LAW OFFICES OF RONALD A. MARRON
RONALD A. MARRON (SBN 175650)
ron@consumersadvocates.com
MICHAEL T. HOUCHIN (SBN 305541)
mike@consumersadvocates.com
LILACH HALPERIN (SBN 323202)
lilach@consumersadvocates.com
651 Arroyo Drive
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665
Attorneys for Plaintiff and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES

RONA KOMINS, on behalf of herself, her children, B.K. and M.K, and all others similarly situated,

Plaintiff,

v.

DAVE YONAMINE, JOHN LIBBY, MOBILITYWARE, LLC; DOES 1-100, inclusive, and ROES Software Development Kit Business Entities 1-100, inclusive,

Defendants.

Case No.: 19STCV24865

THIRD AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Rona Komins, on behalf of herself and her children, B.K., and M.K., and all others similarly situated ("Plaintiff"), by and through her undersigned counsel, hereby sues Defendants Dave Yonamine, John Libby, and MobilityWare, LLC. ("MobilityWare"), DOES 1-100, and ROES 1-100, hereafter collectively named as "Defendants," and, upon information and belief and investigation of counsel, allege as follows:

I. INTRODUCTION

1. This is an action brought by a parent to protect the privacy of her children, whom, while playing games via gaming apps on mobile devices, have had their personal identifying information tracked, collected, and shared by MobilityWare and its partners for targeted advertising and other commercial exploitation, in direct violation of California state laws. Plaintiff seeks an injunction to stop Defendants' unlawful practices and sequester their unlawfully obtained information, and an award of reasonable damages.

II. JURISDICTION AND VENUE

2. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(d)(4)(A), the local controversy exception to federal jurisdiction under the Class Action Fairness Act of 2005 (CAFA) because greater than two-thirds of all members in the proposed Class are citizens of California; the Defendants are citizens of California and Defendants' conduct forms a significant basis for the claims asserted by the Class; the principal injuries resulting from Defendants' conduct were incurred in California; and during the three-year period preceding the filing of this action, no other class action has been filed asserting the same or similar factual allegations against the Defendants on behalf of the same person. Additionally, the number of members of the proposed Class in the aggregate is more than 100 and the Defendants are not a State, State official, or other governmental entity against whom the Court may be foreclosed from ordering relief.

3. This Court has both general and specific personal jurisdiction over the Defendants.

4. The Court has personal jurisdiction over Defendants because Defendants Dave Yonamine and John Libby reside in California and Defendant MobilityWare has its principal place of business in California, Defendants transact business in California, have substantial aggregate contacts with California, engaged and are engaging in conduct that has and had a direct, substantial,

reasonably foreseeable, and intended effect of causing injury to persons throughout California, and purposely availed themselves of the laws of California, rendering the exercise of jurisdiction by the Court permissible under traditional notions of fair play and substantial justice.

5. Venue is proper in this Court pursuant to California Code of Civil Procedure §§ 395 and 395.5 because a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, Defendants transact business in this District, and Defendants reside in this District. Defendants' business practices and wrongful acts have occurred and continue to occur in this county, and the adverse effects of Defendants' alleged wrongful conduct have harmed and will continue to harm the residents of this county and the rest of the state.

III. PARTIES

Plaintiff

6. Plaintiff Rona Komins ("Plaintiff") is the parent of children "B.K." and "M.K." who played the online gaming applications or apps ("apps") operated by the Defendants.

7. Plaintiff and her children are residents and citizens of Los Angeles, California. Ms. Komins brings this action on behalf of herself, B.K., M.K., and all others similarly situated.

8. B.K. was under the age of 13 while using the MobilityWare gaming apps FreeCell Solitaire, and Solitaire**.** M.K. was under the age of 18 while using the MobilityWare gaming apps FreeCell Solitaire and Solitaire.

Defendants

9. Defendant, MobilityWare, LLC is a California limited liability company headquartered at 440 Exchange, Ste. 100, Irvine, California 92602. Defendant MobilityWare, LLC is registered to do business in California as entity number 201800810207.

10. MobilityWare generates revenue primarily from, among other things, in-game purchases, and advertising through online video content. MobilityWare developed and marketed the online gaming apps used by Plaintiff, including Solitaire and FreeCell, and apps used by millions of people in the United States.

11. Defendant Dave Yonamine, an individual, is, or was during the applicable period of this lawsuit, the Chief Executive Officer, and also an Agent for Service of Process of

MobilityWare, LLC and is located at 440 Exchange, Ste. 100, Irvine, CA 92602. Dave Yonamine is the co-founder and Chairman of the Board of MobilityWare, LLC. Upon information and belief, Defendant Dave Yonamine, during all times relevant to Plaintiff's claims, specifically, individually, and personally directed and authorized all of the unlawful data collection described herein, and was intimately involved in the software programing that unlawfully collects user data. Upon information and belief, Defendant Yonamine was the guiding spirit and central figure behind the unlawful data collection described herein.

12. Defendant, John Libby, an individual, is, or was during the applicable period of this lawsuit, the Secretary, Chief Financial Officer, and an Agent for Service of Process in California for MobilityWare, LLC and is located at 440 Exchange, Ste.100, Irvine, CA 92602. Upon information and belief, Defendant John Libby, during all times relevant to Plaintiff's claims, specifically, individually, and personally directed and authorized all of the unlawful data collection described herein, and was intimately involved in the software programing that unlawfully collects user data. Upon information and belief, Defendant Libby was the guiding spirit and central figure behind the unlawful data collection described herein.

SDK Defendants

13. The "SDK Defendants" are entities which provided their own proprietary computer code to MobilityWare, known as Software Development Kits ("SDKs"), for installation and use in MobilityWare's gaming apps, including Solitaire and FreeCell, causing the transmittal of app users' Personal Data to the SDK Defendants to facilitate subsequent tracking and targeted advertising. "Personal Data" as used herein is any data that refers to, is related to, or is associated with an identified or identifiable individual.

14. The true names and capacities of the defendants named herein under California Code of Civil Procedure § 474 as "ROE Software Development Kit Business Entities 1 through 100" are presently unknown to Plaintiff, who therefore sues them by fictitious names. Plaintiff will amend this Complaint to allege the true names and capacities of these defendants when they have been determined. Each of the fictitiously named defendants is responsible in some manner for the conduct alleged herein. The ROE defendants are private individuals, associations,

partnerships, corporations, or institutes who participated in the wrongful conduct alleged herein in ways which are unknown to Plaintiff at this time.

15. At all relevant times, MobilityWare purposefully installed and implemented the SDK Defendants' tracking software kits into its mobile gaming apps, the SDK Defendants were agents of MobilityWare, and MobilityWare is vicariously liable for the acts of the SDK Defendants as alleged herein.

