IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JENA HECKER, on behalf of herself and others similarly situated, Plaintiffs, vs. EASY HEALTHCARE CORPORATION 360 Shore Drive, #B Burr Ridge, Illinois 60607 (Cook County) Defendant.	)	Case no.: 1:21-cv-0349 Jury Trial Demanded

AMENDED COMPLAINT
Class Action Claims under FED.R.CIV.P. 23

COMES NOW, the Plaintiff Jena Hecker, on behalf of herself and all others similarly situated, and brings this action against Defendant Easy Healthcare Corporation for damages and other relief as follows:

NATURE OF ACTION

1. Plaintiff brings this class action under Fed.R.Civ.P. 23 on behalf of herself and all other similarly situated persons who downloaded Defendant's "Premom" application to their smart phones, tablets, and laptop computers – portable electronic devices (hereafter "PEDs") – that utilize Google's Android operating software system from the date of Premom's inception in 2017 to the present. Without their knowledge or consent, and in direct contradiction of Defendant's Terms of Service and Privacy Policies, once Premom was downloaded to these PEDs, Defendant shared personal information and location data regarding the Plaintiff and other proposed class members via its Premom application software with at least three known Chinese

third-party data collection entities. By its conduct, Defendant violated the Plaintiff's and proposed class members' rights by (i) breaching Premom's Terms of Service and Privacy Policies; (ii) unjustly enriching itself; (iii) committing fraud; and (iv) violating the Illinois Consumer Fraud & Deceptive Business Practices Act, 815 ILCS § 505/1 *et seq*. (hereafter "ICFA"). Plaintiff and the proposed class were damaged as a direct result of this conduct.

JURISDICTION AND VENUE

2. This Court has original subject matter jurisdiction to hear this Complaint and to adjudicate the claims stated herein under 28 U.S.C. § 1332(a) in that this is a civil action between citizens of different states and the amount in controversy exceeds $75,000.

3. This Court has personal jurisdiction over the Defendant as an Illinois corporation with its principal place of busines located at 360 Shore Drive, #B, Burr Ridge, Cook County, Illinois 60527.

4. This Court has supplemental jurisdiction under 28 U.S.C. § 1367(a) for all state common law claims asserted herein.

5. In addition, regarding all claims asserted herein, the Plaintiff and proposed class members all accepted and agreed to "Terms of Service" agreements for the Premom application requiring all parties to submit to the exclusive jurisdiction and venue of this court in the state of Illinois[1] for any action or legal proceeding against Premom.

6. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1), in as much as the Defendant is a "resident" of the Northern District of Illinois as set forth under 28 U.S.C. § 1391(c)(2) because Defendant operates its principal place of busines at 360 Shore Drive, #B,

[1] The Terms of Service Agreement dated May 19, 2017 and updated on September 22, 2020 states all claims "must be resolved in a court [state or federal] located in Chicago, Illinois." The Terms of Service Agreement updated on November 19, 2020 states, "The parties hereto hereby submit to the exclusive jurisdiction and venue of the courts of the State of Illinois."

Burr Ridge, Cook County, Illinois 60527.

PARTIES

7. Defendant Easy Healthcare Corporation ("Easy Healthcare") (p/k/a Easy at Home Medical, L.L.C.) is an Illinois corporation registered and in good standing to do business in the state of Illinois. Its principal place of busines is located at 360 Shore Drive, #B, Burr Ridge, Cook County, Illinois 60527. Its President and registered agent Xiaolian Liu is located at this same address.

8. Plaintiff Jena Hecker is an adult female of sound mind over eighteen years in age who currently resides in Clifton, Virginia. On or about February 2020, the Plaintiff downloaded Defendant's Premom application on her One-Plus PED that operates the Android operating software system.

9. Plaintiff brings this action on behalf of herself and others similarly situated.

FACTUAL ALLEGATIONS

10. Defendant Easy Healthcare is one of the largest on-line providers of home and workplace healthcare products selling various devices such as thermometers, oximeters, pregnancy tests, drug tests, *etc.* Its website states, "Easy Healthcare is dedicated to providing user-friendly healthcare products. Its notable brands include Easy@Home for home use healthcare and Areta for professional use."[2] Defendant also sells under the product names "Premom" and "Sweetie Song."[3]

[2] *See* www.healthcare-manager.com/pages/about-us

[3] See https://premom.com/collections/all-products/sweetiesong+easy-home-fertility

11. As part of its business operations, Defendant created and offers an application ("app") for PEDs called "Premom"[4] on the internet and various on-line stores (*e.g.,* Google Play, Apple's App Store) for persons such as the Plaintiff to download free of cost. In particular to the claims made herein, the Plaintiff and proposed class members downloaded this app on PEDs with Google's Android operating software system.

12. This app acts as an ovluation tracker, period calendar, and fertility tool. Its website states: "Premom is dedicated to helping women get pregnant sooner and naturally. As a unique and innovative ovulation prediction app, Premom is a simple, effective and affordable solution for all trying to conceive women. Premom has constantly worked as [*sic*] game changer in the women's reproductive health industry." It claims to be one of the most popular fertility apps among Android and iOS users.[5]

13. Purchasers of Defendant's healthcare products, like Plaintiff, are encouraged to utilize Defendant's Premom app. Also, users of Defendant's Premom app are solicited to purchase Defendant's healthcare products to assist in their fertility.

14. Since its inception, Premom has been downloaded on over 500,000 PEDs using the Android operating software system worldwide.[6]

15. Sometime during February 2020, Plaintiff Jena Hecker downloaded the Defendant's Premom app onto her One-Plus PED using the Android operating software system

[4] Any reference to the Premom application herein includes all versions and updates offered by Defendant at all relevant times herein.

