at 15:48:57 UTC
User's device operating system and version	"os_version": "iPhone OS 10.3.2"	Jane Minor's phone is running Apple iOS 10.3.2
User's Kochava device ID	"kochava_device_id": KMN7FB4801DD4328V2VFE5931HB3F2272A	Jane Minor's unique device identifier assigned by Kochava
Screen dimensions of the user's device	• "disp_h": 1136 "disp_w": 640	Jane Minor's device screen is 1136 by 640
Application name, developer, and version	• "package_name": "com.disney.SwampyGame" • "app version": "1.0"	Jane Minor is a Where's My Water? (v.1.0) user

Where's My Water? 2

48. To exfiltrate Where's My Water? 2 users' Personal Data for tracking and profiling purposes, the embedded Kochava SDK makes a call to Kochava's servers (as evidenced by, for example, data being sent to servers affiliated with the address control.kochava.com). This call contains the user's Personal Data, in the form of persistent identifiers including, among others, her IDFA (for Apple devices) or AAID (for Android devices).

49. Kochava also receives the IP address of the child user's device.

50. Kochava's call to its servers also discloses other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, track and profile specific users. This information can include, *inter alia*:

a. The user's language;

b. The manufacturer, make, and model of the user's device;

c. The user's device operating system and version;

d. The user's Kochava device ID;

e. The screen dimensions of the user's device; and

f. The name, developer, and version of the app the user is operating.

Data Point	Exemplar Data Field[25]	Personal Information Derived from Data
IDFA (Apple users)	B3626A74-54CZ-314C-C825-C2A87669D561	Jane Minor's device's unique IDFA
AAID (Android users)	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
User's device's IP address	216.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number.
User's language	Accept-Language: en-US	Jane Minor's Where's My Water? 2 app is in American English
Manufacturer, make, and model of the user's device	"device": "iPhone 6,1"	Jane Minor is playing Where's My Water? 2 on her Apple iPhone
User's device operating system and version	"os_version": "iOS 10.3.2"	Jane Minor's phone is running Apple's iOS 10.3.2
User's Kochava device ID	"kochava_device_id": KMN7FB4801DD4328V2VFE5931HB3F2272A	Jane Minor's unique device identifier assigned by Kochava
Screen dimensions of the user's device	"disp_h": "1136" "disp_w": "640"	Jane Minor's device screen is 1136 by 640
Application name and developer	"package_name": "com.disney.wheresmywater2"	Jane Minor is a Where's My Water? 2 user

[25] The figures in this table are exemplars and, to protect the Plaintiffs' privacy, do not disclose their Personal Data. Except where indicated otherwise, data points are derived from an Apple device.

Where's My Water? (Free/Lite)

51. To exfiltrate Where's My Water? Free/Lite users' Personal Data for tracking and profiling purposes, the embedded Kochava SDK makes a call to Kochava's servers (as evidenced by, for example, data being sent to servers affiliated with the address control.kochava.com). This call contains the user's Personal Data, in the form of persistent identifiers including, among others, her IDFA (for Apple devices) or AAID (for Android devices).

52. Kochava also receives the IP address of the child user's device.

53. Kochava's call to its servers also discloses other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, track and profile specific users. This information can include, *inter alia*:

a. The user's language;

b. The screen dimensions of the user's device;

c. The user's device operating system and version;

d. The user's Kochava device ID;

e. The manufacturer, make, and model of the user's device; and

f. The name, developer, and version of the app the user is operating.

Data Point	Exemplar Data Field[26]	Personal Information Derived from Data
IDFA (Apple users)	B3626A74-54CZ-314C-C825-C2A87669D561	Jane Minor's device's unique IDFA
AAID (Android users)	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID

[26] The figures in this table are exemplars and, to protect the Plaintiffs' privacy, do not disclose their Personal Data. Except where indicated otherwise, data points are derived from an Apple device.

Data Point	Exemplar Data Field[26]	Personal Information Derived from Data
User's device's IP address	216.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number.
User's language	Accept-Language: en-US	Jane Minor's Where's My Water? Free/Lite app is in American English
Manufacturer, make, and model of the user's device	"device": "iPhone6,1"	Jane Minor is playing Where's My Water? Free/Lite on her Apple iPhone 6,1
User's device operating system and version	"os_version": "iPhone OS 10.3.2"	Jane Minor's phone is running Apple iOS 10.3.2.
User's Kochava device ID	"kochava_device_id": KMN7FB4801DD4328V2VFE5931H B3F2272A	Jane Minor's unique device identifier assigned by Kochava
Screen dimensions of the user's device	• "disp_h": 1136 • "disp_w": 640	Jane Minor's device screen is 1136 by 640
Application name, developer, and version	• "package_name": "com.disney. SwampyGameLite" • "app version": "1.0"	Jane Minor is a Where's My Water? Free/Lite (v.1.0) user

D. The Privacy-Invasive and Manipulative Commercial Purposes Behind Defendant's Data Exfiltration, and its Effect on Child Users

1. The Role of Persistent Identifiers in User Profiling and Online Advertising

54. Kochava collects and uses the Personal Data described above to track and profile children.

55. 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 mobile 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 commercially.

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

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

> [O]ne ad network received information from 31 different apps. Two of these apps transmitted geolocation to the ad network along with a device identifier, and the other 29 apps *transmitted other data (such as app name, device configuration details, and the time and duration of use) in conjunction with a device ID. The ad network could thus link the geolocation information obtained through the two apps to all the other data collected through the other 29 apps by matching the unique, persistent device ID*.[27]

[27] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade," FTC Staff Report (Dec. 2012), at 10 n. 25 (citing David Norris, Cracking the Cookie Conundrum with Device ID, AdMonsters (Feb. 14, 2012), *available at* http://www.admonsters.com/blog/cracking-cookie-conundrum-device-id (accessed on August 6, 2021) ("Device ID technology is the ideal solution to the problem of remembering what a user has seen and what actions he or she has taken: over time, between devices and across domains. … *Device ID can also help businesses understand visitor behavior across devices belonging to the same person or the same residence.*").

58. The FTC expressed particular "[c]oncerns about creations of detailed profiles based on device IDs [such as those created and facilitated by Defendant]…where…companies (like ad networks and analytics providers) collect IDs and other user information through a vast network of mobile apps. This practice can allow information gleaned about a user through one app to be linked to information gleaned about the same user through other apps."[28]

59. Kochava traffics in the same data identified by the FTC (persistent identifiers such as IDFA/AAID and Device Fingerprint data)[29] causing the same harm the FTC identified—allowing ad networks to combine data points about child users from a multitude of apps.

60. The FTC Mobile Apps for Kids Report cautions that it is standard practice—and long has been standard practice—for ad networks, mobile advertisers, and ad middlemen (including, for example, Kochava and its partners and agents) to link the persistent identifiers they acquire with *additional* Personal Data—such as name, address, email address—allowing those entities and their partners to identify individual users whom they profile with indisputable, individual specificity.[30]

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

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

[28] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade." FTC Staff Report (Dec. 2012), at 9.

[29] *See* ¶¶ 40-52 (demonstrating that Kochava transmits, *inter alia*, IDFA/AAID and Device Fingerprint data when serving targeted ads to child users).

[30] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade." FTC Staff Report (Dec. 2012), at 10 n. 25 (citing Jennifer Valentino-DeVries, *Privacy Risk Found on Cellphone Games, Digits Blog*, Wall St. J. (Sept. 19, 2011), *available at* http://blogs.wsj.com/digits/2011/09/19/privacy-risk-found-on-cellphone-games/ (accessed on August 6, 2021) (noting how app developers and mobile ad networks often use device IDs to keep track of user accounts and store them along with more sensitive information like name, location, e-mail address or social-networking data)).

> 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.[31]

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

> Although consumers are becoming increasingly vigilant about safeguarding the information they share on the Internet, many are less informed about the plethora of information created about them by online companies as they travel the Internet. *A consumer may be aware, for example, that a search engine provider may use the search terms the consumer enters in order to select an advertisement targeted to his interests*. *Consumers are less aware, however, of the true scale of the data being collected about their online activity*. A visit to an online news site may trigger interactions with hundreds of other parties that may be collecting information on the consumer as he travels the web. The Subcommittee found, *for example, a trip to a popular tabloid news website triggered a user interaction with some 352 other web servers as well.…The sheer volume of such activity makes it difficult for even the most vigilant consumer to control the data being collected or protect against its malicious use*.[32]

63. A 2012 chart of the mobile digital marketplace,[33] attached hereto as **Exhibit A**, indicates that hundreds of intermediaries from location trackers to data aggregators to ad

[31] 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).