IV. FACTUAL ALLEGATIONS

16. MobilityWare is a mobile gaming app developer and publisher that offers a host of mobile gaming apps, including, but not limited to: Solitaire, Tripeaks Solitaire, Pyramid Solitaire, FreeCell Solitaire, Crown Solitaire, Spider Solitaire, Spider Go Solitaire, Castle Solitaire, Addiction Solitaire, Mahjong Solitaire, Yukon Russian Solitaire Game, Aces Up Solitaire, Destination Solitaire, Hearts Card Game, Puzzle Cats, Sudoku Simple, Spades Card Game, Tropical Treats, Word Wiz, Word Warp, Sunny Shapes, Word Search, Tetra Block – Puzzle Game, and Dice Merge Puzzle Master (collectively, "Gaming Apps").[1]

17. The Gaming Apps are available for download in online stores, including Google's "Play Store" and Apple's "App Store."

18. Collectively, the Gaming Apps have been downloaded over 400 million times.[2]

19. As one of the most popular and ubiquitous gaming apps, MobilityWare's Solitaire gaming app has been downloaded more than 100 million times. Tripeaks Solitaire has been downloaded more than 1 million times; Pyramid Solitaire has been downloaded more than 1 million times; FreeCell Solitaire has been downloaded more than 10 million times; Crown Solitaire has been downloaded more than 1 million times; Spider Solitaire has been downloaded more than 10 million times; Spider Go Solitaire has been downloaded more than 100 thousand times; Castle Solitaire has been downloaded more than 500 thousand times; Addiction Solitaire has been downloaded more than 500 thousand times; Mahjong Solitaire has been downloaded more than

[1] https://www.mobilityware.com/games

[2] https://www.mobilityware.com/ourstory

500 thousand times; Yukon Russian Solitaire Game has been downloaded more than 100 thousand times; Aces Up Solitaire has been downloaded more than 50 thousand times; Destination Solitaire has been downloaded more than 33 thousand times; Hearts Card Game has been downloaded more than 100 thousand times; Puzzle Cats has been downloaded more than 10 thousand times; Sudoku Simple has been downloaded more than 50 thousand times; Spades Card Game has been downloaded more than 100 thousand times; Tropical Treats has been downloaded more than 100 thousand times; Word Wiz has been downloaded more than 100 thousand times; Word Warp has been downloaded more than 6 thousand times; Sunny Shapes has been downloaded more than 46 times; Word Search has been downloaded more than 50 thousand times; Tetra Block – Puzzle Game has been downloaded more than 10 thousand times; and Dice Merge Puzzle Master has been downloaded more than 10 thousand times. *See* **Exhibit 1**.

20. MobilityWare styles and promotes the Gaming Apps as fun, free, kid-friendly games, and markets the games to a family audience that includes children. Each of the Gaming Apps in Google's Play Store are rated as E for "Everyone." *See* **Exhibit 1**. The Google Play Store describes the "Everyone" rating as, "Content is generally suitable for all ages. May contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language."[3]

21. In Apple's App Store, the Gaming Apps are rated "Age 4+". *See* **Exhibit 1**. 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] A 4+ rating indicates that the Gaming Apps are suitable for users ages 4 and older.

A. Mobile Online Gaming Apps are Programmed to Enable the Collection of Personal Data.

22. According to the Pew Research Center in April of 2019, there are only 10% of adult

[3]https://support.google.com/googleplay/answer/6209544?p=appgame_ratings&visit_id=636966522887185954-2966504457&rd=1 (last accessed October 8, 2020).

[4] https://developer.apple.com/app-store/review/guidelines/ (last accessed October 8, 2020).

Americans that do not use the internet.[5] Since the inception of online gaming, consumers have increasingly been using their mobile devices to play their favorite online games, many of which are aimed at children.

23. Most adult consumers, including those that are parents of children consumers, are unaware that the apps are specifically engineered to surreptitiously and unlawfully collect the adult, and child-users' personal information from their mobile device, and then "share" that information for profit to advertisers.

24. App developers contract with third-parties for the right to embed third-party computer code into the developers' apps, for various purposes.

25. Advertising-specific SDKs (Software Development Kits) are blocks of computer code which operate to secretly collect an app user's personal information and track online behavior to facilitate behavioral advertising or marketing analysis.

26. In the case of an advertising SDK, the creator of the SDK will embed its SDK code into the underlying code of the app itself, collect personal information to serve behavioral advertisements, and then pay the app developer based on the number of ads shown.

27. This practice is a substantial source of many app developers' revenue, enabling app developers to allow users to download the apps without charging a purchase price. This is a common practice as demonstrated in 2020 with 96.1% of Android apps on the Google Play Store being free to download.[6]

B. <u>MobilityWare and the SDK Defendants Track Children's Online Behavior and Collect Children's Personal Data As They Play MobilityWare's Gaming Apps</u>

28. Unbeknownst to parents and their children, as users play one of MobilityWare's Gaming Apps, MobilityWare in partnership with the SDK Defendants collect Personal Data and

---

[5] "10% of Americans don't use the internet. Who are they?" Pew Research Center (Apr. 22, 2019), *available at* https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/ (accessed Oct. 15, 2020).

[6] "Android and Google Play Statistics," AppBrain (October 15, 2020), *available at* https://www.appbrain.com/stats/free-and-paid-android-applications (accessed Oct. 15, 2020).

track online behavior to profile users for targeted advertising.

29. As soon as a user downloads and opens up one of the Gaming Apps on his or her mobile device, MobilityWare immediately begins to collect Personal Information, defined in its Privacy Policy as "information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device." *See* **Exhibit 2** (Privacy Policy). MobilityWare also collects users' Personal Data, defined as "any information that enables us to identify you, directly or indirectly, by reference to an identifier such as your name, identification number, location data, online identifier or one or more factors specific to you." *Id*.

30. Targeted advertising is driven by users' Personal Data and employs sophisticated algorithms that interpret the Personal Data to determine the most effective advertising for individual users.

31. When children engage in online activity, such as playing a game, their every action on the device they are using is linked to a unique and persistent identifier that constructs a profile of the child on that mobile device. These identifying numbers are unique to each device and put in place by app developers so that their SDK partners can collect the users' personal information and build an immense online profile across all the devices they use. Their app usage, geographic location (including likely domicile), and internet navigation all help to build a personal profile that can then be exploited in a commercial context for profit.

32. The process in which this occurs will typically follow this sequence of events: an app developer installs an SDK in an app, which collects persistent identifiers, permitting the SDK entity to sell the child's persistent identifier to an advertising network or third-party data aggregator (who then further resells the data to additional partners). An "Ad Network" will store the persistent identifiers on its servers. Later, other app or SDK developers sell that same child's persistent identifier to the Ad Network, bolstering the Ad Network's profile of the child, increasing the value of the child's data and, relatedly, the ability to serve a more highly-targeted ad to a specific device. Multiple Ad Networks or other third-parties can then buy and sell data, exchanging databases amongst themselves, creating an increasingly sophisticated and merchantable 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.

33. In sum, children's personal information is collected by MobilityWare and its SDK partners, which is then sold to third parties who track and use the collected information and analyze it with sophisticated algorithms to create a user profile of the child. This profile is then used to serve behavioral advertising to children whose profile fits a set of demographic and behavioral traits.

i. What Are Persistent Identifiers

34. MobilityWare and its SDK partners track children's behavior while they play online games with their mobile devices by obtaining critical pieces of data from the mobile devices, including "persistent identifiers." These identifiers are a set of unique data points (typically numbers and letters), akin to a social security number, that 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 devices (*e.g.* smart phones, tablets, laptops, desktops and smart TVs).