[5] *See* www.premom.com/pages/about-us

[6] *Id.* at fn. 5.

while in Virginia and began using this app. Plaintiff had learned about the Premom app when she was purchasing online healthcare products offered by Defendant.

16. Like all others downloading Defendant's Premom app on their PEDs, once this app was downloaded by Plaintiff, the Plaintiff and Defendant entered into and agreed to a "Terms of Service Agreement" (hereafter "TSA") provided by Defendant (dated May 19, 2017; attached as **Exhibit A**).[7]

17. The TSA is posted on Defendant's website and incorporates by reference Defendant's "Privacy Policy" by providing a link thereto.[8] Via its Privacy Policy (dated May 2, 2017; attached as **Exhibit B**) posted on Defendant's website,[9] the Plaintiff and other Premom app users entered into agreement with Defendant for this Policy's terms and conditions. Defendant makes the following promises to the Plaintiff and other Premom app users regarding the significance and materiality of their personal information:

> EASY HEALTHCARE CORPORATION (the "Company") is committed to safeguarding any personal information that may be collected through our site or mobile application and to ***ensuring that you are fully informed as to how your personal information will be used***. (Ex. B, preamble, emphasis added)

[7] The TSA states, "By visiting or using the services [*e.g.,* the PREMOM app] available on the PREMOM website . . . you are agreeing to the following terms without change." (Ex. A, pg. 1) The Defendant's Privacy Policy dated May 2, 2017 (Ex. B, pg. 1), states, "By accepting this Privacy Policy and our End User License Agreement, or by using the PREMOM Application (hereafter "Application"), You expressly consent to our collection, use, and disclosure of Your personal information in the manner described in this Privacy Policy." There are subsequent TSA agreements effective on September 22, 2020 and November 19, 2020 stating the same.

[8] Note: Any terms of service presented on one's PED when downloading the Premom app refers to the current TSA on Defendant's website. https://premom.com/pages/terms-of-service

[9] https://premom.com/pages/privacy-policy Note: The Privacy Policy presented on one's device when downloading the Premom app refers to the current Privacy Policy on Defendant's website.

18. As referenced herein, any TSA or Privacy Policy was drafted solely by the Defendant with no input from Plaintiff or other Premom app users.

19. These agreements emanated from Defendant's Illinois location and were posted on its website and Premom app from there. Any and all complaints by Premom customers regarding this product are directed to Defendant's Illinois location. All of Defendant's fraudulent and contractual actions addressed herein occurred primarily and substantially in the state of Illinois.

20. In this Privacy Policy, the Plaintiff and other app users provide express consent to Defendant to collect, use, and disclose their personal information, but only "in the manner described in this Privacy Policy." (Ex. B)

21. In the Privacy Policy, Defendant sets forth a description of the information that "we" (*i.e.,* Defendant) collect from Plaintiff and other app users. (Ex. B, § 1)

22. Regarding the use of personal information that Defendant collects from Plaintiff and other app users, the Privacy Policy states, "We [*i.e.,* Defendant] use information in the files and databases we maintain about You . . ." (Ex. B, § 2) In other words, Defendant represents that only it will use information obtained from app users and said information will only be stored on Defendant's databases.

23. In the Privacy Policy, Defendant states how "we" (*i.e.,* Defendant) will use the Plaintiff and other app user's personal information. (Ex. B, § 2) Defendant sets forth a series of bullet points describing how Plaintiff and other app user's personal information will be used by Defendant only. (*Id.*) None of these bullet points set forth Defendant sharing any of Plaintiff's or other app users' personal information with any third parties.

24. In the Privacy Policy, the Defendant lists specific exceptions regarding how it may share Plaintiff's and the other Premom app users' information with others. Defendant sets forth specific examples such as required disclosure to government or law enforcement, or how other unlawful interceptions (*e.g.,* hacking) may occur. (*Id.*)

25. In the Privacy Policy, again acknowledging the significance and materiality regarding disclosure of personal information to third parties, the Defendant states, "***We will not use your personal information for any purposes***, other than those outlined in this Privacy Policy and/or in the EULA, ***unless we have your consent***." (Ex. B, § 4) (emphasis added) Defendant outlined the specific scenarios as follows:

> We will not share your ***personal information with any other third parties without your permission***, ***unless***: (a) we are required to do so by law or when necessary to ***comply with*** a current judicial proceeding, a court order or legal process served on the Company. In all cases, such information will only be disclosed in accordance with applicable laws and regulations, and/or (b) in the event of a ***sale, merger, liquidation, dissolution, reorganization or acquisition*** of the Company so long as the party acquiring the information agrees to be bound by the terms of this Privacy Policy. In addition, and notwithstanding the foregoing, we may provide aggregate statistics about users, information regarding the use of the Application, information for hash encryption purposes and other information to third parties that will ***not include*** any ***personally identifiable information***.
>
> (Ex. B, § 4) (emphasis added).

26. In the Privacy Policy, the Defendant further states "you explicitly consent to the following use by us [*i.e.,* Defendant] and disclosure by us of your information:" (Ex. B, § 4). It then sets forth three bullet points:

- OBTAINING AND TRACKING YOUR INVENTORY OF INSTALL APPLICATIONS TO PERMIT OUR APPLICATION TO PROPERLY FUNCTION.
- OBTAINING AND TRACKING YOUR USAGE AND ***NONIDENTIFIABLE INFORMATION*** OF YOU PERTAINING TO

> THE APPLICATION FOR THE PURPOSES OF TRACKING ANALYTICS OF THE USAGE OF OUR APPLICATION, INCLUDING SHARING INFORMATION WITH ANALYTIC SOFTWARE EXTENSIONS PROVIDED BY THIRD PARTIES
>
> - OBTAIN ***NONIDENTIFIABLE DATA*** ABOUT YOU, COMPILE THAT DATA WITH THE ***NONIDENTIFIABLE DATA*** OF OTHER USERS, AND DISCLOSE THAT INFORMATION TO THIRD PARTIES