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

[33] Laura Stampler, "This RIDICULOUS Graphic Shows How Messy Mobile Marketing Is Right Now," Business Insider (May 23, 2012) (*available at* http://www.businessinsider.com/this-ridiculous-graphic-shows-how-the-insanely-complicated-world-of-mobile-marketing-works-2012-5) (accessed on August 6, 2021).

networks "touch" the data that is used to track and profile an individual in a given online transaction.

64. By 2017, the number of unique companies in this space swelled to almost 5,000, as shown in **Exhibit B**, attached hereto.[34]

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

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

67. Permitting technology companies to obtain children's persistent identifiers exposes those children to targeted advertising. The ad networks, informed by the surreptitious

[34] Scott Brinker, "Marketing Technology Landscape Supergraphic" Chief Marketing Technology Blog (May 10, 2017) (*available at* https://chiefmartec.com/2017/05/marketing-techniology-landscape-supergraphic-2017/) (accessed on August 6, 2021).

collection of Personal Data from children, will assist in the sale of advertising placed within the gaming apps and targeted specifically to children.

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

2. Kochava Uses Children's Personal Data to Profile Them, Despite Children's Heightened Vulnerability to Advertising

69. Kochava uses Child App users' Personal Data to facilitate targeted advertising, marketing, and profiling of children. It engages in this behavior despite the known risks associated with and ethical norms surrounding advertising to children.[35]

70. Advertisers regard children as valuable advertising targets.[36] Children influence the buying patterns of their families—an influence that amounts to billions of dollars each year—and have lucrative spending power themselves.[37] Children and teens are thus prime targets for advertisers.

71. Kochava enhances advertising efforts at children despite widespread awareness that children are more vulnerable to deception by advertisers because they are easily influenced

---

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

[36] Lara Spiteri Cornish, *'Mum, can I play on the Internet?' Parents' understanding, perception, and responses to online advertising designed for children*, 33 Int'l J. Advertising 437, 438 (2014) ("Indeed, in recent years, marketers targeting children have developed a strong online presence…"); Issie Lapowsky, "Why Teens are the Most Elusive and Valuable Customers in Tech," Inc., *available at* https://www.inc.com/issie-lapowsky/inside-massive-tech-land-grab-teenagers.html (accessed August 6, 2021).

[37] Sandra L. Calvert, *Children as Consumers: Advertising and Marketing*, 18 Future Child 205, 207 (2008).

by its content, lack the cognitive skills to understand the intention of advertisers, and can struggle to distinguish between advertisements and other content.[38] This is particularly problematic when using targeted advertising which, by design, more effectively sways target audiences.[39] Research supports that online advertisements pose heightened risks to children.[40]

72. Exposure to advertising can also lead to negative outcomes for children, including increasing conflict with their parents, cynicism, health issues, and increased materialism.[41]

73. Children often lack the skills and knowledge necessary to assess and appreciate the risks associated with online data exfiltration and tracking.[42] Even attempts to disclose privacy-violative behavior are not easily understood. Research has found that policies explaining the exfiltration and use of children's data are difficult even for adults to understand, and marketers make no effort to explain their targeted marketing practices to child and teen audiences in developmentally appropriate and easy-to-understand ways.[43] This practice "could mislead these vulnerable emerging consumers into thinking that they are only playing games and their data are not collected for any purpose."[44]

---

[38] Xiaomei Cai and Xiaoquan Zhao, Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues, 29 Computers in Human Behavior 1510-1518 (2013), at 1510 (collecting studies); *Children as Consumers: Advertising and Marketing*, *supra* at fn 42; *Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors*, *supra* at fn 40, at 2 (collecting studies); *'Mum, can I play on the internet?'*, *supra* at fn 41, at 438-39 (collecting studies).

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

[40] *'Mum, can I play on the Internet?'*, *supra* at fn 41, at 440-42 (collecting studies).

[41] *Children as Consumers: Advertising and Marketing*, *supra* at fn 42, at 118-119.

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

[43] *Internet Research in Online Environments for Children*, *supra* at fn 44, at 9.

[44] *Internet Research in Online Environments for Children*, *supra* at fn 44, at 10.

3. Defendant Exfiltrates and Analyzes Children's Personal Data to Track the Effect of Their Ads on Children's Behavior

74. Kochava exfiltrates and analyzes users' Personal Data to facilitate the targeted advertising and profiling of children, specifically to determine whether the ad is successful in affecting children's behavior. This is called ad attribution.

75. Kochava tracks the impact and value of rewarded videos and other ads by tracking users' activities across the Internet after they interact with those ads.

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

a. Kochava markets its ability to offer ad attribution services through its SDK. For example, Kochava markets that "attribution is one of the most powerful tools at an advertiser's disposal."[45] Kochava further states that it provides attribution services "[b]y considering every available data point (impressions, clicks, installs and events) before determining the winning engagement. . ."[46] It markets that it collects "device information when an impression is served or a user clicks on an advertisement served by a network. Each of these

[45] "Configurable Attribution," Kochava, *available at* https://www.kochava.com/configurable-attribution/ (accessed on August 6, 2021).
[46] *Id.*

engagements are eligible for attribution. This collected device information ranges from unique device identifiers to the IP address of the device at the time of click or impression. . .”[47]

77. Kochava exfiltrates Plaintiffs’ and Class Members’ children’s Personal Data from their devices to support targeting them for advertising based on their behavior, demographics, and location. Kochava continues to track children via their Personal Data after ads are shown in order to monitor their behavior into the future and analyze whether and how it was influenced by those same targeted ads. This ongoing exfiltration, tracking, and analysis violates Plaintiffs’ privacy and exploits their vulnerabilities as children.

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

78. Kochava, developers, and third-party advertisers benefit from increased mobile device usage among children. The longer and more often a child plays Child Apps, the more Personal Data about that child Kochava can exfiltrate and commercialize. Particularly for free apps, this increased opportunity to exfiltrate and monetize children’s Personal Data and expose them to advertising is critically important to Kochava.[48]

79. The mobile advertising ecosystem does not simply benefit from increasing app use and mobile device addiction, it actively feeds it. Kochava and its partners use user data to program their apps to “hook” users, and to keep them playing the App.[49] A key service marketed by Kochava is its ability to use marketing to retain App users, *i.e.*, to keep users playing an

[47] “Attribution Overview,” Kochava, *available at* https://support.kochava.com/reference-information/attribution-overview (accessed on August 6, 2021).
[48] “Your phone is trying to control your life,” PBS News Hour, *available at* https://www.youtube.com/watch?v=MacJ4p0vITM (accessed August 6, 2021).
[49] 60 Minutes, “Brain Hacking,” *available at* https://www.youtube.com/watch?v=awAMTQZmvPE (accessed August 6, 2021); Nicholas Kardaras, Glow Kids (2016), at XVIII-XIX, 22, 32.

App.[50] Retention strategies are used to combat "churn," or loss of users due to the user becoming disinterested in the app.[51] Kochava markets its ability to help app developers (such as Disney and other Child App developers) increase user retention, and thereby their profits.[52]

80. Kochava's retention services are fueled by user data. Kochava touts its "predictive behavior modeling" technology, which was "developed by Kochava data science and engineering teams to help clients predict the churn of a user before it happens."[53]

81. Predictive behavior modeling involves constant (and secret) monitoring of an individual child's activity within a Child App during the first seven days after installation. As described by Kochava, "[a]fter a new install, our machine learning algorithms go to work using a form of decision tree modeling to analyze recency, frequency, trend metrics, and other data variables during the first 7 days of a user's interactions with the app."[54] On the 8th day, the individual "is assigned a churn score. 'Churn' in this case means how likely is the device to not have activity in the app between day 8 and day 38 after install."[55]

82. Categorizing individual users (including children) with this "churn score" enables developers to manipulate the users who are least likely to continue to play a Child App. Put another way: Kochava identifies children who need extra motivation to become hooked on a given game. Kochava's privacy invasive and surreptitious monitoring and profiling technologies allow developers "to strategically intercept that user with targeted reengagement efforts. Using

---

[50] *See, e.g.*, "Predictive Behavior Modeling," Kochava, *available at* https://www.kochava.com/predictive-behavior-modeling/ (marketing the Kochava's ability to monitor user activity and, based on sophisticated algorithms, determine a user's likeliness to play (or not play) a given app, and further how to "push" potentially reluctant users into continuing to play that app) (accessed August 6, 2021).
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*

analytics, marketers can segment audiences according to churn-likelihood scores and syndicate 'Medium High' and/or 'High' likelihood segments to reengagement partners like Kochava for focused targeting campaigns to drive retention."[56]

83. Thus, to enhance retention, Kochava uses children's Personal Data to analyze their demographics and behavior, and trigger events—both within the App and across the Internet—that will encourage them to play the App more often and for longer periods. Kochava's retention tool allows developers to sort and analyze User Data by myriad different categories in order to see "a visualization of the retention of Installs, RPU (Revenue per User), Revenue, and events for a selected timeframe."[57] Developers can see how successful they were at retaining users by app, by device data (including type and carrier), events, and location.[58]

84. Kochava also markets that it keeps user data "in perpetuity" so that it can "recognize[] when dormant users return to the app or when users, who have deleted an app, reinstall regardless of the timing."[59]

85. Kochava exfiltrates Child App users' Personal Data—including Plaintiffs' Children's Personal Data—from their devices and uses it for tracking to entice users to play the App longer and more often. Kochava uses sophisticated algorithms to determine whether and when to target users with specific in-App cues or out-of-App ads. This behavior increases Kochava's revenue, all the while violating Plaintiffs' privacy, manipulating their desire to play a Child App, and exposing them to the negative outcomes associated with increased mobile device usage by children.