35. The common persistent identifiers for Apple 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.

36. The common persistent identifiers in the Android operating system 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.

37. Additional persistent identifiers include data about a specific device, including details about its hardware—such as the device's brand (e.g., Apple or Android), 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, such as 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 provide a level of detail about the given device that allows that device and its user to be identified individually, uniquely, and persistently.

38. Defendants track, collect, and analyze these persistent identifiers in order to learn more about users, including their behaviors, demographics, and preferences, and, thereafter, to serve them with tailored and targeted advertising. Defendants also use persistent identifiers to track the effectiveness of those advertisements after the user sees them (to determine, for example, whether the user downloaded the app or bought the product advertised).

39. Defendants then store and analyze 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, Defendants (and other entities in the ad network) can generally monitor, profile, track a user over time, across devices, and across the Internet.

40. The Center for Digital Democracy, and the FTC described how and why a persistent identifier alone facilitates behavioral advertising:

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

See Comments of The Center for Digital Democracy, et al., FTC, In the Matter of Children's Online Privacy Protection Rule at 13-14 (Dec. 23, 2011).[7]

ii. MobilityWare Collects Persistent Identifiers and More

[7] *See also* Jessica Rich, Director, FTC Bureau of Consumer Protection, Keeping Up with the Online Advertising Industry (Apr. 21, 2016), available at https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry (accessed Oct. 15, 2020).

41. As soon as a user opens up one of MobilityWare's Gaming Apps, MobilityWare collects users' first and last names, usernames, unique personal identifiers, online identifiers, Internet Protocol addresses, email addresses, or other similar identifiers. *See* **Exhibit 2** (Privacy Policy).

42. MobilityWare also collects Gaming App users' geo-location,[8] passwords, and other specific identifying information. *Id*.

43. As soon as a user plays one of the Gaming Apps, MobilityWare automatically collects the following categories of information:

i. **Specific device information**, including a user's hardware model, operating system and version, unique device identifiers, device software platform and firmware, data about usage of the Gaming Apps, geographical data and mobile network information, and other data.

ii. **Information about a user's use of the Gaming Apps**, including the type of browser used, access times, pages viewed, game play activity, interactions with other players, user's IP address and the page a user visited before navigating to the Gaming Apps.

iii. **Information collected by cookies, web beacons, and other tracking technologies**, including the pages users view, users' movements around the Gaming Apps, the links users click and other actions users take on the Gaming Apps to understand usage and ad campaign effectiveness.

iv. **Protected classification characteristics** under California or federal law, including age and sex (including gender).

v. **Professional or employment-related information**, including current or past job history or performance evaluations.

---

[8] As the Supreme Court recently recognized in *Carpenter v. United States,* 138 S. Ct. 2206 (2018), location data is highly sensitive, not just because of what the data point alone says about an individual (*i.e.,* where they were at a particular time), but also because of the massive amount of personal information that can be extracted from location data (such as medical treatment, personal relationships, and private interests).

vi. **Commercial information**, including products or services purchased or considered in the past and other purchasing and consuming histories or tendencies.

vii. **Internet or other similar network activity**, including browsing history, search history, and information on a consumer's interaction with a website, application, or advertisement.

viii. **Geo-location data**, including physical location and movements.

ix. **Information regarding a user's preferences**, characteristics, psychological trends, predispositions, and behavior.

x. **Equipment information**, including information about a user's internet connection, the equipment used to access the Gaming Apps, and usage details. *Id*.

44. MobilityWare also uses mobile analytics software to record information such as how often users use the Gaming Apps, the events that occur within the Gaming Apps, performance data, and where the Gaming App was downloaded from (*e.g*. Apple Store, Google Play Store). *Id*.

45. MobilityWare then matches and combines this information automatically collected from users' devices with personal information obtained from users or other sources, including third parties from whom MobilityWare purchases data. *Id*.

46. For example, MobilityWare receives reports from its partners, such as Google Analytics that provide it with this collected information on an individual basis. *Id*.

47. MobilityWare also collects information, such as users' IP addresses from social networking sites like Facebook, Twitter or LinkedIn.

48. MobilityWare processes, uses, combines, discloses, and retains such information to manage and deliver contextual and behavioral advertising to users of the Gaming Apps. *Id*.

49. In sum, MobilityWare collect a host of other items of Personal Data to comingle those into expansive data profiles, which it then sells to third party SDKs.

iii. MobilityWare Discloses and Sells Gaming App Users' Personal Information to Third Parties

50. With this combined Personal Data, MobilityWare tracks, profiles, and targets users for advertising purposes, and sells this combined information to third-party SDKs who do the same.

51. Defendant MobilityWare has contracted with at least thirty-eight (38) SDKs for advertising purposes during the proposed Class Period. *See* **Exhibit 3** (Cookie Policy).

52. A user's personal information is transferred to, stored, and processed throughout the United States and to MobilityWare's affiliates, partners, and service providers located around the world.

53. With these SDKs, MobilityWare collects and shares the following data:

i. Performance Data

ii. IP address, IDFAs, and hashed Android ID;

iii. User's social network ID; and/or

iv. Other contextual data about a user's game play. *See* **Exhibit 2**.

54. The information collected is used to measure the effectiveness of the ads, offer targeting advertising, and undertake web analytics (like Google analytics). *Id*. Defendants collect this information through the use of tracking technologies and share this information with their customers and clients.

55. Defendants use such personal information to personalize the Gaming Apps to deliver content and product and service offerings relevant to a user's interests, including targeted offers and ads.

56. Within the past year, MobilityWare has disclosed and/or sold the following categories of personal information to third party SDKs:

i. User Names (*e.g.* a real name, alias, etc.), unique personal identifier, online identifier, Internet Protocol address, email address, or other similar identifiers;

ii. Protected classification characteristics under California or federal law, including age and sex,

iii. Commercial information, including products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

iv. Internet and other similar network activity, including browsing history,

search history, information on a user's interaction with the Gaming Apps or advertisements;

v. Inferences drawn from other personal information, including profile reflecting a person's preferences, characteristics, psychological trends, predispositions, and behavior, and;

vi. Equipment information, including information about a user's internet connection, the equipment used to access the Gaming Apps, and usage details.[9]

57. 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 violate users' privacy.

C. <u>The Privacy-Invasive and Manipulative Commercial Purposes Behind Defendants' Data Exfiltration, and its Effect on Child Users.</u>

i. The Role of Persistent Identifiers in User Profiling and Targeted Advertising

58. MobilityWare and the SDK Defendants, in coordination, collect and use the Personal Data described above to track, profile, and target children with targeted advertising.

59. 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 in a commercial context.

60. Defendants aggregate this data, and also buy it from and sell 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

[9] MobilityWare Privacy Policy (Apr. 24, 2020), *available at* https://www.mobilityware.com/privacy (accessed Oct. 26, 2020).

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.