(Ex. B, § 4) (emphasis added)

27. In its Privacy Policy effective October 8, 2020 (attached as **Exhibit C,** and still incorporated by reference via the "Terms of Service" agreement) posted on its website[10] (hereafter "Privacy Policy II"), Defendant continues to acknowledge the significance and materiality of Plaintiff's and other Premom app users' personal information by promising:

> EASY HEALTHCARE CORPORATION ("Easy Healthcare", "we", "us", "our") ***is committed to safeguarding the personal data*** that is collected from you through our website ("Site") and the Premom mobile application ("Premom") (the Site and Premom together are called the "Services").
>
> ***Your privacy and the security of your personal data are very important to us*** and we are ***dedicated to protecting the privacy*** of those who use our Services.
>
> Except as disclosed in this Privacy Policy, ***we will not sell, share,*** license, trade, or rent ***your personal data to others***.

(Ex. C, pg. 1) (emphasis added)

28. In the Privacy Policy II, the Defendant defines "personal data" as follows:

> "Personal Data" means ***any information*** relating to an identified ***or identifiable*** natural person. Basically, information is Personal Data if it's possible to identify an individual directly from the information, or ***if an individual can be identified by combining that information with other information***.

(Ex. C, pg. 1) (emphasis added)

[10] https://premom.com/pages/privacy-policy

29. In the Privacy Policy II, the Defendant states how "we" (*i.e.,* Defendant) will use the Plaintiff and other Premom app users' Personal Data. (Ex. C, pgs. 3-4) None of these specific uses state Defendant will provide Personal Data to any third-party. Indeed, Defendant promises, "***We will not share or sell*** your ***Personal Data*** to advertising platforms, data brokers, or information resellers." (Ex. C, pg. 4) (emphasis added)

30. When it comes to sharing Plaintiff and other Premom app users' Personal Data, the Privacy Policy II states that Defendant will only "share Personal Data when ***we have your consent***." (Ex. C, pg. 4) Defendant sets forth other exceptions to sharing Personal Data such as employing other companies to perform tasks on Defendant's behalf, requests from law enforcement or government agencies, subpoenas, other legal processes, and business transactions such as mergers and acquisitions. (Ex. C, pgs. 4-5) It further states, "We may provide aggregate and ***anonymous information*** derived from your Personal Data to third parties as long as that information ***does not include any of your Personal Data***." (Ex. C, pg. 5)

31. Reiterating the significance and materiality regarding the Plaintiff and other Premom app users' Personal Data, and further describing what constitutes Private Data, the Privacy Policy II states, "We believe that the ***biggest threat to security and privacy*** is that someone gets ***your device and account information***." (Ex. C, pg. 12) (emphasis added)

32. Plaintiff and other Premom app users had every reason to rely upon the representations made by Defendant in its Privacy Policies regarding the significance and materiality of the protection of their personal information and location data.

33. On or soon after August 20, 2020, Plaintiff learned that Defendant had been sharing her and other Premom App users' personal information and location data from their

Android operating software system PEDs with three Chinese entities. This data sharing began as of the Premom app's availability for download in 2017.[11]

34. This was being done in secrecy without Plaintiff or other Premom app users' knowledge and consent and in violation of Defendant's Privacy Policies.

35. These three third-party Chinese entities are:

Jiguang (a/k/a Aurora Mobile, Ltd.)[12] – located in Shenzhen, Guangdong, China. It claims to provide its clients with user activity analysis, precision marketing, financial risk control and location-based analysis. It is traded on NASDQ under "JG".[13] If allowed access to an Android user's app, its third-party push notification services (*i.e.,* JPush software development kit ("SDK")) can collect users' GPS locations, immutable persistent device identifiers (*see* Router MAC (a/k/a BSSID) and IMEI, ¶ 40, *infra*) and identification of apps the users have installed. Jiguang's transmission results "in consumers' personal data being trivially vulnerable to eavesdroppers."[14]

Umeng, located in Beijing, China, claims to be the leading provider of mobile app analytics in China. Umeng was originally founded in April 2010 and was acquired by Alibaba in 2013. Umeng claims that its state-of-the-art mobile app analytics and data-powered cross-promotion/advertising platform helps mobile apps increase the size and value of audiences. Umeng offers enterprise-class analytics and other solutions to hundred thousands of mobile app companies in over 65,000 apps across iOS, Android, and other platforms.[15] It is traded on the New York Stock Exchange as BABA.

UMSNS, a China based data collection firm. The website UMSNS.com is operated by Alibaba Cloud Computing and is not accessible outside China.

---

[11] From her investigation, Plaintiff believes the Premom App became available in Spring 2017.

[12] Defendant alleges to have stopped allowing Jiguang access to Premom app user data in August 2020. *See "A popular fertility app shared data without user consent, researchers say,"* The Washington Post, Tonya Riley, Aug. 20, 2020. This denial of access would only apply to app users who have downloaded Premom's most recent version. Interestingly, Defendant failed to address inquiries regarding the other two Chinese entities. *Id.*

[13] https://www.crunchbase.com/organization/jiguang

[14] *JPush Away Your Privacy: A Case Study of Jiguang's Android SDK*; J. Reardon, N. Good, R. Ritcher, N. Vallina-Rodriguez, S. Egelman, Q. Palfrey; Aug. 2020; International Computer Science Institute.

[15] https://www.linkedin.com/company/umeng/about/

36. These three Chinese entities were formed and are located in China. These entities store all the Premom app users' data set forth herein on servers located in China. Under Chinese law, all of this data is accessible by the People's Republic of China, and in turn the Communist Party of China.[16]

37. Defendant deceived the Plaintiff and other Premom app users because, unknowing to them, it directly worked with these three Chinese entities prior to launching the Premom app. Prior to its launch, Defendant coded into the Premom app software the ability for these Chinese entities to access and take Plaintiff's and Premom app users' personal information and location data. Defendant did this in exchange for receiving remuneration from these three Chinese entities. While having done this, Defendant misrepresented to Plaintiff and other Premom app users that it would not do so, and in fact, concealed this from them. Such conduct by Defendant is an unfair, immoral, and unscrupulous business practice.