---

[56] *Id.*

[57] "Analytics Retention," Kochava, *available at* https://support.kochava.com/analytics-reports-api/analytics-overview/analytics-retention (accessed August 6, 2021).

[58] *Id.*

[59] "Data Retention," Kochava, *available at* https://www.kochava.com/data-retention/ (accessed August 6, 2021).

86. Mobile device usage among children is widespread and growing. As of 2017, 95% of families with children younger than 8-years-old had a smartphone, and 78% had a tablet.[60] The proportion of homes with a tablet has nearly doubled over the past four years.[61] Often, children have their own devices; as of 2017, 45% of children younger than 8-years-old had their own mobile device, up from only 3% in 2011 and 12% in 2013.[62]

87. Children spend increasingly more time on mobile devices. On average, a child younger than 8-years-old spends 48 minutes every day on a mobile device, more than four times the average time spent in 2013,[63] while children between the ages of eight and twelve spend 141 minutes on mobile devices and teens spend 252 minutes.[64] Mobile games are popular among children, second only to watching TV or videos.[65] Children younger than 8-years-old spend an average of 16 minutes every day gaming, more than doubling since 2013.[66] Twenty-seven percent of children ages 8 to 18 report playing mobile games every day,[67] and those who play games average about 70 minutes *every day* doing so.[68]

---

[60] Victoria Rideout, The Common Sense Census: Media Use By Kids Age Zero To Eight, Common Sense Media (2017) at 3, *available at* https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2017 (accessed August 6, 2021).

[61] Media Use By Kids Age Zero To Eight, *supra* at fn 65, at 23.

[62] *Id.*

[63] *Id.*

[64] Victoria Rideout, "The Common Sense Census: Media Use by Tweens and Teens," Common Sense Media (2015) at 21, *available at* https://www.commonsensemedia.org/sites/default/files/uploads/research/census_researchreport.pdf (accessed August 6, 2021).

[65] Media Use By Kids Age Zero To Eight, *supra* at fn 65, at 23.

[66] *Id.* at 31.

[67] Media Use by Tweens and Teens, *supra* at fn 69, at 15.

[68] *Id.*, at 24.

88. As the use of mobile devices rises, so too do awareness of and concern about the effects of this use on children.[69] The consequences of mobile device overuse, particularly among children, is well-known in the tech industry,[70] with many industry leaders refusing to allow their own children to own or use devices,[71] or attend schools where such devices are prevalent.

89. In a study, forty percent of parents of 5- to 8-year-olds reported difficulty getting their children to turn off mobile devices.[72] 53% percent of teens and 72% of kids age 8-12 report conversations with their parents about how much time they spend on mobile devices.[73] Parents are increasingly concerned about their children's mobile device usage, and for good reason: research has associated increasing usage with negative consequences for children,[74] such as

[69] *See, e.g.*, Xiaomei Cai and Xiaoquan Zhao, Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues, 29 Computers in Human Behavior 1510-1518 (2013); Barry Rosenstein and Anne Sheehan, "Open letter from JANA Partners and CALSTRS to Apple Inc.," Jan. 6, 2018, *available at* https://thinkdifferentlyaboutkids.com/letter/ (accessed August 6, 2021) (letter to Apple citing "growing body of evidence" that increasing mobile device use leads to "unintentional negative consequences" for young users).

[70] *See, e.g.*, Farhad Majoo, "It's Time for Apple to Build a Less Addictive iPhone," New York Times, Jan. 17, 2018, *available at* https://www.nytimes.com/2018/01/17/technology/apple-addiction-iphone.html (accessed August 6, 2021) ("Tech 'addiction' is a topic of rising national concern."); Thuy Ong, "Sean Parker on Facebook: 'God only knows what it's doing to our children's brains'," The Verge, Nov. 9, 2017, *available at* https://www.theverge.com/2017/11/9/16627724/sean-parker-facebook-childrens-brains-feedback-loop (accessed August 6, 2021) (former tech industry leader recognizing that app creators intentionally "exploit[] human vulnerabilities" to increase app engagement).

[71] Nick Bilton, "Steve Jobs Was a Low-Tech Parent," New York Times, September 10, 2014, *available at* https://www.nytimes.com/2014/09/11/fashion/steve-jobs-apple-was-a-low-tech-parent.html (accessed August 6, 2021); Claudia Dreifus, "Why We Can't Look Away From Our Screens," New York Times, March 6, 2017, *available at* https://www.nytimes.com/2017/03/06/science/technology-addiction-irresistible-by-adam-alter.html (accessed August 6, 2021).

[72] Media Use By Kids Age Zero To Eight, *supra* at fn 65, at 41.

[73] Media Use by Tweens and Teens, *supra* at fn 69, at 71.

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

increasing rates of ADHD,[75] depression,[76] anxiety,[77] and reduced focus in the classroom.[78] One recent study showed that children between the ages of 12 and 18 who spent more time playing games had lower average social-emotional well-being.[79]

90. Most parents think that children are better off spending less time on their mobile devices.[80] Three out of four parents are worried about their children's use of screen devices.[81] A study showed that 67% of parents of children under age 8 worry about companies collecting data about their children through media, while 69% are concerned about too much advertising.[82]

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

91. "Invasion of privacy has been recognized as a common law tort for over a century. *Matera v. Google Inc*., 2016 U.S. Dist. LEXIS 130778, at * 27 (N.D. Cal, Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A-I for the proposition "that the right to privacy was first accepted by an American court in 1905, and 'a right to privacy is now recognized in the great majority of the American jurisdictions that have considered the question'"). As Justice Brandeis explained in his seminal article, *The Right to Privacy*, "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890). The Second Restatement of Torts recognizes the same privacy rights through its tort of intrusion upon

[75] Glow Kids, *supra* at fn 54, at 123-124.
[76] *Id.*, at 127.
[77] *Id.*, at 127; "Brain Hacking," *supra* at fn. 54.
[78] Glow Kids, *supra* at fn 54, at 123.
[79] Media Use by Tweens and Teens, *supra* at [fn 69, at 79].
[80] Media Use By Kids Age Zero To Eight, *supra* at fn 65, at 39.
[81] *Id*., at 42.
[82] *Id*., at 42.

seclusion, explaining that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy." Restatement (Second) of Torts § 652B (1977). The Supreme Court has similarly recognized the primacy of privacy rights, explaining that the Constitution operates in the shadow of a "right to privacy older than the Bill of Rights." *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).

92. Most recently, the Supreme Court explicitly recognized the reasonable expectation of privacy an individual has in her cell phone, and the Personal Data generated therefrom, in its opinion in *Carpenter v. United States,* 138 S. Ct. 2206 (2018). There, the Court held that continued access to an individual's cell phone location data constituted a search under the Fourth Amendment, and that the third-party doctrine (which obviates Fourth Amendment protections when a party knowingly provides information that is the subject of the search to third parties) did not apply to such data. Critical to the Court's analysis was the fact that

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

Id. at 2218 (internal citations omitted).