61. Similarly, a critical (and thus, fiercely desired) component of user profiles is an individual's geolocation, which the FTC describes as a "key data point" for advertisers.[10]

62. The Federal Trade Commission (the "FTC") provides an illustration of these precise data points 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*.[11]

63. The FTC expressed particular "[c]oncerns about creations of detailed profiles based on device IDs [such as those created and facilitated by Defendants]…where…companies (like ad

---

[10] *Track or Treat? InMobi's location tracking ignored consumers' privacy settings*, Federal Trade Commission, (June 22, 2016) (*available* https://www.ftc.gov/news-events/blogs/business-blog/2016/06/track-or-treat-inmobis-location-tracking-ignored-consumers (accessed on Oct. 15, 2020).

[11] *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, Federal Trade Commission, FTC Staff Report (Dec. 2012), at 10 n. 25 (emphasis added) (citing David Norris, Cracking the Cookie Conundrum with Device ID, AdMonsters (Feb. 14, 2012) (*available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf (accessed on Oct. 15, 2020) ("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.").

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."[12]

64. Defendants traffic in the same data identified by the FTC (persistent identifiers such as IDFA/Android ID and device-specific data) causing the same harm identified by the FTC: allowing ad networks to combine data points about child users from a multitude of apps.

65. 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, Defendants and their 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.[13]

66. 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, any meaningful distinctions between personal and so-called nonpersonal 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

---

[12] *Id*. at 9.

[13] *Id.* 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/ (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) (accessed on Oct. 15, 2020).

identify, target and contact that particular user.[14]

67. 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.[15]

68. 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), MobilityWare 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.

69. 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

---

[14] 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).

[15] 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, available at https://www.hsgac.senate.gov/media/permanent-subcommittee-on-investigations-releases-report-online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy- (accessed Oct. 15, 2020).

(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.

70. Permitting technology companies to obtain children's persistent identifiers exposes those children to targeted advertising. The ad networks, informed by the surreptitious collection of Personal Data from children, will assist in the sale of advertising placed within the gaming apps and targeted specifically to children.

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

D. Defendants Use Children's Personal Data to Target and Profile Them, Despite Children's Heightened Vulnerability to Advertising

72. Defendants use children's Personal Data to serve them targeted advertising and for other privacy-invasive commercial purposes. Defendants engage in this behavior despite the known risks associated with and ethical norms surrounding advertising to children.[16]

73. Advertisers regard children as valuable advertising targets.[17] Children influence the

---

[16] 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."), *available at* https://www.tandfonline.com/doi/abs/10.1080/13527266.2017.1409250?scroll=top&needAccess=true&journalCode=rjmc20 (accessed Oct. 15, 2020).

[17] 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 Oct. 15, 2020).

buying patterns of their families—an influence that amounts to billions of dollars each year—and have lucrative spending power themselves.[18] Children and teens are thus prime targets for advertisers.

74. MobilityWare intentionally profits from embedding SDKs, to collect and exploit children's Personal Data, into its "free-to-play" Gaming Apps.

75. Defendants target advertising efforts at children despite widespread awareness that children are more vulnerable to deception by advertisers because they are easily influenced by its content, lack the cognitive skills to understand the intention of advertisers, and can struggle to distinguish between advertisements and other content.[19] This is particularly problematic when targeted advertising is used which, by design, more effectively sways target audiences.[20]

76. Research supports that online advertisements pose heightened risks to children.[21]

77. Exposure to advertising can also lead to negative outcomes for children, including increasing conflict with their parents, cynicism, health issues, and increased materialism.[22]

78. Children often lack the skills and knowledge necessary to assess and appreciate the risks associated with online data exfiltration and tracking.[23] Even attempts to disclose privacy-

---

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

[19] 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) (collecting studies); *Children as Consumers: Advertising and Marketing*, *supra*; *Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors, supra*, (collecting studies).

[20] 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).

[21] *Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues*, *supra* (collecting studies); *Children as Consumers: Advertising and Marketing*, *supra; Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors, supra* (collecting studies).

[22] *Children as Consumers: Advertising and Marketing*, *supra*.

[23] 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).

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.[24] 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." *Id*. at 10.

E. Defendants Exfiltrate and Analyze Children's Personal Data to Track the Effect of Their Ads on Children's Behavior.

79. Defendants exfiltrate and analyze users' Personal Data before and after serving advertisements. On the front end, the data helps them know what ads to serve (based on users' demographics and behaviors). On the back end, the data helps them determine whether the ad is successful in affecting children's behavior. This is called ad attribution.

80. Defendants track the impact and value of ads by tracking users' activities across the Internet after they interact with those ads.

81. Defendants exfiltrate Plaintiff's and Class Members' children's Personal Data from their devices in order to target them for advertising based on their behavior, demographics, and location. Defendants continue to track Plaintiff's and Class Members' 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 ads. This ongoing exfiltration, tracking, and analysis violate Plaintiff's and Class Members' children's privacy and exploit the vulnerabilities of their children.

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

82. Invasion of privacy has been recognized as a common law tort for over a century. *Matera v. Google Inc*., 15-CV-0402, 2016 WL 5339806, at *10 (N.D. Cal, Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A-I for the proposition "that the right to privacy was first

[24] *Internet Research in Online Environments for Children*, *supra*.

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'"). *Id*. 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 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).

83. 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).

84. 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).

85. 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.

86. California amended its constitution in 1972 to specifically enumerate a right to privacy in its very first section. *See* Cal. Const. Art. I, § 1.

i. Defendants' Surreptitious and Deceptive Collection of Personal Data Violates Children's Reasonable Expectations of Privacy and is Highly Offensive.

87. A reasonable person believes the Defendants' conduct, described above, violates Plaintiff's and her children's, and Class Members' and their children's expectations of privacy.

88. 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.[25]

a. 75% of the parents who were polled strongly disagreed with the statement: "It is okay for advertisers to track and keep a record of a child's behavior online if they give the child free content."

b. 69% of the parents who were polled strongly disagreed with the statement: "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."

c. 84% of the parents who were polled strongly disagreed with the statement: "It is okay for advertisers to collect information about a child's location from that child's mobile phone."

d. 89% of the parents who were polled strongly agreed with the statement: "Before advertisers put tracking software on a child's computer, advertisers should receive the parent's permission." *Id*.

89. In a 2013 primer designed for parents and kids to understand their privacy rights

[25] 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 (accessed on October 14, 2020).

online, the CDD noted similar findings.[26]

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 "OK for a website to ask children for personal information about their friends."

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.

90. 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."[27]

91. 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% of adults claim to clear their cookies and browser histories in an attempt to be less visible online.

92. Smartphone owners are particularly 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.[28] Such behaviors exemplify people's expectation that their personal information—

---

[26] *See* Center for Digital Democracy, The New Children's Online Privacy Rules: *What Parents Need to Know*, (June 2013), available at https://www.democraticmedia.org/sites/default/files/CDDCOPPAParentguideJune2013.pdf (accessed October 15, 2020).

[27] Lee Rainie, et al., *Anonymity, Privacy, and Security Online*, Pew Research Center 7 (Sept. 5, 2013), available at https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/ (accessed October 15, 2020).