38. These three Chinese entities are "third parties" and/or "advertising platforms, data brokers, or information resellers" referenced in Defendant's Privacy Policies.

39. The Plaintiff and other Premom app users have not provided any consent to Defendant to share any personal information or location data with these Chinese entities, and Defendant never informed Plaintiff and other Premom app users that their personal information would be provided to these Chinese entities.

[16] https://www.cnbc.com/2019/09/23/china-to-place-government-officials-in-100-companies-including-alibaba.html Referencing China's National Intelligence Law from 2017 requires organizations and citizens to "support, assist and cooperate with the state intelligence work."

40. The Plaintiff's and Premom app users' personal information and location data that Defendant shared with these three Chinese entities include geolocation data, device activity data, user and advertiser IDs, and non-resettable device hardware identifiers. These are also known as "persistent identifiers;" meaning identifiers that tend not to change over time. Combining persistent identifiers with information about where it was observed allows a data collector to reconstruct an individual's activities. Some of the persistent identifiers Defendant shared were:[17]

a. **Wi-Fi MAC** (media access control) address:

> A MAC address is a unique identifier assigned to a network interface controller (NIC). Using this address; phones, computers, printers, routers, and essentially every device connected to a router can be identified, so that communications can be correctly routed to it. Any PED that has Wi-Fi capabilities has a MAC address associated with that device's network interface, which can also be used to uniquely identify it. Collection of this identifier by apps can be used to track each individual users' activities across various apps and services. It cannot be changed without modifying the device's hardware. MAC addresses are rarely collected by app companies, because doing so violates platform policies. As an example, about 1% of Android apps collect MAC addresses.[18] "[A]pp makers and third-party analytics firms [use MAC addresses] to build profiles of consumer behavior that persist through any privacy measure short of the owner getting a new phone." *Id.*

[17] The complete list of all types of personal information and location data collected would be:

Jiguang:
- Geolocation (GPS)
- Router MAC
- AAID

UMSNS:
- Android ID
- HWID
- IMEI
- Wi-Fi MAC

Umeng:
- AAID
- Android ID
- HWID
- IMEI
- Wi-Fi MAC
- Bluetooth Name
- Bluetooth MAC
- Geolocation
- Router SSID
- Router MAC

[18] https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738

b. **Router MAC** (a/k/a BSSID) address**:**

The MAC address of the Wi-Fi router to which a Wi-Fi-enabled device is connected is known as the BSSID, and like other MAC addresses (described above), is not resettable without modifying hardware. Because Wi-Fi routers tend to be in fixed geographical locations, the collection of BSSIDs, which uniquely identify them, is often used to infer a device's physical location. Several databases exist for the sole purpose of mapping BSSIDs to GPS coordinates.[19] Similarly, when apps collect both BSSIDs and GPS coordinates, it is often because they are building their own such databases.

c. **IMEI** (International Mobile Equipment Identity):

This is a hardware identifier tied to a device, particularly to cellphones. It cannot be changed without changing the device.

d. **AAID** (Android Advertising ID):

This is an identification code that allows advertisers and data brokers to build a personalized profile for ad suggestions and other purposes, allowing companies to track users' interests and tendencies across different apps and web activities. The identifier enables advertising networks to trace the habits and hobbies of device users.[20] This can theoretically be changed but is typically outside a lay person's ability. Also, even if this identifier is changed, if a recipient collects it alongside other non-resettable identifiers (*e.g.,* MAC addresses, IMEI), the data collector can connect the old AAID to the new one (a/k/a "ID Bridging"). In other words, even if you "keep resetting your advertising ID, the ad network will use other, more persistent identifiers to attach the fresh advertising ID to your existing profile."[21]

e. **Hardware ID** (Serial Number):

This is a hardware-based serial number that uniquely identifies the device and cannot be changed or reset.

[19] https://en.wikipedia.org/wiki/Wi-Fi_positioning_system#Public_Wi-Fi_location_databases

[20] https://usa.kaspersky.com/blog/android-device-identifiers/20040/

[21] https://usa.kaspersky.com/blog/android-device-identifiers/20040/

f. **Router SSID** (Service Set ID) :

This is the technical term for a Wi-Fi network name, which may be used to infer a user's location or reveal other information. Most users' SSID names are personalized.[22] Router SSIDs can be used to infer accurate geolocation of the router being used by the device, in much the same way as one can do with a BSSID. The key difference is that BSSIDs are guaranteed to be uniquely-identifying, whereas an SSID may not be (though many are).

41. The personal information and location data set forth in ¶ 40 is shared by Defendant with the three Chinese entities when the Plaintiff and other Premom app users unlock/use their PED.[23] This occurs whether the person is using the Premom app or not.

42. The types of data set forth in ¶ 40 are unique personal identifiers for the Plaintiff and each Premom app user. The importance and significance of this private data is not only material under Defendant's Privacy Policies, but also reflected in Google Play's Developer Policy. It prohibits connecting AAID to "personally-identifiable information or associated with any persistent device identifier [for example, SSID, MAC address, IMEI] without explicit consent."[24] As a further example, the Federal Trade Commission found that MAC addresses alone are considered personally identifiable information under the Children's Online Privacy Protection Act.[25]

---

[22] Suranga Seneviratne, Fangzhou Jiang, Mathieu Cunche, Aruna Seneviratne. *SSIDs in the Wild: Extracting Semantic Information from WiFi SSIDs*. The 40th IEEE Conference on Local Computer Networks (LCN), Oct 2015, Clearwater Beach, Florida, United States.