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

1. Kochava's Surreptitious and Deceptive Collection of Children's Personal Data Violates Plaintiffs' Reasonable Expectations of Privacy and is Highly Offensive

94. A reasonable person believes the conduct described above violates Plaintiffs' expectations of privacy.

95. A survey conducted by the Center for Digital Democracy ("CDD") and Common Sense Media of more than 2,000 adults found overwhelming support for the basic principles of privacy embedded in state common law, as well as federal law.[83] The parents who were polled responded as follows when asked whether they agreed or disagreed with the following statements:

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

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

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

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

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

[83] Center for Digital Democracy, Survey on Children and Online Privacy, Summary of Methods and Findings, *available at* https://www.democraticmedia.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf

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

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

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

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

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

96. In a 2013 primer designed for parents and kids to understand their privacy rights online, the CDD noted similar findings:[84]

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

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

[84] *See* Center for Digital Democracy, The New Children's Online Privacy Rules: What Parents Need to Know, 6 (June 2013), https://www.democraticmedia.org/sites/default/files/CDDCOPPAParentguideJune2013.pdf. (accessed August 6, 2021)

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

97. In a Pew Research Center study, nearly 800 Internet and smartphone users were asked the question, "how much do you care that only you and those you authorize should have access to information about where you are located when you use the Internet?" 54% of adult Internet users responded "very important," 16% responded "somewhat important," and 26% responded "not too important."[85]

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

99. Smartphone owners are especially active when it comes to these behaviors. Some 50% of smartphone owners have cleared their phone's browsing or search history, while 30% have turned off the location tracking feature on their phone due to concerns over who might access that information.[86] Such behaviors exemplify people's expectation that their personal information—including their location—not be tracked by others online.

100. In another study by the Pew Research Center on the Internet and American Life, respondents were asked, "Which of the following statements comes closest to exactly how you, personally, feel about targeted advertising being used online—even if neither is exactly right?" 68 percent said, "I'm not okay with it because I don't like having my online behavior tracked and

[85] Lee Rainie, et al., Pew Research Center, Anonymity, Privacy, and Security Online, 7 (Sept. 5, 2013) (accessed August 6, 2021), https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/.

[86] Jan Lauren Boyles, et al., Pew Research Center Privacy and Data Management on Mobile Devices (Sept. 5, 2012), *available at* https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/ (last accessed on August 6, 2021).

analyzed." 28 percent said, "I'm okay with it because it means I see ads and get information about things I'm really interested in."[87] Thus, more often than not, attitudes toward data collection for use in targeted advertising are negative.

101. A survey of 802 parents and their age 12 to17 year-old teenage children showed that "81% of parents of online teens say they are concerned about how much information advertisers can learn about their child's online behavior, with some 46% being 'very' concerned."[88]

102. A study comparing the opinions of young adults between the ages of 18 to 23 with other typical age categories (25-34, 35-44, 45-54, 55-64, and 65+) found that a large percentage is in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions.[89] For example, 88% of young adults surveyed responded that "there should be a law that requires websites and advertising companies to delete all stored information about an individual"; for individuals in the 45-54 age range, 94% approved of such a law.

103. The same study noted that "[o]ne way to judge a person's concern about privacy laws is to ask about the penalties that companies or individuals should pay for breaching them." A majority of the 18-24 year olds polled selected the highest dollar amount of punishment ("more than $2,500") in response to how a company should be fined if it purchases or uses

[87] Kristen Purcell, et al., Pew Research Center, *Search Engine Use 2012* (2012) *available at* https://www.pewresearch.org/internet/2012/03/09/search-engine-use-2012/#:~:text=For%20more%20than%20a%20decade,email%20as%20an%20internet%20pursuit.&text=On%20any%20given%20day%20in,a%20search%20engine%20(59%25) (last accessed August 6, 2021).

[88] Mary Madden, et al., Pew Research Center, *Parents, Teens, and Online Privacy* (2012), *available at* https://www.pewresearch.org/internet/2012/11/20/parents-teens-and-online-privacy/#:~:text=42%25%20of%20parents%20of%20online,that%20their%20child%20is%20using (last accessed August 6, 2021).

[89] Chris Hoofnagle et al., *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (2010), *available at* http://ssrn.com/abstract=1589864 (last accessed August 6, 2021).

someone's personal information illegally; across all age groups, 69% of individuals opted for the highest fine. Finally, beyond a fine, around half of the sample (across all age groups) chose the harshest penalties for companies using a person's information illegally—putting them out of business and jail time.

104. Another study's "findings suggest that if Americans could vote on behavioral targeting today, they would shut it down." The study found that 66% of 1000 polled individuals over the age of 18 did not want online advertisements tailored for them, and that when the same individuals were told that tailored advertising was "based on following them on other websites they have visited," the percentage of respondent rejecting targeted advertising shot up to 84%.[90]

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

106. The study found that 55% of 18-24 year old Americans rejected tailored advertising when they were not informed about the mechanics of targeted advertising. As with the general sample, the percentage of rejections shot up to 67% when those 18-24 year olds were informed that tailored advertising was based on their activities on the website they are visiting, and then 86% when informed that tailored ads were based on tracking on "other websites" they had visited. Despite the overwhelming aversion to targeted advertising, these findings suggest that public concern about privacy-intrusive targeted advertising is *understated* based on the fact that the public may not fully understand how a targeted advertisement is delivered to it. When

[90] Joseph Turow et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (2009), *available at* http://ssrn.com/abstract=1478214 (last accessed August 6, 2021).

properly understood by consumers, targeted advertising, and the tracking and profiling in the background, is decried across all age groups.

107. A survey on consumer expectations in the digital world, conducted by Deloitte's Technology, Media & Telecommunications practice[91] and based on polling conducted in 2017 of 2,088 individuals (from the following age groups: ages 14-20 (born 1997–2003); ages 21–34 (born 1983–1996); ages 35-51 (born 1966-1982); ages 52-70 (born 1947-1965); ages 71+ (born 1946 or earlier) found:

a. 73% of all U.S. consumers indicated they were concerned about sharing their personal data online and the potential for identity theft.

b. In 2017, there was a 10-point drop in willingness to share personal data in exchange for personalized advertising (from 37% to 27%).

c. The reason for the sudden change in U.S. consumers' attitudes is they overwhelmingly lack confidence in companies' ability to protect their data: 69% of respondents across generations believe that companies are not doing everything they can to protect consumers' personal data.

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

108. In the same vein, one news organization recently summarized a *Journal of Consumer Research* article, capturing society's discomfort with and feelings of revulsion toward

[91] Kevin Westcott et al., Center for Technology, Media & Telecommunications, *Digital Media Trends Survey: A New World of Choice for Digital Consumers* (12th ed.), *available at* https://www2.deloitte.com/content/dam/insights/us/articles/4479_Digital-media-trends/4479_Digital_media%20trends_Exec%20Sum_vFINAL.pdf (last accessed August 6, 2021).

the practice of targeted advertising and the data exfiltration required: "There's something unnatural about the kind of targeting that's become routine in the ad world, this paper suggests, something taboo, a violation of norms we consider inviolable — it's just harder to tell they're being violated online than off. But the revulsion we feel when we learn how we've been algorithmically targeted, the research suggests, is much the same as what we feel when our trust is betrayed in the analog world."[92]

109. By collecting and sharing Plaintiffs' personal information in order to assist in profiling and tracking them across multiple online platforms, and failing to obtain Plaintiffs' permission, Defendants have breached Plaintiffs' expectations of privacy.

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

a. Legislative enactments reflect society's growing concern for digital privacy. For example, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501, *et seq.*, which prohibits online services (including SDKs like Kochava) from collecting children's personal information without first obtaining verifiable parental consent.

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

c. Self-regulation agencies in the online advertising industry note the American consumers' reasonable concern with online privacy (92% of Americans worry about

[92] Sam Biddle, "You Can't Handle the Truth about Facebook Ads, New Harvard Study Shows" The Intercept, (May 9, 2018), *available at* https://theintercept.com/2018/05/09/facebook-ads-tracking-algorithm/?utm_source=digg&utm_medium=email (accessed August 6, 2021).

their online data privacy) and that the top causes of that concern include Defendants conduct at issue here: companies collecting and sharing personal information with other companies.[93]

2. Kochava's Breach of Privacy Norms Is Compounded by Its Tracking and Profiling of Children

111. Defendant's unlawful intrusion into users' privacy is made even more egregious and offensive by the fact that it has collected *children's* information, without obtaining parental consent.

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

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

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

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

[93] "Data Privacy is a Major Concern for Consumers," TrustArc Blog, Jan. 28, 2015 *available at* https://www.trustarc.com/blog/2015/01/28/data-privacy-concern-consumers/ (accessed August 6, 2021).

b. Under state law, children are frequently protected via parental consent requirements. Idaho Code § 33-133 requires that schools entering into contracts with private vendors that contain aggregated student data "disclose[] in clear detail the secondary uses and receive[] written permission from the student's parents or legal guardian" and that the private vendor detail any secondary uses of the data and "obtain express parental consent for those secondary uses."

c. As discussed *supra*, at the federal level, the Children's Online Privacy Protection Act ("COPPA"), protects, *inter alia*, children's personal information from being collected and used for targeted advertising purposes without parental consent, and reflects a clear nationwide norm about parents' expectations to be involved in how companies profile and track their children online.