[28] Jan Lauren Boyles, *et al*., "*Privacy and Data Management on Mobile Devices*," Pew Research Center, Sept. 5, 2012, available at https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/ (accessed October 15, 2020).

including their location—not be tracked by others online. However, children and the elderly often lack the technical know how to clear their history or adjust their tracking settings.

93. In another study by the Pew Research Center on the Internet and American

94. 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?" Sixty-eight percent said, "I'm not okay with it because I don't like having my online behavior tracked and analyzed." Twenty-eight percent said, "I'm okay with it because it means I see ads and get information about things I'm really interested in."[29] Thus, more often than not, attitudes toward data collection for use in targeted advertising are negative.

95. A survey of 802 parents and their 12- to17-year-old 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."[30]

96. 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.[31] 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.

97. 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

---

[29] Kristen Purcell, *et al*., "*Search Engine Use*," Pew Research Center March 9, 2012, available at https://www.pewresearch.org/internet/2012/03/09/search-engine-use-2012/ (accessed October 15, 2020).

[30] Mary Madden, *et al*., *Parents, Teens, and Online Privacy*, Pew Research Center November 20, 2012, available at https://www.pewresearch.org/internet/2012/11/20/parents-teens-and-online-privacy/ (accessed October 15, 2020).

[31] Chris Hoofnagle, *et al*., "*How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies*?," Apr. 14, 2010, *available at* http://ssrn.com/abstract=1589864 (accessed October 15, 2020).

than $2,500") in response to how a company should be fined if it purchases or uses 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.

98. 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 one thousand 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%.[32]

99. 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.

100. The study found that 55% of 18-24 year old Americans rejected tailored advertising when they were not informed about the mechanics of such 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. When properly understood by consumers, targeted advertising, and the tracking and profiling in the background, is decried across all age groups.

101. A survey on consumer expectations in the digital world, conducted by Deloitte's

---

[32] Joseph Turow, et al., "*Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It*," Sept. 29, 2009, *available at* http://ssrn.com/abstract=1478214 (accessed October 15, 2020).

Technology, Media & Telecommunications practice[95] 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. Seventy-three percent 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.[33]

d. Seventy-three percent 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.

102. 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 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

[33] Kevin Westcott, *et al*., "*Digital Media Trends Survey: A New World of Choice for Digital Consumers*," Center for Technology, Media & Telecommunications, 12th ed., March 19, 2018, *available at* https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey-2018.html (accessed October 15, 2020).

world."[34]

103. By collecting and sharing Plaintiff's and her children's Personal Data in order to assist in profiling and tracking them across multiple online platforms, and failing to obtain Plaintiff's permission, Defendants have breached Plaintiff's and her children's expectations of privacy.

104. Legislative enactments also reflect society's growing concern for digital privacy.

105. For example, California's Shine the Light Law, Cal. Civ. Code § 1798.83, provides that companies that share a user's personal information with a third-party for direct marketing purposes must disclose to consumers, upon request, the category of personal information that is shared and the identities of the third-parties receiving the personal information.

106. The California Online Privacy Protect Act of 2003 ("CalOPPA"), Cal. Bus. & Prof. Code § 22575, provides that an operator of an online service that collects "personally identifiable information" must provide notice in a public privacy policy to California consumers of, *inter alia*, any categories of such information collected and whether other parties may collect such information "overtime and across different Web sites" when a consumer uses the operator's service.

107. The California Consumer Privacy Act (2018) ("CCPA") secures privacy rights for California consumers, including the right to know about the personal information a business collects about them and how it is used and shared; the right to delete personal information collected from businesses, and the right to opt-out of the sale of their personal information. *See* Cal. Civ. Code § 1798.120(c).

108. 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.

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

---

[34] 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-adstracking-algorithm/?utm_source=digg&utm_medium=email (accessed June 4, 2018).

data privacy) and the top causes of that concern include Defendants' conduct at issue here: companies collecting and sharing personal information with other companies.[35]

iv. Defendants Breach of Privacy Norms Is Compounded by Defendants' Targeting, Tracking, and Profiling of Children.

110. Defendants' unlawful intrusion into Plaintiff's child's privacy is made even more egregious and offensive by the fact that MobilityWare and its SDK partners have targeted and collected *children*'s information, without obtaining parental consent.

111. 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.

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

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:

---

[35] *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 on Oct. 15, 2020).

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.

b. Under state law, children are frequently protected via parental consent requirements. Cal. Civ. Code § 3344 requires "the prior consent of [a] parent or legal guardian" in order for a person to use the name or likeness of a minor under the age of eighteen for advertising purposes. The California Education Code does not allow access to personal data collected from students without parental consent. Cal. Educ. Code § 49076(a).

c. State laws also outright ban certain forms of targeted advertising to children. The California Student Online Personal Information Protection Act ("SOPIPA") requires operators of mobile applications marketed for use in K-12 schools not engage in "targeted advertising," "amass a profile" of children, or sell children's information, based upon any information, including "persistent unique identifiers" (including geolocation), that the operator acquires via the mobile app.

d. The California Privacy Rights for California Minors in the Digital World Act similarly reveals society's concern with the ability of sophisticated ad tech companies to exploit minors under the age of eighteen through targeted advertising, and thus bans certain types of targeted advertising. The Act was passed in part as a response to the surreptitious manner in which companies could exploit children's information: "[w]eb sites and online advertising networks often use persistent identification systems - like a cookie in a person's browser, the unique serial number on a mobile phone, or the I.P. address of a computer - to collect information about a user's online activities and tailor ads for that person."

e. The California Consumer Privacy Act (2018) ("CCPA") provides that a business cannot sell the personal information of minors that are under 16 years of age without consent and cannot sell the personal information of minors that are under 13 years of age without parental or guardian consent. See Cal. Civ. Code §

1798.120(c).

f. 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. Under COPPA, developers of child-focused apps, and any third parties working with these app developers, cannot lawfully obtain the personal information of children under 13 years of age without first obtaining verifiable parental consent.

> COPPA defines "personal information" as including basic and commonly collected information such as names, email addresses, and social security numbers, but it also includes "persistent identifiers that can be used to recognize a user over time and across different Web sites or online services." 16 C.F.R. § 312.2. COPPA's broad definition of "personal information" includes: (1) first and last names; (2) physical address; (3) email address (4) screen name or user name; (5) telephone number; (6) geolocation data; or (7) other persistent identifiers such as IP address, a processor or device serial number, or unique device identifier.

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."[36]

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."[37]

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.[38]

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 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

---

[36] *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)

[37] 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), *supra*, at 42.

[38] Children's Advertising Review Unit, Self-Regulatory Program for Children's Advertising (2014), *available at* https://bbbprograms.org/programs/all-programs/caru (accessed Oct. 15, 2020).

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 their data collection practices, and (3) take other steps to preclude children from accessing apps that surreptitiously capture their Personal Data, Defendants have 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.

G. MobilityWare's Omissions and Misrepresentations Create the False Impression That Its Apps Are Compliant with Privacy Laws and Norms.

121. MobilityWare markets the Gaming Apps as apps that are suitable for children, both explicitly (through public-facing representations) and implicitly (through the game's content, design, and distribution channels).