[23] "Americans now check their phones 96 times a day – that's once every 10 minutes, according to new research by global tech care company Asurion." https://www.prnewswire.com/news-releases/americans-check-their-phones-96-times-a-day

[24] https://support.google.com/googleplay/android-developer/answer/10286120?hl=en&visit_id=637439180084707377-112706663&rd=1

[25] *Id.* at fn. 14. "'It's a way of enabling long-term tracking of users without any ability to opt-out,' said Joel Reardon, an assistant professor at the University of Calgary and co-founder of AppCensus, Inc. 'I don't see another reason to collect it.'" *Id.*

43. Also, if any of these three Chinese entities have their data "hacked" by parties with nefarious intentions, it is possible that neither Defendant nor the Chinese entities are under any obligation from state or federal laws to report said data violations to any Premom users. Therefore, Premom users are completely vulnerable to illegal data breaches of personal information and location data with no notice thereof or the ability to address the same.

44. Defendant admits that its sharing of this data with these three third-party Chinese entities damages Premom users' security and privacy. "We believe that the ***biggest threat to security and privacy*** is that someone gets your ***device and account information***." (Ex. C, pg. 12) (emphasis added)

45. Due to Defendant's conduct set forth herein, the three third-party Chinese entities, and in turn the Chinese government:

a. know the exact geolocation of the Premom app user (and ability to track said user's movements) by possessing unique identifiers from: their PEDs, personal and/or workplace wi-fi routers, all wi-fi routers utilized by the users, and precise GPS readings from devices;

b. know all other apps that Premom users have on their PEDs which reveals a great deal of highly personal and private information (*e.g.,* personal interests, hobbies, health, politics, religion, dating, banking, sexual orientation, *etc.*);

c. know and track Premom users' consumer activity, and in turn, the ability to construct a personal advertisement profile;

d. have the ability to determine the phone number for each Premom user; and

e. conduct "ID Bridging" capabilities with this combined data providing them an accurate permanent profile of the user, their activities, preferences, and personal details, even if the user tries to protect their privacy by changing the system-wide privacy settings.

46. By Defendant sharing Plaintiff's and other Premom users' personal information and location data set forth in ¶ 40, *supra*, and the pervasive intrusion available from this data as set forth in ¶ 45, *supra*, Defendant violated the material terms and conditions of its Privacy Policies directly harming the Plaintiff and other Premom app users by disclosing the personal information and location data it explicitly promised it would not.

47. The only manner in which Plaintiff and other Premom app users can remedy themselves from the damage caused by Defendant providing these three Chinese entities with their personal information and location data is to physically replace their PEDs and routers (*e.g.,* to eliminate the ability to track location provided via MAC, IMEI and other hardware identifiers) and to engage a technical professional to change personal advertising identifiers (*i.e.,* AAID, Android IDs).

48. In November 2020, the Plaintiff replaced her One Plus PED with a new device at the cost of $499.00. Plaintiff estimates that replacing all other routers in her home with MAC addresses will be $1,200.00.

APPLICABLE LAW

49. When Plaintiff and other Premom app users download Defendant's Premom app, the Terms of Service and Privacy Policy agreements apply to said users.

50. Under Premom's Terms of Service agreement (dated May 19, 2017, Ex. A), all claims related to the agreement are to be governed by the laws of the State of Illinois. In particular, it states, "This Agreement is governed in all respects by the laws of the State of Illinois, without giving effect to any principle that may provide for the application of the law of

another jurisdiction." (*Id.* at pg. 7) The same applies to all subsequent Terms of Service Agreements.[26]

CLASS ALLEGATIONS

51. Plaintiff and the proposed class hereby incorporate by reference paragraphs 1 through 50 set forth above.

52. Plaintiff brings this class action under Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and the following class:

> All persons located in the United States who have downloaded Defendant's Premom application on PEDs with the Android opearting software system (hereafter "Proposed Class").[27]

53. Class action treatment of Plaintiff's claims are appropriate because, as alleged in paragraphs 54-60, *infra*, all of Federal Rule of Civil Procedure Rule 23's class action requisites are satisfied.

54. Class certification is appropriate under Federal Rule of Civil Procedure 23(a)(1). Plaintiff estimates that the proposed class includes at least 50,000 persons and, as such, is so numerous that joinder of all class members is impracticable.[28]

---

[26] Under Premom's Terms of Service agreement (updated September 20, 2020), all claims related to the agreement are to be governed by the laws of the State of Illinois. In particular, it states, "This Agreement is made subject to, and shall be construed in accordance with, the laws of the state of Illinois (without regard to its conflict of laws provisions)." Under the Defendant's Premom Terms of Service agreement (updated November 19, 2020), all claims related to the agreement are to be governed by the laws of the State of Illinois. In particular, it states, "These Terms will be construed and governed in accordance with the laws of the State of Illinois, without regard to any rules of conflicts or choice of law provisions that would require the application of the laws of any other jurisdiction."

[27] There is no time limitation on the class definition as Plaintiff believes Defendant's Premom app became available in Spring 2017. In turn, all persons who downloaded this app would fall within the applicable statute of limitations for the legal claims asserted in all Counts herein.

[28] This applies the conservative estimate that only 10% of the 500,000 plus persons who have downloaded Premom on Android PEDs worldwide are located in the U.S.