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

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

parents the reassurance that when our children are on the Internet they will not be asked to give out personal information to commercial Web site operators without parental consent."[94]

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

117. For example, a survey of professionals in the advertising industry found that a "substantial majority of the respondents [advertising professionals] (79%) agrees that the collection of personal information of children should be prohibited," and over "[h]alf of the advertisers (56.8%) agrees with this statement if teenagers are concerned."[95]

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

119. In the same vein, the Children's Advertising Review Unit, an arm of the advertising industry's self-regulation branch, recommends that companies take the following steps, *inter alia*, to meet consumers' reasonable expectations of privacy and avoid violating the law:[96]

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

---

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

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

[96] Children's Advertising Review Unit, *Self-Regulatory Program for Children's Advertising* (2014), *available at* https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/self-regulatory-program-for-childrens-advertising-revised-2014-.pdf (last accessed August 6, 2021).

should recognize that younger children have a limited capacity to evaluate the credibility of information, may not understand the persuasive intent of advertising, and may not even understand that they are being subject to advertising.

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

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

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

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

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

120. By failing to (1) obtain parental consent, (2) disclose to parents the nature of its data collection practices, and (3) take other steps to preclude children from accessing apps that surreptitiously capture their personal information, Kochava has breached parents' and their children's reasonable expectation of privacy, in contravention of privacy norms that are reflected

in consumer surveys, centuries of common law, state and federal statutes, legislative commentaries, industry standards and guidelines, and scholarly literature.

F. The Child Apps Containing the Kochava SDK are Marketed as Suitable for Children and in Compliance with All Applicable Privacy Laws and Norms

121. Like Kochava, the developers of the Child Apps fail to inform children that their Personal Data is being surreptitiously siphoned in order to monitor, track, and profile those children for privacy-invasive purposes. The Kochava SDK is embedded in myriad Child Apps that market the apps as suitable for children and in compliance with privacy laws and norms.

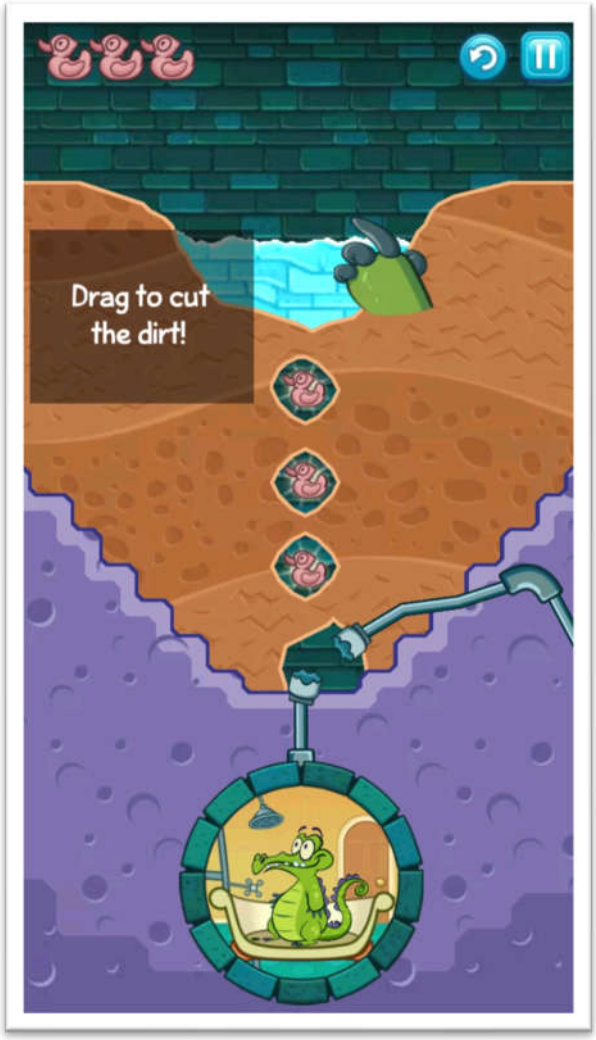
122. For example, the Apps include these representations while marketing and designing the apps expressly for children, and whose subject matter, design, and distribution mechanisms all suggest that the apps are appropriate for children.

1. Princess Palace Pets

123. Princess Palace Pets is a game in which players are tasked with taking care of the pets of various Disney princesses. Per the game's description, children playing the game are encouraged to "[e]nter the enchanted world of the Disney Princess Palace Pets. Meet Pumpkin, Teacup, Blondie, Treasure, Berry, Beauty, Lily, Summer, Sultan, and Petit! These adorable pets are all different, but each one loves to be cared for and can't wait to go on new adventures with you. Learn how the pets met the princesses, find out their unique talents, and treat them to a delightful day at the Royal Pet Salon!" Below is a screenshot from the game:

2. Where's My Water?

124. Where's My Water? is a puzzle game in which players must help a cartoon alligator named "Swampy" to re-direct a subterranean water flow in order to let Swampy take a shower. Per the app's description, players are encouraged to "[h]elp Swampy by guiding water to his broken shower. Each level is a challenging physics-based puzzle with amazing life-like mechanics. Cut through dirt to guide fresh water, dirty water, toxic water, steam, and ooze through increasingly challenging scenarios! Every drop counts!" Below is a screenshot from the game:



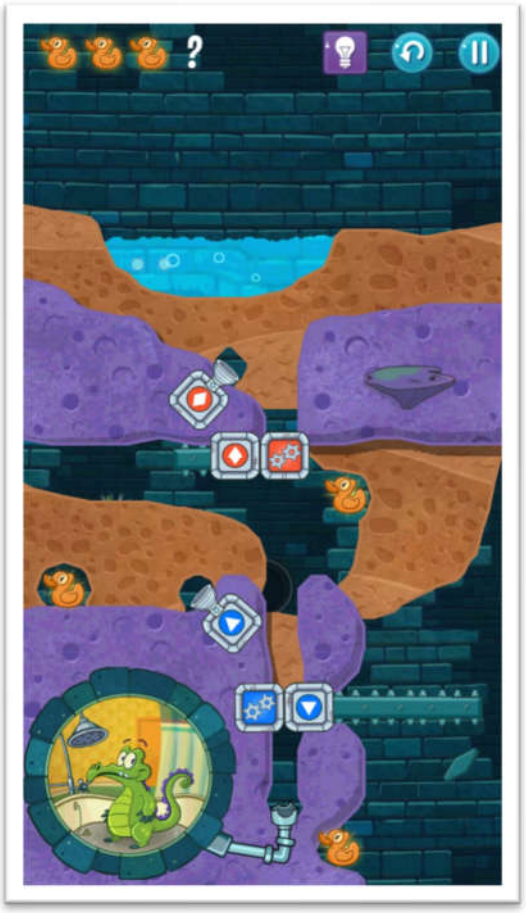
3. Where's My Water? Free/Lite

125. Where's My Water? Free and Where's My Water? Lite are, respectively, the Android and Apple free versions of Where's My Water?. The descriptions of the game and the general game play are identical in all material respects.

4. Where's My Water? 2

126. Where's My Water? 2 is the sequel to Where's My Water? and, as one might expect, involves directing water to Swampy the alligator so that he may take a shower. Per Disney, "[t]he sequel to the most addicting physics-based puzzler from Disney has finally arrived. Where's My Water? 2 launches with three brand new locations including the Sewer, the

Soap Factory, the Beach. Best of all, the puzzles are all free! Cut through dirt, and guide fresh water, purple water, and steam to help Swampy and his friends!"[97] Below is a screenshot from the game:



127. In the Apple App Store and Google Play Store, Princess Palace Pets and each of the Where's My Water? Apps are or were[98] rated as being appropriate for children. In marketing Princess Palace Pets and the Where's My Water? Apps as being suitable for children, Disney implicitly and explicitly purports to acknowledge and adhere to privacy-protective norms.

[97] https://play.google.com/store/apps/details?id=com.disney.wheresmywater2_goo (last accessed August 6, 2021).

[98] Several Disney Apps are now deprecated and are therefore no longer available on app stores (although they are still functional apps and are played by millions of children).

128. For example, Princess Palace Pets, Where's My Water? and Where's My Water? Free are or were featured in the "Family" section of the Google Play Store, which Google describes as "a rich platform for developers to showcase their high-quality, age appropriate content for the whole family."[99]

129. In order to be featured in the Family section of Google Play, Google requires that the app (here, Princess Palace Pets and the Where's My Water? Apps) be a part of the "Designed for Families" program,[100] which comes with specific requirements.