122. Despite such marketing and representations—and despite having indisputable knowledge that children play the app—MobilityWare omits any meaningful mention of the privacy-invasive collection of Personal Data by the SDKs embedded within the Gaming Apps, and

indeed makes affirmative misrepresentations regarding the collection of children's Personal Data.

123. Such omissions and misrepresentations create the false impression that the Gaming Apps conform to established norms regarding children's privacy, and that Defendants respect those norms.

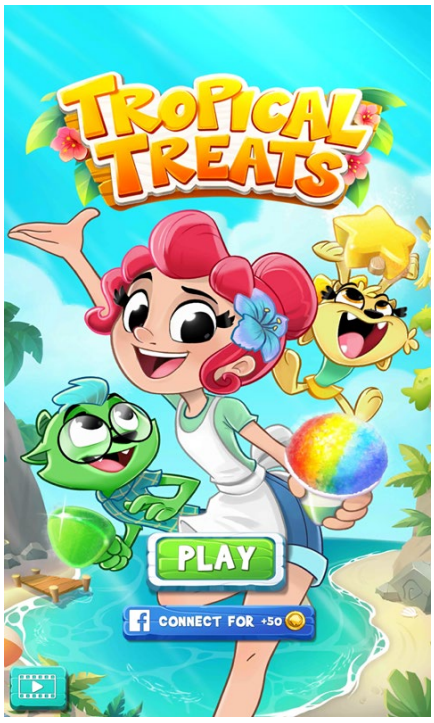
i. MobilityWare Markets the Gaming Apps as Suitable for Children and in Compliance With All Applicable Privacy Laws and Norms.

124. MobilityWare expressly designed many of the Gaming Apps to be played by minor children.

125. For example, "Tropical Treats: Ice Cream Match 3" is a gaming app that includes child-like characters with cartoonish graphics, ice cream, and fun character names such as "Mother Moo" that are attractive to children.

126. The app description in the Google Play Store states: "Welcome to Paradise! Cruise the island in your ice cream truck solving scrumptiously fun puzzles and setting up new shops to grow your mouthwatering business. You'll help Zoey and her spunky, sugared-up pals save the island from Mother Moo—a corporate cow who's taken over paradise with her industrial ice cream.

127. The picture below is a true and correct copy of a screenshot taken from Tropical Treat's opening screen:



128. In marketing the Gaming Apps as suitable for children, MobilityWare implicitly and explicitly purports to acknowledge and adhere to privacy-protective norms.

129. MobilityWare specifically holds the Gaming Apps out to its audience as being family friendly, knowing that its audience reasonably expects such an app *not* to engage in privacy violative behavior.

130. MobilityWare falsely represents that it does not collect children's personal data in violation of any privacy laws or norms.

131. MobilityWare's "Use by Minors" section in its privacy policy states in relevant part:

> "If you are a minor under the age of 18, you must obtain your parent's permission to access the site and our games. If you are under the age of 13, you are not permitted to access the site, use any of our services, or play any of our games. This site and all of our games are not intended for children under the age of 13 and we do not knowingly market to or collect, use or disclose information from children under the age of 13. If MobilityWare learns that we have inadvertently gathered personal information from children under such age, MobilityWare will take reasonable measures to promptly erase such personal information from our records." *See* **Exhibit 2**.

132. However, in the App Store and Play Store, the Gaming Apps are rated as being appropriate for children. Specifically, the Gaming Apps are presented with an "E for Everyone" rating in the Google Play Store and an Age "4+" rating in the Apple App Store. *See* **Exhibit 1**.

133. As discussed above, MobilityWare represents that the Gaming Apps are safe for children and complies with all applicable privacy laws and data collection guidelines.

134. MobilityWare has deceived the public as to the data exfiltration functionality of the Gaming Apps. In so doing, it has created the false impression that the Gaming Apps adhere to child privacy norms.

135. MobilityWare does not attempt to obtain age verification on the Gaming Apps' start screen.

136. In some instances during the gaming experience, a pop-up will appear on a user's screen that says "Quick Survey: Your Age?" The user can either select from four options: (a) 18-34; (b) 35-44; (c) 45-55; or (d) 56+; or the user may simply click an "X" button to exit out of the

pop-up.

137. MobilityWare's belated implementation of age verification or age gating to identify child users of the Gaming Apps is illusory and does not protect children's privacy.

138. MobilityWare's purported age gating does not even attempt to identify users under 18 years of age, as none of the age range options in the "Quick Survey: Your Age?" pop-ups are for children under 18 years of age.

139. MobilityWare's age gating depends exclusively on the reliability of the user's inputted data. It fails to require any method to verify a user's age, explain the purpose behind requiring a user to provide their age, or contain any advisory message that minors should not themselves download the app. As such, MobilityWare's age gating can be easily circumvented with uninformed and inaccurate self-reporting, and therefore fails to adhere to minimal standards of best practices.

140. The presence of MobilityWare's age gate heightens the intrusiveness of the app and increases the potential for the exfiltration of child users' Personal Data, because the mere presence of the age gate implies that MobilityWare will abide by social norms that require parental consent before conducting business with a minor.

141. MobilityWare has control over and responsibility for any advertising and data mining permitted by or undertaken in its app. MobilityWare has failed to safeguard children's personal information and failed to ensure that third parties' collection of data from children is lawful, in part, by allowing its SDK partners to embed advertising SDKs in its family-friendly games.

H. Named Plaintiff Allegations

142. In or around 2017 and 2018 Plaintiff Rona Komins or her children downloaded MobilityWare's Solitaire and Freecell Solitaire gaming apps onto B.K.'s and M.K.'s mobile devices for B.K. and M.K. to play. B.K. and M.K. thereafter frequently played Solitaire and FreeCell Solitaire on their mobile devices on an ongoing and continuous basis.

143. During the time B.K. and M.K. played Solitaire and FreeCell, one or more of the SDK partners of MobilityWare had, with the permission of MobilityWare, embedded one or more

advertising SDKs which collected, disclosed, or used personal information and persistent identifiers of B.K. and M.K. Defendants collected B.K.'s or M.K.'s personal information to track, profile, and target them for commercial gain.

144. Plaintiff Komins did not know that MobilityWare had embedded the SDK Defendants' coding in the Gaming Apps that her children played, and did not know that Defendants were exfiltrating her children's personal data as they played the Gaming Apps.

145. The Defendants never asked Rona Komins for her parental consent—in any form or at any time—to collect, disclose, or use her children's personal information.

146. Defendants' tracking and collection of B.K.'s and M.K.'s personal information parental consent is highly offensive to Ms. Komins and constitutes an invasion of her children's privacy and of Plaintiff's right to protect her children from such invasions.