55. Class certification is appropriate under Federal Rule of Civil Procedure 23(a)(2). Questions of law and fact are common to the class. The Plaintiff and the Proposed Class have been subjected to Defendant's common acts and practices described in paragraphs 16-50, *supra*, and the success of their claims depends on the resolution of common questions of law and fact. Common questions of law include*, inter alia*:

- Did the Plaintiff and Proposed Class enter into a contractual agreement with Defendant via its Terms of Service and Privacy Policy agreements under Illinois law (*i.e.,* offer, acceptance, consideration)?
- If so, under Illinois law, was the data shared by Defendant with the third parties set forth herein a breach of its Privacy Policies or a permitted exception under those Policies?
- Did Plaintiff and the Proposed Class suffer damages as a result of this breach under Illinois law?
- Have the Plaintiff and Proposed Class met all the necessary elements to assert a claim of unjust enrichment under Illinois law?
- Have the Plaintiff and Proposed Class met all the necessary elements to assert a claim of fraud under Illinois law?
- Did the Defendant engage in "trade and commerce" under the ICFA by offering the Premom app to Plaintiff and the Proposed Class on app stores under its Terms of Service and Privacy Policies?
- Was the Defendant "advertising" under the ICFA when it published on its website, and on the Premom app, its Terms of Service and Privacy Policies?
- Is Defendant offering "merchandise" via its Premom app as defined in the ICFA?

Common questions of fact include, *inter alia*:

- Were the Defendant's Terms of Service and Privacy Policy applicable to the Plaintiff and the Proposed Class regarding Defendant's Premom app?
- Did the Defendant provide access to the Plaintiff's and Proposed Class's personal information and location data described herein to third-party Chinese companies?
- What data was provided to these third-party Chinese companies?
- Did the Defendant obtain consent from Plaintiff and the Proposed Class to provide personal information and location data described herein to third-party Chinese companies?
- Did the Defendant fail to fully inform Plaintiff and the Proposed Class that it provided personal information and location data described herein to third-party Chinese companies?
- Did the Defendant receive any remuneration for providing this information to the third-party Chinese companies?
- Does the data provided create the ability for these third parties to track Premom app users' location, residential addresses, apps being used on their PEDs, consumer activity, IDs related to physical phones and routers used, and other information allowing "ID Bridging?"

56. Class certification is appropriate under Federal Rule of Civil Procedure 23(a)(3). Plaintiff is a member of the Proposed Class and her claims are typical of the claims of other Class members. For example, Plaintiff and the Proposed Class share an identical legal interest in obtaining a judicial finding that Defendant breached the Terms of Service and Privacy Policy agreements, violated the ICFA, committed fraud, and was unjustly enriched based on Defendant's representations and subsequent provision of highly personal data to third parties. In

turn, Plaintiff and the Proposed Class share the same financial interest in needing compensation necessary to remedy damages caused by taking their personal information and location data and share the same financial interest to recoup the remuneration paid to Defendant by these third parties. Plaintiff has no interests that are antagonistic to or in conflict with the Proposed Class's interest in obtaining such a judicial finding.

57. Class certification is appropriate under Federal Rule of Civil Procedure 23(a)(4). Plaintiff will fairly and adequately represent the interests of the Proposed Class and has retained competent and experienced counsel who will effectively represent the interests of the Proposed Class.

58. Class certification is appropriate under Federal Rule of Civil Procedure 23(b)(1) because the prosecution of separate actions by Plaintiff and Proposed Class members would create a risk of inconsistent or varying adjudications which would establish incompatible standards of conduct for Defendant and/or because adjudications with respect to individual class members would, as a practical matter, be dispositive of the interests of non-party Class members.

59. Class certification is appropriate under Federal Rule of Civil Procedure 23(b)(2) because the Defendant has acted on grounds that apply generally to the Proposed Class, so that final injunctive relief or corresponding declaratory relief sought under the ICFA is appropriate respecting the Proposed Class as a whole.

60. Class certification is appropriate under Federal Rule of Civil Procedure 23(b)(3) because common questions of law and fact, as referenced in paragraph 55, *supra*, predominate over any questions affecting only individual Proposed Class members. In the absence of class litigation, such common questions of law and fact would need to be resolved in multiple

proceedings, making class litigation superior to other available methods for the fair and efficient adjudication of this litigation.

COUNT I
Breach of Contract

61. Plaintiff and the Proposed Class hereby incorporate by reference paragraphs 1 through 60 set forth above.

62. On Defendant's Premom website, Defendant offered the terms of utilizing its app as set forth in the TSA (dated May 19, 2017, Ex. A)[29] to the Plaintiff and Proposed Class. This TSA incorporated by reference the terms and conditions of Defendant's Privacy Policy (dated on May 2, 2017, Ex. B). By their terms, when downloading Defendant's Premom app on their PEDs, Plaintiff and the Proposed Class accepted the terms of Defendant's TSA and Privacy Policy. Therefore, the Plaintiff and Proposed Class and Defendant entered into a contractual agreement encompassing these terms and were bound by such terms.

63. In consideration for Plaintiff's and Proposed Class's ability to use Defendant's Premom app free of charge, Defendant gained the ability to access and use the files and databases it maintained on Plaintiff and the Proposed Class and information it obtained from Plaintiff's and Proposed Class's current and past activities on the app. However, Defendant promised and agreed that Plaintiff's and Proposed Class's personal information and location data would never be shared with any third party without notice and/or their express consent.

64. As set forth in ¶¶ 22-26, 29-30, *supra*, Defendant agreed to use Plaintiff's and Proposed Class's personal information and data for very limited and specific purposes unique to itself only, and furthermore, as set forth in ¶¶ 25-27, 29-30, *supra*, agreed to not disclose any of

[29] There are subsequent Terms of Service agreements. *See* fn. 7.

this personal information to third parties. The Plaintiff's and Proposed Class's agreement with Defendant reflected in Defendant's Privacy Policies acknowledges the material significance of Defendant not sharing Plaintiff's and Proposed Class's personal information and location data with third parties.

65. After the Plaintiff's and Proposed Class's downloading of Defendant's Premom app, the Defendant breached and failed to perform under the terms of the Privacy Policies when it provided their personal information and location data to the three third-party Chinese entities as set forth in ¶¶ 35, 40, *supra*.