130. In order to be included in the Family section of Google Play (and therefore for developers to enroll in the Designed for Families program), developers have to expressly warrant, *inter alia*, that their apps meet specific criteria related to privacy laws (set by Google). This includes a requirement that all SDKs are compliant with COPPA (and its attendant prohibitions on collecting Personal Data from children without first obtaining verifiable parental consent).[101]

131. Apple's App Store Review Guidelines contain identical, privacy-protective requirements for developers, including Disney:

> 1.3 Kids Category
>
> The Kids Category is a great way for people to easily find apps that are appropriate for children. If you want to participate in the Kids Category, you should focus on creating a great experience specifically for younger users. These apps must not include links out of the app, purchasing opportunities, or other distractions to kids unless reserved for a designated area behind a parental gate. Keep in mind that once customers expect your app to follow the Kids Category requirements, it will need to continue to meet these

[99] https://support.google.com/googleplay/android-developer/topic/9877766 (last accessed August 6, 2021).
[100] *Id.*
[101] https://support.google.com/googleplay/android-developer/answer/9893335?hl=en&ref_topic=9877766#1&2&3&4&5&6&7&87&9 (last accessed August 6, 2021).

> guidelines in subsequent updates, even if you decide to deselect the category. Learn more about parental gates.
>
> Apps in the Kids Category may not include behavioral advertising (e.g. the advertiser may not serve ads based on the user's activity), and any contextual ads must be appropriate for young audiences. You should also pay particular attention to privacy laws around the world relating to the collection of data from children online. Be sure to review the Privacy section of these guidelines for more information.[102]

132. The document from Apple provides further clarification about data collection practices and privacy obligations for developers listing apps in the Kids section of the Apple App Store:

> 5.1.4 Kids
>
> For many reasons, it is critical to use care when dealing with personal data from kids, and we encourage you to carefully review all the requirements for complying with laws like the Children's Online Privacy Protection Act ("COPPA") and any international equivalents.
>
> Apps may ask for birthdate and parental contact information only for the purpose of complying with these statutes, but must include some useful functionality or entertainment value regardless of a person's age.
>
> Apps intended primarily for kids should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics and third-party advertising may be permitted provided that the services adhere to the same terms set forth in Guideline 1.3.
>
> Moreover, apps in the Kids Category or those that collect, transmit, or have the capability to share personal information (*e.g.* name, address, email, location, photos, videos, drawings, the ability to chat, other personal data, or persistent identifiers used in combination with any of the above) from a minor must include a privacy policy and must comply with all applicable children's privacy statutes. For the sake of clarity, the parental gate requirement for the Kid's Category is generally not the same as

[102] https://developer.apple.com/app-store/review/guidelines/#kids-category (last accessed August 6, 2021).

> securing parental consent to collect personal data under these privacy statutes.[103]

133. Thus, in marketing Princess Palace Pets and the Where's My Water? Apps and seeking the commercial advantage of the improved visibility to parents afforded by its family-oriented positioning in Google Play and the Apple App Store, Disney warrants that Princess Palace Pets and the Where's My Water? Apps are family-friendly, that the apps (and Disney, generally) act in accordance with all applicable privacy laws and regulations, and that any SDKs contained within Princess Palace Pets and the Where's My Water? Apps will comply with all applicable privacy laws and regulations.

134. Indeed, Disney specifically holds or held Princess Palace Pets and the Where's My Water? Apps out to its audience as being family-friendly, knowing that its audience reasonably expects such apps *not* to engage in privacy-violative behavior.

135. Moreover, Kochava, itself, is aware of Disney's representations (and comparable representations by other Child App developers) given that (1) it contracts with each of the developers of Child Apps (including Disney) and is aware of the nature, content, and functionality of the apps at issue and (2) it acquires and acts upon the Personal Data of the child users of the Child Apps, which it then *uses* to profile children individually. Therefore, Kochava has notice of the developer, the Child App, and the audience.

G. Kochava Violates Its Own Privacy Commitments

136. As alleged herein, Kochava fails to comply with its own privacy commitments. Kochava's online policy expressly disclaims its suitability for Child Apps, or makes statements about complying with privacy laws and norms that have been proven false by forensic analysis. This applies to Kochava's privacy policies in effect during all periods relevant to the litigation.

---

[103] *Id.*

H. Fraudulent Concealment and Tolling

137. The applicable statutes of limitations are tolled by virtue of Defendant's knowing and active concealment of the facts alleged above. Plaintiffs and Class Members were ignorant of the information essential to the pursuit of these claims, without any fault or lack of diligence on their own part.

138. At the time the action was filed, Defendant was under a duty to disclose the true character, quality, and nature of its activities to Plaintiffs and the classes. Defendant is therefore estopped from relying on any statute of limitations.

139. Defendant's fraudulent concealment is common to the classes.

I. Named Plaintiff Allegations

1. Plaintiff Amanda Rushing and Her Child, L.L.

140. In January 2014, Ms. Rushing or her child downloaded Disney Princess Palace Pets onto mobile devices in order for her child, L.L., to play the game. L.L. thereafter frequently played Princess Palace Pets on these devices on an ongoing and continuous basis.

141. During the time L.L. played Princess Palace Pets, Kochava partnered with Disney to collect the personal data of L.L. for the purposes of tracking and profiling her.

142. Prior to the forensic investigation conducted for this action, Ms. Rushing was not aware of the existence of Kochava, did not know that Disney had embedded the Kochava's code in the Princess Palace Pets app her child played, and did not know Kochava was exfiltrating her child's Personal Data as she played Princess Palace Pets to track and profile her.

143. Kochava's tracking and profiling of L.L. without parental consent is highly offensive to Ms. Rushing and constitutes an invasion of her child's privacy and of Ms. Rushing's right to protect her child from this invasion.

2. Plaintiff Ashley Supernault and Her Child, M.S.

144. In or around 2014, Ms. Supernault or her child downloaded the Disney Apps Where's My Water? Free and Where's My Water? 2 onto mobile devices in order for her child, M.S., to play the games. M.S. thereafter frequently played Where's My Water? Free and Where's My Water? 2 on these devices on an ongoing and continuous basis.

145. During the time M.S. played Where's My Water? Free and Where's My Water? 2, Kochava partnered with Disney to collect the Personal Data of M.S. for the purposes of tracking and profiling her.

146. Prior to the forensic investigation conducted for this action, Ms. Supernault was not aware of the existence of Kochava in the apps, did not know Disney had embedded Kochava's code in the Where's My Water? Free and Where's My Water? 2 apps her child played, and did not know Kochava was exfiltrating her child's Personal Data as she played Where's My Water? Free and Where's My Water? 2 to track and profile her.

147. Kochava's tracking and profiling of M.S. without parental consent is highly offensive to Ms. Supernault and constitutes an invasion of her child's privacy and of Ms. Supernault's right to protect her child from this invasion.

3. Plaintiff Julie Remold and Her Children, N.B. and C.B.

148. In or around July 2016, Ms. Remold or her children downloaded Disney's Where's My Water? app onto a mobile device in order for her children, N.B. and C.B., to play the game. N.B. and C.B. thereafter frequently played Where's My Water? on this device on an ongoing and continuous basis.

149. During the time N.B. and C.B. played Where's My Water?, Kochava partnered with Disney to collect the Personal Data of N.B. and C.B. for the purposes of tracking and profiling them.

150. Prior to the forensic investigation conducted for this action, Ms. Remold was not aware of the existence of Kochava in the app, did not know that Disney had embedded the Kochava's code in Where's My Water? app her children played, and did not know Kochava was exfiltrating her children's Personal Data as they played Where's My Water? to track and profile them.

151. Kochava's tracking and profiling of N.B. and C.B. without parental consent is highly offensive to Ms. Remold and constitutes an invasion of her children's privacy and of Ms. Remold's right to protect her children from this invasion.

4. Plaintiff Ted Poon and His Children, R.P. and K.P.

152. In or around December 2013 and November 2017, Mr. Poon or his children downloaded Disney's App "Where's My Water? Lite" onto mobile devices in order for his children, R.P. and K.P., to play the game. R.P. and K.P. thereafter frequently played Where's My Water? Lite on these devices on an ongoing and continuous basis.

153. During the time R.P. and K.P. played Where's My Water? Lite, Kochava partnered with Disney to collect the Personal Data of R.P. and K.P. for the purposes of tracking and profiling them.

154. Prior to the forensic investigation conducted for this action, Mr. Poon was not aware of the existence of Kochava in the app, did not know that Disney had embedded Kochava's code in the Where's My Water? Lite app his children played, and did not know Kochava was exfiltrating his children's personal data as they played Where's My Water? Lite to track and profile them.

155. Kochava's tracking and profiling of R.P. and K.P. without parental consent is highly offensive to Mr. Poon and constitutes an invasion of his children's privacy and of Mr. Poon's right to protect his children from this invasion.