V. CLASS ALLEGATIONS

147. Pursuant to California Code of Civil Procedure § 382 and California Rules of Court, Rule 3.765, Plaintiff seeks class certification of the following classes:

> **Parents of California Children Residents Under 13 Years Old:** All parents or legal guardian(s) of children residing in the State of California who are younger than 13 years of age, or were younger than the age of 13 when they played the MobilityWare Gaming Apps, from whom Defendants collected, used, or disclosed personal information.
>
> **Parents of California Children Residents Under 18 Years Old:** All parents or legal guardian(s) of children residing in the State of California who are younger than 18 years of age, or were younger than the age of 18 when they played the MobilityWare Gaming Apps, from whom Defendants collected, used, or disclosed personal information.
>
> **California Adult Class**: All persons residing the United States of America who were older than 18 years of age when they played the MobilityWare Gaming Apps from whom Defendants collected, used, or disclosed personal information without disclosures, permissions, or consent.

148. Excluded from each Class are the following individuals: officers and directors of

MobilityWare and its parents, subsidiaries, affiliates, and any entity in which MobilityWare has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

149. Plaintiff reserves the right to modify or amend the definitions of each of the proposed Classes before the Court determines whether certification is appropriate.

150. Numerosity. The members of the classes are so numerous that a joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiff at this time, download figures indicate that the Gaming Apps have been downloaded millions of times.

151. Typicality. Plaintiff's claims are typical of the claims of the class members because, among other things, Plaintiff sustained similar injuries to that of Class Members as a result of Defendant's uniform wrongful conduct, and their legal claims all arise from the same events and wrongful conduct by Defendants.

152. Plaintiff will fairly and adequately protect the interests of the class members. Plaintiff's interests do not conflict with the interests of the Class Members and Plaintiff has retained counsel experienced in complex class action cases to prosecute this case on behalf of the Classes.

153. Commonality. Common questions of law and fact exist as to all class members and predominate over any questions solely affecting individual members of the Classes and Subclasses, including the following:

i. Whether Defendants engaged in the activities referenced herein;

ii. Whether Defendants' acts and practices complained of herein amount to acts of intrusion upon seclusion under the law of California;

iii. Whether Defendants' conduct violated Class Members' California constitutional right to privacy;

iv. Whether Defendants' conduct violated the Unfair Competition Law;

v. Whether members of the classes have sustained damages, and, if so, in what amount; and

vi. What is the appropriate injunctive relief to ensure Defendants no longer unlawfully collect children's personal information to track, profile, and target them over time and across different websites or online services.

154. Ascertainability. Class Members can easily be identified by an examination and analysis of the business records maintained by MobilityWare, among other records within MobilityWare's possession, custody, or control. Additionally, further class member data can be obtained through forensic analyses or through SDK Defendants who may retain data obtained from the Gaming Apps.

155. Predominance. The common issues of law and fact identified above predominate over any other questions affecting only individual members of the Class. The Class issues fully predominate over any individual issue because no inquiry into individual conduct is necessary; all that is required is a narrow focus on Defendants' conduct.

156. Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since a joinder of all members is impracticable. Furthermore, as damages suffered by class members may be relatively small, the expense and burden of individual litigation make it impossible for class members to individually redress the wrongs done to them. 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.

157. Accordingly, this class action is properly brought and should be maintained as a class action because questions of law or fact common to Class Members predominate over any questions affecting only individual members, and because a class action is superior to other available methods for fairly and efficiently adjudicating this controversy.

158. This class action is also properly brought and should be maintained as a class action because Plaintiffs seek injunctive relief and declaratory relief on behalf of the Class Members on grounds generally applicable to the proposed Classes. Certification is appropriate because

Defendants have acted or refused to act in a manner that applies generally to the proposed Classes, making final declaratory or injunctive relief appropriate.

VI. CAUSES OF ACTION

A. CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY

California Constitution, Article I, Section 1

159. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

160. Plaintiff Rona Komins, her children B.K. and M.K., and Class Members have reasonable expectations of privacy in their mobile devices and their online behavior, generally.

161. Plaintiff's 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 or otherwise enabled by the Gaming Apps.

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

163. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, right of privacy, or private affairs by intentionally designing the Gaming Apps (as well as all SDKs identified in this Complaint) to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class Members' activities through the monitoring technologies and activities described herein.

164. 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.

165. Further, the extent of the intrusion cannot be fully known, as the nature of privacy

invasion involves sharing Plaintiff's and Subclass 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 Defendants' conduct is the fact that Defendants' 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.

166. Defendants' 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 Defendants' activities.

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

168. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

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

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

B. INTRUSION UPON SECLUSION

171. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

172. Plaintiff, her children B.K. and M.K., and Class members have reasonable expectations of privacy in their mobile devices and their online behavior, generally. Plaintiff's 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 or otherwise enabled by the Gaming Apps.

173. The reasonableness of such expectations of privacy is supported by MobilityWare's unique position to monitor Plaintiff's and Class members' behavior through its access to Plaintiff's and Class members' private mobile devices. It is further supported by the surreptitious and non-intuitive nature of Defendants' tracking.

174. Defendants intentionally intruded on and into Plaintiff's and Class members' solitude, seclusion, or private affairs by intentionally designing the Gaming Apps to obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class Members' activities through the monitoring technologies and activities described herein.

175. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia,* Supreme Court precedent (most recently and forcefully articulated in the *Carpenter* opinion), legislation enacted by Congress, rules promulgated, and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying location tracking. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's 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 Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiff 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.

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

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

178. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

179. As a result of Defendants' actions, Plaintiff and Class Members seek injunctive

relief, in the form of Defendants' cessation of tracking practices in violation of state law, and destruction of all personal data obtained in violation of state law.

180. Plaintiff and Class Members also seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class Members seek punitive damages because Defendants' 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 Defendants from engaging in future misconduct.

C. VIOLATIONS OF THE UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

181. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

182. Defendants are subject to California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*. The UCL provides, in pertinent part: "Unfair competition shall mean and include unlawful, unfair or fraudulent business practices…"

"Unfair" Prong

183. The UCL prohibits "unfair competition," which is broadly defined as including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." Bus. & Prof. Code §17200.

184. Defendants' business practices, described herein, violated the "unfair" prong of the UCL in that their conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous, as the gravity of the conduct outweighs any alleged benefits. Defendants' tracking, collect, and selling of Gaming App users' personal identifying information for advertising purposes is of no benefit to Gaming App users.

185. Defendants have made material misrepresentations and omissions, both directly and indirectly, related to the privacy-invasive and unlawful behaviors and practices detailed herein.

186. As such, Defendants have engaged in unfair or deceptive acts in violation of the UCL.

187. Defendants' unfair acts allege herein deceived and misled California consumers. Defendants have taken advantage of the lack of knowledge, ability, experience, or capacity of California consumers to the detriment of those consumers.

188. Defendants' conduct also injures competing app developers, software designers and website operators that do not engage in the same unfair and unethical behavior.

189. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable. Defendants are aware of the violations, but have failed to adequately and affirmatively take steps to cure the misconduct.

"Fraudulent" Prong

190. Under the "fraudulent" prong, a business practice is prohibited if it is likely to mislead or deceive a reasonable consumer or, where the business practice is aimed at a particularly susceptible audience, a reasonable member of that target audience. *See Lavie v. Proctor & Gamble Co.,* 105 Cal.App.4th 496, 506-07 (2003).