66. After the Plaintiff's and Proposed Class's downloading of Defendant's Premom app, the Defendant breached and failed to perform on the terms of the Privacy Policy when it failed to fully inform, or obtain the necessary consent from, the Plaintiff and Proposed Class regarding it providing their personal information and location data to the three third-party Chinese entities as set forth in ¶¶ 17, 20, 25, 29-30, *supra*.

67. The Defendant's disclosure of this information to these third parties did not meet any of the exceptions to third-party disclosures set forth in ¶¶ 23-26, 29-30, *supra*.

68. As a result of the Defendant's breach and the Defendant's disclosure of the information to the third-parties described herein, the Plaintiff and the Proposed Class are damaged as followed: (a) the cost of replacing their PEDs onto which the Premom app was downloaded, (b) the cost of replacing their router device(s), and (c) the costs of retaining a technician with sufficient skills to modify their unique advertiser IDs.

COUNT II
Unjust Enrichment

69. Plaintiff and the Proposed Class hereby incorporate by reference paragraphs 1 through 60 set forth above.

70. On Defendant's Premom website, Defendant offered the terms of utilizing its app as set forth in the TSA (dated May 19, 2017, Ex. A)[30] to the Plaintiff and Proposed Class. This TSA incorporated by reference the terms and conditions of Defendant's Privacy Policy (dated on May 2, 2017, Ex. B).

71. As set forth in ¶¶ 22-26, 29-30, *supra*, Defendant agreed to use Plaintiff's and Proposed Class's personal information and location data for very limited and specific purposes unique to itself only, and furthermore, as set forth in ¶¶ 25-27, 29-30, *supra*, agreed to not disclose any of this personal information to third parties. The Plaintiff's and Proposed Class's agreement with Defendant reflected in Defendant's Privacy Policies acknowledges the material significance of Defendant not sharing Plaintiff's and Proposed Class's personal information and location data with third parties.

72. In exchange for remuneration paid by the three Chinese entities, ¶ 37, *supra*, Defendant programed code into its Premom app so Plaintiff's and Proposed Class's personal information and location data could be taken by these entities. The Defendant's disclosure of this information to these third parties did not meet any of the exceptions to third-party disclosures set forth in ¶¶ 23-26, 29-30, *supra*, and was done so without notice or consent of Plaintiff and Proposed Class.

73. The Defendant received this remuneration benefit to the detriment of the Plaintiff and Proposed Class as set forth in ¶¶ 42, 45, 47-48, *supra*.

[30] There are subsequent Terms of Service agreements effective on September 22, 2020 and November 19, 2020.

74. The Defendant's gain and retention of the remuneration provided by the three Chinese entities would be unjust and should be returned in full value to the Plaintiff and Proposed Class.

COUNT III
Fraud

75. Plaintiff and the Proposed Class hereby incorporate by reference paragraphs 1 through 60 set forth above.

76. Defendant made material factual representations to the Plaintiff and Proposed Class in its Terms of Service and Privacy Policies as set forth in ¶¶ 22-26, 29-30, *supra*, that it would utilize personal information and data for very limited and specific purposes unique to itself, and furthermore, as set forth in ¶¶ 17, 20, 25, 29-30, *supra*, agreed to not disclose any of this personal information to third parties without providing notice and obtaining consent.

77. The Defendant also materially represented to Plaintiff and the Proposed Class the fact that disclosure of this information to third parties would only occur under limited exceptions set forth in ¶¶ 22-26, 29-30, *supra*.

78. The Plaintiff's and Proposed Class's agreement with Defendant reflected in Defendant's Privacy Policies acknowledges the material significance of Defendant not sharing Plaintiff's and Proposed Class's personal information and location data with third parties.

79. Defendant knew or believed that the representations set forth in ¶¶ 76-77, *supra*, were untrue because Defendant intentionally programed code into its Premom app software allowing Plaintiff's and Proposed Class's personal information and data to be taken by the three third-party Chinese entities.

80. Plaintiff and the Proposed Class had a right to rely on the Defendant's representations regarding the protection of their personal information and location data, and, in fact, did so.

81. Defendant made the material factual representations set forth in this Count for the purpose of inducing the Plaintiff and Proposed Class to feel secure in the terms and conditions of secrecy and privacy regarding their personal information and location data when downloading Defendant's Premom app to their PEDs.

82. As a result of the Defendant's conduct, the Plaintiff and the Proposed Class are damaged as follows: (a) the cost of replacing their PEDs onto which the Premom app was downloaded, (b) the cost of replacing their router device(s), and (c) the costs of retaining a technician with sufficient skills to modify their unique advertiser IDs.

83. Due to Defendant's willful or outrageous conduct due to evil motive, or a reckless indifference to the rights of the Plaintiff and Proposed Class, Plaintiff and the Proposed Class are entitled to and will seek punitive damages.

COUNT IV
Violation of Illinois Consumer Fraud & Deceptive Business Practices Act

84. Plaintiff and the Proposed Class hereby incorporate by reference paragraphs 1 through 60 set forth above.

85. The Illinois Consumer Fraud & Deceptive Business Practices Act, 815 ILSC § 505/1, *et seq.* (hereafter "ICFA") states:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact . . . in the conduct of any trade or commerce are

> hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.[31]

815 ILCS § 505/2.

86. "The terms 'trade' and 'commerce' mean the advertising, offering for sale, sale, or distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity, or thing of value wherever situated, and shall include any trade or commerce directly or indirectly affecting the people of this State." 815 ILCS § 505/1(f).

87. "The term 'advertisement' includes the attempt by publication, dissemination, solicitation or circulation to induce directly or indirectly any person to enter into any obligation or acquire any title or interest in any merchandise and includes every work device to disguise any form of business solicitation by using . . . language to mislead any person in relation to any sought after commercial transaction." 815 ILCS § 505/1(a).