V. CLASS ALLEGATIONS

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

157. Plaintiffs seek class certification of claims under Idaho law for the common law privacy cause of action "Intrusion Upon Seclusion," on behalf of a class defined as follows:

> **The Intrusion Upon Seclusion Class:** all parents and/or legal guardians of persons residing in the States of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia who are younger than the age of 18, or were younger than the age of 18 when they played a Child App containing the Kochava SDK, from whom Defendant collected, used, or disclosed Personal Data.

158. Plaintiff Amanda Rushing, on behalf of herself and as parent and guardian of her child, L.L., and Plaintiff Julie Remold, on behalf of herself and as parent and guardian of her children, N.B. and C.B., are the proposed Class Representatives for the Intrusion Upon Seclusion Class.

159. Plaintiffs seek class certification of a claim for violation of the State of California Constitution Right to Privacy and of the State of California Unfair Competition Law Cal. Bus. & Prof. Code §§ 17200, *et seq.*, on behalf of a subclass of the Intrusion Upon Seclusion Class defined as follows:

> **The California Subclass:** all parents and/or legal guardians of persons residing in the State of California who are younger than the age of 18, or were younger than the age of 18 when they played a Child App containing the Kochava SDK, from whom Defendant collected, used, or disclosed Personal Data.

160. Plaintiff Amanda Rushing, on behalf of herself and as parent and guardian of her child, L.L., is the proposed Class Representative for the California Constitutional Right to

Privacy claim. Plaintiff Julie Remold, on behalf of herself and as parent and guardian of her children, N.B. and C.B., is the proposed Class Representative for both the California Constitutional Right to Privacy claim and the California UCL claim.

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

> **The New York Class:** all parents and/or legal guardians of persons residing in the State of New York who are younger than the age of 18, or were younger than the age of 18 when they played a Child App containing the Kochava SDK, from whom Defendant collected, used, or disclosed Personal Data.

162. Plaintiff Ted Poon, on behalf of himself and as parent and guardian of his children, R.P. and K.P., is the proposed Class Representative for the New York Class.

163. Plaintiffs seek class certification of a claim for violation of the State of Massachusetts General Laws ch. 93A, *et seq.*, and Massachusetts General Laws ch. 214, § 1B on behalf of a class defined as follows:

> **The Massachusetts Class:** all parents and/or legal guardians of persons residing in the State of Massachusetts who are younger than the age of 18, or were younger than the age of 18 when they played a Child App containing the Kochava SDK, from whom Defendant collected, used, or disclosed Personal Data.

164. Plaintiff Ashley Supernault, on behalf of herself and as parent and guardian of her child, M.S., is the proposed Class Representative for the Massachusetts Class.

165. 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.

166. 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) Defendant, Defendant's predecessors, parents, successors, heirs, assigns, subsidiaries, and

any entity in which Defendant or its parents have a controlling interest, as well as Defendant's current or former employees, agents, officers, and directors; (c) persons who properly execute and file a timely request for exclusion from the Classes or Subclass; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) counsel for Plaintiffs and Defendant; and (f) the legal representatives, successors, and assigns of any such excluded persons.

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

168. **Numerosity (Rule 23(a)(1)).** The Classes and Subclass are so numerous that joinder of individual members herein is impracticable. The exact number of Class or Subclass Members, as herein identified and described, is not known, but download figures indicate that the Apps, alone, have been downloaded hundreds of millions of times or more.

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

i. Whether Kochava engaged in the activities referenced in paragraphs 41 to 53 via the Child Apps;

ii. Whether Kochava's acts and practices complained of herein amount to acts of intrusion upon seclusion under the law of Idaho;

iii. Whether Kochava's conduct violated Subclass Members' California constitutional Right to Privacy;

iv. Whether Kochava's acts and practices complained of herein violate California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*.;

v. Whether Kochava's acts and practices complained of herein violate New York General Business Law § 349;

vi. Whether Kochava's acts and practices complained of herein violate Massachusetts General Laws ch. 93A, *et seq*.;

vii. Whether Kochava's acts and practices complained of herein violate Massachusetts General Laws ch. 214, § 1B;

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

ix. What is the appropriate injunctive relief to ensure Kochava no longer illegally collects children's personal information to track and profile, them over time and across different websites or online services.

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

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

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

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

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

VI. CLAIMS FOR RELIEF

COUNT I
Intrusion Upon Seclusion
(Brought on Behalf of the Intrusion Upon Seclusion Class)

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

176. Idaho law on intrusion upon seclusion is applicable for all members of the Intrusion Upon Seclusion Class because there is no conflict of law between the law in Idaho and any of the states in which the Class Members reside. The jurisprudence in Idaho and each of the relevant states adheres to Restatement (Second) of Torts, § 652B with no material variation. Accordingly, because the law on intrusion upon seclusion in each of the states where the Class Members reside does not materially differ from the law of the forum state of Idaho, the law of Idaho applies for adjudication of all members of the Class.

177. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts, § 652B.

178. Plaintiff Amanda Rushing, and her child, L.L., and Plaintiff Julie Remold, and her children, N.B. and C.B., and Class Members have reasonable expectations of privacy in their mobile devices and their online behavior, generally. Plaintiffs' and Class Members' private affairs include their behavior on their mobile devices as well as any other behavior that may be monitored by the surreptitious tracking employed by Kochava through its embedded SDK.

179. The reasonableness of such expectations of privacy is supported by Kochava's unique position to monitor Plaintiffs' and Class Members' behavior through their access to Plaintiffs' and Class Members' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Kochava's tracking.

180. Kochava intentionally intruded on and into Plaintiffs' and Class Members' solitude, seclusion, or private affairs by intentionally designing its SDK to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiffs' and Class Members' activities through the monitoring technologies and activities described herein.

181. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Class Members' personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Kochava's conduct is that Kochava's principal goal was to surreptitiously monitor Plaintiffs and Class Members—in one of the most private spaces available to an individual in modern life—and to allow third parties to do the same.

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

183. Plaintiffs and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

184. Kochava's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class Members.

185. As a result of Kochava's actions, Plaintiffs and Class Members seek injunctive relief, in the form of Kochava's cessation of tracking practices in violation of state law, and destruction of all personal data obtained in violation of state law.

186. As a result of Kochava's actions, Plaintiffs and Class Members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class Members seek punitive damages because Kochava's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Kochava from engaging in future misconduct.

187. Plaintiffs seek restitution for the unjust enrichment obtained by Kochava as a result of unlawfully collecting Plaintiffs' and Class Members' children's personal data. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the legislation enacted by Congress, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying the online tracking of children. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Class Members' children's personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Kochava's conduct is the fact that Kochava's principal goal was to surreptitiously monitor Plaintiffs' and Class Members' children—in one of the most private spaces available to an individual in modern life—and to allow third parties to do the same.

COUNT II
California Constitutional Right to Privacy
(Brought on Behalf of the California Subclass of the Intrusion Upon Seclusion Class)

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

189. Plaintiff Amanda Rushing, and her child, L.L., and Plaintiff Julie Remold, and her children, N.B. and C.B., and Subclass Members have reasonable expectations of privacy in their mobile devices and their children's online behavior, generally. Plaintiff's and Subclass Members' children's private affairs include their behavior on their mobile devices, as well as any other behavior that may be monitored by the surreptitious tracking employed by Kochava.

190. The reasonableness of such expectations of privacy is supported by Kochava's unique position to monitor Plaintiff's and Subclass Members' children's behavior through its access to Plaintiff's and Subclass Members' children's private mobile devices. It is further supported by the surreptitious, highly technical, and non-intuitive nature of Kochava's tracking.

191. Kochava intentionally intruded on and into Plaintiff's and Subclass Members' and their children's solitude, seclusion, right of privacy, or private affairs by intentionally designing its SDK to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Subclass Members' children's activities through the monitoring technologies and activities described herein.

192. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential information about children, constituting an egregious breach of social norms. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Subclass Members' children's personal information with potentially countless third parties, known and unknown, for undisclosed and potentially

unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Kochava's conduct is that Kochava's principal goal was to surreptitiously monitor Plaintiff's and Subclass Members' children—in one of the most private spaces available to an individual in modern life—and to allow third parties to do the same.

193. Defendant's intrusion into the sacred relationship between parent and child and subsequent commercial exploitation of children's special vulnerabilities online also contributes to the highly offensive nature of Kochava's activities.

194. Plaintiff and Subclass Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

195. Kochava's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Subclass Members and their children.

196. As a result of Kochava's actions, Plaintiff and Subclass Members seek injunctive relief, in the form of Defendant's cessation of tracking practices in violation of state law, and destruction of all personal data obtained in violation of state law.

197. As a result of Kochava's actions, Plaintiff and Subclass Members seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class Members seek punitive damages because Kochava's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and made in conscious disregard of Plaintiff's rights and her child's rights. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

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

198. Plaintiff repeats and realleges all preceding paragraphs contained herein.

199. Plaintiff Ted Poon and his children, R.P. and K.P., and Class Members are "persons" within the meaning of New York General Business Law § 349(h).