191. The UCL authorizes a civil enforcement action against "[a]ny person who engages, has engaged, or proposes to engage in unfair competition." Bus. & Prof. Code §17203. "[P]erson" includes "natural persons, corporations, firms, partnerships, joint stock companies, associations and other organizations of persons." *Id.* §17201.

192. MobilityWare intentionally misleads and deceives Gaming App users to believe MobilityWare adheres to privacy-protected norms and child privacy norms.

193. MobilityWare further misleads customers by advertising the Gaming Apps as "E" for Everyone, or "Ages 4+" when its privacy policy states that the games are not intended for children under the age of 13.

194. When users download and play the Gaming Apps, MobilityWare and its SDK partners surreptitiously collect and sell the users' personal identifying information and profile them for behavioral and contextual targeted advertising.

195. Plaintiff and Class Members acted reasonably when they downloaded the Gaming Apps, which they believed to be fun, free, and kid-friendly games.

196. Plaintiff and Class Members lost money or property as a result of Defendants' UCL

violations because (a) they would not have downloaded or played the Gaming Apps absent Defendants' representations and omission of a warning that their information would be tracked, collected, and sold for contextual and behavioral advertising.

"Unlawful" Prong

197. Defendants' business practices, described herein, violated the "unlawful" prong of the UCL by violating California's Constitutional Right to Privacy; Intrusion Upon Seclusion, the California Online Privacy Protect Act of 2003 (CalOPPA), Cal. Bus. & Prof. Code § 22575; the California Consumer Privacy Act (2018) (CCPA), Cal. Civ. Code § 1798.120(c); and the federal Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506.

198. Such conduct is ongoing and continues to date.

199. Defendants' conduct further violates other applicable California and Federal regulations as alleged herein.

200. Plaintiff and Class Members are likely to continue to be damaged by Defendants' deceptive practices, because Defendants continue to omit important app permissions. Thus, injunctive relief enjoining Defendants' deceptive practices is proper.

201. There were reasonably available alternatives to further Defendants' legitimate business interests, other than the conduct described herein.

202. Defendants' practices are therefore unfair, unlawful, and fraudulent under Section 17200 *et. seq.* of the California Civil Code.

D. FRAUD BY OMISSION

Cal. Civ. Code §§ 1709-1711, *et seq.*

203. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

204. MobilityWare actively concealed material facts, in whole or in part, with the intent to induce Plaintiff, her children, and Class Members to download the Gaming Apps. Specifically, Defendants actively concealed the truth about tracking Gaming App users' online behavior, collecting personal information and location data, and selling that Personal Data to third parties to facilitate subsequent tracking, profiling, and targeting.

205. MobilityWare had a duty to disclose that it was surreptitiously collecting users' online behavior and Personal Data, and selling that information to profile users for commercial purposes.

206. Plaintiff and Class members have reasonable expectations of privacy and security of their personal information in their mobile devices and their online behavior, generally.

207. MobilityWare intentionally intruded on and into Plaintiff's, her children's, and Class members' solitude, seclusion, right of privacy, or private affairs by intentionally tracking their online behavior and location, mining their personal information, and selling that information to third parties.

208. MobilityWare actively and intentionally suppressed the discovery of these facts through its marketing and advertising of the Gaming Apps, and the Gaming Apps' interfaces, in which MobilityWare omits or otherwise conceals the full extent of the privacy-violative conduct detailed herein.

209. Similarly, MobilityWare omitted the privacy-protective nature of the Gaming Apps (and their underlying technologies), the lawful nature and use of the SDKs (and related technologies), and the suitability of the Gaming Apps for children, generally.

210. These omitted material facts are facts known or accessible only to Defendants, and Defendants know they are not known to or reasonably discoverable by Plaintiff and the Class Members.

211. Plaintiff and Class Members were unaware of these omitted material facts and would not have downloaded the Gaming Apps had they known of these concealed facts.

212. Plaintiff and Class Members suffered injuries that were proximately caused by Defendants' active concealment and omission of these material facts.

213. Defendants' fraudulent concealments and omissions were a substantial factor in causing the harm suffered by Plaintiff and the Class.

E. NEGLIGENT MISREPRESENTATION

Cal. Civ. Code §§ 1709-1710

214. Plaintiff re-alleges and incorporates by reference each and every allegation

contained elsewhere in this Complaint as if fully set forth herein.

215. MobilityWare represented that the Gaming Apps were rated "E for Everyone" and could be played by minors ages "4+". MobilityWare misrepresented the suitability of the Gaming Apps for children, as the Gaming Apps collected and exfiltrated children's Personal Data.

216. The misrepresentations were communicated to Plaintiff and the Class Members through the Gaming App interfaces.

217. The misrepresentations concerned material facts that influenced Plaintiff and the Class Members' downloading of the Gaming Apps.

218. MobilityWare knowingly made the misrepresentations with the intent to induce Plaintiff and the Class Members to download and play the Gaming Apps.

219. At the time MobilityWare made the misrepresentations, MobilityWare knew or should have known that the misrepresentations were false, or MobilityWare made the misrepresentations without knowledge of their truth or veracity.

220. Plaintiff and the Class Members reasonably, justifiably, and detrimentally relied on the misrepresentations and, as a proximate result thereof, have and will continue to suffer damages.

F. QUASI-CONTRACT

221. Plaintiff re-alleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

222. At all times mentioned herein, Plaintiff and Class Members conferred a benefit upon Defendants in the form of a fee, commission, profit, recurring revenue stream, or other form of monetary payment, which came from Defendants' collecting, tracking, and selling of Plaintiff and Class Members' personal identifying information.

223. Defendants knowingly received, accepted, and retained such fees, commissions, profits, recurring revenue streams, or other monetary payments and have retained the monies as profits.

224. By collecting, storing, and using Plaintiff's, her children's, and Class members' Personal Data without their permission, Defendants were unjustly enriched at the expense of Plaintiff and Class members. It would be inequitable, unjust, and unconscionable for Defendants

to retain the benefits they obtained from using Plaintiff's and Class members' Personal Data for advertising purposes.

225. Plaintiff seeks disgorgement of all proceeds, profits, benefits, and other compensation obtained by Defendants from their improper and unlawful use and collection of Plaintiff's and her children's and the Class members' and their children's Personal Data, as well as all other appropriate relief against Defendants which the Court deems proper, including reasonable attorneys' fees and costs of suit pursuant to California Code of Civil Procedure § 1021.5.

VII. PRAYER FOR RELIEF

226. WHEREFORE, Plaintiff, individually, on behalf of her children, and all others similarly situated, requests that the Court:

A. Certify this case as a class action, appoint Plaintiff as class representative, and appoint Plaintiff's counsel to represent the Class;

B. Enter judgment against Defendants' for the causes of action asserted herein;

C. Award Plaintiff and Class Members appropriate relief, including actual, nominal and/or statutory damages and punitive damages, in an amount to be determined at trial;

D. Award restitution to Plaintiff and Class 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.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all issues so triable.

DATED: March 1, 2020

Respectfully submitted,

Ronald A. Marron

LAW OFFICES OF RONALD A. MARRON
RONALD A. MARRON
ron@consumersadvocates.com
651 Arroyo Drive
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665
Attorney for Plaintiff and the Proposed Class