88. "The term 'merchandise' includes any objects, wares, goods, commodities, intangibles, real estate situated outside the State of Illinois, or services." 815 ILCS § 505/1(b).

89. Defendant conducted "trade" and/or "commerce" when it began "advertising" its Premom app on or around 2017 on the worldwide web and various public app locations (*e.g.,* Google Play, App Store) by "publishing, disseminating, soliciting" and/or "circulating to induce directly or indirectly" "persons" such as Plaintiff and the Proposed Class to "acquire" an "interest" in said "merchandise" in the form of an "intagible" title or interest in acquiring, downloading, and utilizing Defendant's Premom app.

90. As set forth in ¶¶ 22-26, 29-30, *supra*, Defendant represented and advertised to Plaintiff and the Proposed Class that their personal information and location data obtained from

[31] Any text underlining in these paragraphs is not in the original but is being done in order to follow the relevant definition of terms in the ICFA.

its Premom app would be for very limited and specific purposes unique to itself only, and furthermore, as set forth in ¶¶ 25-27, 29-30, *supra*, agreed to not disclose any of this personal information to third parties.

91. Through its actions, Defendant deceived the Plaintiff and the Proposed Class. Defendant misrepresented to, and concealed from, Plaintiff and other Premom app users that it would not do so.

92. Defendant violated the ICFA, 815 ILCS § 505/2, as it deceived, defrauded, created false pretense, made a false promise, and misrepresented to the Plaintiff and the Proposed Class when it shared their personal information and location data with the three third-party Chinese entities as set forth in ¶¶ 35, 40, *supra*.

93. Defendant violated the ICFA, 815 ILCS § 505/2, because it concealed, suppressed or omitted the material fact of its disclosure of the Plaintiff's and Proposed Class's personal information and location data to third-party Chinese entities - all with intent that Plaintiff and the Proposed Class rely upon the same.

94. Given the Defendant's knowing and conscious conduct of programming into its Premom app software the ability of these three Chinese entities to access such personal information and location data, Defendant performed an unfair, immoral, and unscrupulous business practice, and Defendant intended to harm and damage the Plaintiff and the Proposed Class with said practices.

95. The Plaintiff and Proposed class have suffered actual damages as a result of Defendant's violation of the ICFA in the form of economic damages, and as such, have the right to bring this action and seek relief. 815 ILCS § 505/10.a(a).

96. As a result of the Defendant's conduct, the Plaintiff and the Proposed Class are damaged as follows: (a) the cost of replacing their PEDs onto which the Premom app was downloaded, (b) the cost of replacing their router device(s), and (c) the costs of retaining a technician with sufficient skills to modify their unique advertiser IDs.

97. The Defendant's conduct described herein was willful or outrageous due to evil motive, or a reckless indifference to the rights of Plaintiff and the Proposed Class under ICFA. Therefore, the Plaintiff and Proposed Class are entitled to and seek punitive damages.

98. Pursuant to ICFA § 505/10.a.(c), the Plaintiff and Proposed Class also seek injunctive relief from the Court via an order requiring Defendant to stop sharing any Premom app user's personal information or location data (*see* ¶ 40) with any third-party entity unless it complies with Defendant's existing Terms of Service and Privacy Policy by providing notice and obtaining express consent.

99. Pursuant to the ICFA, the Plaintiff and Proposed Class also seek payment of their reasonable attorney's fees and costs to enforce these claims. 815 ILCS § 505/10.a(c).

PRAYER FOR RELIEF

Plaintiff, on behalf of herself and others similarly situated, pray for relief as follows:

a) Designation of this action as a class action under Fed.R.Civ.P. 23 and appointing Jena Hecker as class representative and Brendan J. Donelon and Daniel W. Craig of Donelon, P.C. as class counsel;

b) Judgment against Defendant finding it breached its contract with Plaintiff and the Proposed Class and awarding the damages sought herein;

c) Judgment against Defendant finding it was unjustly enriched in its actions with Plaintiff and the Proposed Class and awarding the damages sought herein;

d) Judgment against Defendant finding it committed fraud to the Plaintiff and the Proposed Class and awarding the damages sought herein;

e) Judgment against Defendant finding it violated the Illinois Consumer Fraud & Deceptive Business Practices Act with regards to Plaintiff and the Proposed Class and awarding the damages sought herein including an order requiring Defendant to stop sharing any Premom app user's personal information or geolocation data (*see* ¶ 40) with any third-party entity unless Defendant received prior express consent from said users;

f) all costs and attorneys' fees incurred prosecuting these claims;

g) A finding that Defendant's actions were willful or outrageous due to evil motive, or a reckless indifference to the rights of the Plaintiff and Proposed Class, and enter an award of punitive damages; and

h) All further relief as the Court deems just and equitable.

Respectfully submitted,

the law office of DONELON, P.C. www.donelonpc.com
KANSAS CITY ST. LOUIS

/s/ Brendan J. Donelon
Brendan J. Donelon, N.D.Ill #43901
4600 Madison, Suite 810
Kansas City, Missouri 64112
Tel: (816) 221-7100
Fax: (816) 709-1044
brendan@donelonpc.com

Daniel W. Craig, N.D.Ill #6230845
6642 Clayton Rd., #320
St. Louis, Missouri 63117
Tel: (314) 297-8385
Fax: (816) 709-1044
dan@donelonpc.com

Attorneys for Plaintiff

Thomas M. Ryan
Law Offices of Thomas M. Ryan, P.C.
35 E. Wacker Drive, Suite 650
Chicago, IL 60601
Tel: 312.726.3400
Fax: 312.782.4519
tom@tomryanlaw.com

Plaintiff's Local Counsel for Service under LR 83.15