200. Each Defendant is a "person," "firm," "corporation," or "association" within the meaning of N.Y. Gen. Bus. Law § 349.

201. Section 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce."

202. Kochava's conduct constitutes "deceptive acts or practices" within the meaning of N.Y. Gen. Bus. Law § 349. Kochava surreptitiously tracked children without disclosing its activities to their parents, in violation of applicable laws and reasonable expectations of privacy.

203. Kochava's conduct occurred in the conduct of trade or commerce, and was directed at consumers.

204. Kochava's conduct was misleading in a material way, because, *inter alia*, Kochava used the Child Apps as a vehicle for secretly and intentionally tracking and profiling child users, over time and across different online platforms, without providing notice or obtaining consent. As a result, parents are denied the opportunity to make informed decisions on whether to permit Kochava to exfiltrate their children's Personal Data and share it with third parties for commercial and other undisclosed purposes. Given the entirely surreptitious and intentional nature of the tracking technology at play, and Kochava's exclusive knowledge of it, Kochava had a duty to disclose the nature of their conduct. Kochava was also obligated to obtain parental consent before tracking and exfiltrating children's Personal Data. By failing to disclose its ability to track child users who play the Child Apps, Defendant purposely misled Plaintiff and Class Members.

205. As detailed above, unlike aggregated or anonymized data, the Personal Data collected and used by the Kochava is identifiable or associable with specific, individual child

users, is as persistent as a social security number, and can be used to track and profile children across multiple devices and over time.

206. As a result of Kochava's deceptive acts and practices, Plaintiff and Class Members were injured and damaged in that they suffered a loss of privacy and autonomy through Kochava's acquisition and use of children's personal information, for Kochava's own benefit, without Plaintiff's or the Class Members' knowledge or verifiable parental consent.

207. Because Kochava's willful and knowing conduct caused injury to Plaintiff and Class Members and their children, the Class seeks recovery of actual damages or $50, whichever is greater, discretionary treble damages up to $1,000, punitive damages, reasonable attorneys' fees and costs, an order enjoining Kochava's deceptive conduct, and any other just and proper relief available under N.Y. Gen. Bus. Law § 349. Plaintiff and Class Members seek punitive damages because Kochava's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and made in conscious disregard of Plaintiff's rights. Punitive damages are warranted to deter Kochava from engaging in future misconduct.

COUNT IV
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(Brought on Behalf of the California Subclass of the Intrusion Upon Seclusion Class)

208. Plaintiff and Class Members reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

209. Kochava's conduct as alleged herein constitutes unfair, unlawful, or fraudulent business acts or practices as proscribed by Section 17200, *et seq.*, of the California Business & Professions Code ("UCL").

210. Kochava's conduct is "fraudulent" under the UCL because it is likely to deceive the public, including the reasonable parent and child user. Kochava failed to disclose that it

collects and exfiltrates Personal Data for tracking and profiling purposes. Kochava knew or had reason to know that Plaintiff and Class Members could not have reasonably known or discovered the existence of the SDKs, without disclosure by Kochava. Kochava's conduct conveys to parents that it will abide by social norms and not collect the Personal Data of their children without express parental consent. Kochava fails to obtain parental consent and collects children's Personal Data anyway. Kochava prevented Plaintiff and Class Member parents and their children from avoiding Kochava's data practices and prevented parents from protecting their children's right to privacy.

211. Plaintiff reasonably relied on the omissions and misrepresentations of Kochava as alleged herein. Had Kochava disclosed to Plaintiff and Class Member parents that the Where's My Water? app employed tracking software, Plaintiff and Class Member parents, acting reasonably under the circumstances, would not have purchased the Where's My Water? app.

212. Kochava's conduct constitutes "unfair" business acts or practices. Plaintiffs and Class Members have an interest in controlling the disposition and dissemination of their children's Personal Data. Contrary to Plaintiff's and Class Members' interests, Kochava surreptitiously exfiltrated Plaintiff's and Class Members' children's Personal Data, exploiting it for sale and profit without consent. The loss of privacy and autonomy suffered by Plaintiff, Class Members, and their children outweighs the profit motive for Kochava's unauthorized and secretive collection and dissemination of children's Personal Data via the Where's My Water? app.

213. Kochava's conduct constitutes "unlawful" business acts or practices by virtue of its conduct constituting intrusion upon seclusion and violations of California's Constitutional Right of Privacy. In addition, Kochava's conduct violates the standards reflected in the

Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6502, which serves as an additional and independent basis for Defendant's violation of the "unlawful" prong of the UCL.

214. Plaintiff and Class Members have suffered injury in fact and lost money or property as a result of the Kochava's business acts and/or practices. But for Kochava's unfair, unlawful, or fraudulent business acts or practices, Plaintiff would not have purchased the Where's My Water? app.

215. Plaintiff and Class Members seek an order to enjoin Kochava from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs and Class Members their interest in money and/or property that might have been acquired by Kochava by means of unfair competition.

COUNT V
Violation of Massachusetts' Unfair and Deceptive Trade Practices Statute Massachusetts General Laws ch. 93A, et seq.
(Brought on Behalf of the Massachusetts Class)

216. Plaintiff and Class Members reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

217. Kochava's acts and practices complained of herein—including, but not limited to, contracting for the installation of SDKs in Disney's child-oriented Gaming Apps and secretly collecting and sharing Plaintiff's and Class Members' children's Personal Data without parental consent—amount to "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce," as proscribed by Massachusetts General Laws ch. 93A.

218. Plaintiff and Class Members, and their children, suffered actual injury—in the form their loss of privacy and autonomy—as a result of Defendant's acts, practices, and omissions described herein.

219. As a result of Defendant's violation of Massachusetts's Unfair and Deceptive Trade Practices Statute, Plaintiff and Class Members are entitled to—and accordingly seek—actual damages and attorneys' fees, pursuant to Massachusetts General Laws ch. 93A, § 9.

COUNT VI
Violation of Massachusetts' Statutory Right to Privacy Massachusetts General Laws ch. 214, § 1B
(Brought on Behalf of the Massachusetts Class)

220. Plaintiff incorporates by reference all the preceding allegations as if fully set forth herein.

221. Pursuant to Massachusetts General Laws ch. 214, § 1B, Massachusetts guarantees persons freedom from unreasonable, substantial, or serious interference with their privacy.

222. Kochava's acts and practices complained of herein have violated the law guaranteeing the privacy rights of Plaintiff and Class Member parents and their children.

VII. PRAYER FOR RELIEF

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

a. Certify this case as a class action, appoint Plaintiffs as Class and Subclass representatives, and appoint Plaintiffs' counsel to represent the Classes and Subclass;

b. Find that Kochava's actions, as described herein, constitute: (i) violations of New York General Business Law § 349, (ii) breaches of the common law claim of intrusion upon seclusion under the law of the State of Idaho and 34 others as to the Intrusion Upon Seclusion Class; (3) violations of the right to privacy under California Constitution, Article I, Section 1; (4) violations of California's UCL, Cal. Bus. & Prof. Code §§ 17200, *et seq.*; (5)

violations of Massachusetts General Laws ch. 93A, *et seq.*; and (6) violations of Massachusetts General Laws ch. 214, § 1B.

c. Award Plaintiffs and Class and Subclass Members appropriate relief, including actual and statutory damages and punitive damages, in an amount to be determined at trial;

d. Award restitution to Plaintiffs and Class and Subclass Members for Defendants' unjust enrichment;

e. Award equitable, injunctive, and declaratory relief as may be appropriate;

f. Award all costs, including experts' fees, attorneys' fees, and the costs of prosecuting this action; and

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

Dated: August 9, 2021

Respectfully Submitted,

PARSONS BEHLE & LATIMER

By */s/ Brook B. Bond*
Brook B. Bond

Brook B. Bond
BBond@parsonsbehle.com
PARSONS BEHLE & LATIMER
800 West Main Street, Suite 1300
Boise, ID 83702
Telephone: 208.562.4900
Facsimile: 208.562.4901

Douglas I. Cuthbertson
dcuthbertson@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
hbates@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 Classes

DEMAND FOR JURY TRIAL

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

Dated: August 9, 2021

Respectfully Submitted,

PARSONS BEHLE & LATIMER

By */s/ Brook B. Bond*
Brook B. Bond

Brook B. Bond
BBond@parsonsbehle.com
PARSONS BEHLE & LATIMER
800 West Main Street, Suite 1300
Boise, ID 83702
Telephone: 208.562.4900
Facsimile: 208.562.4901

Douglas I. Cuthbertson
dcuthbertson@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
hbates@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 Classes