**12-Person Jury**





**CIRCUIT COURT OF COOK COUNTY, ILLINOIS**
**COUNTY DEPARTMENT, CHANCERY DIVISION**

CHRISTINE FARAG and JESSICA VASIL, individually and on behalf of a class of similarly situated individuals,

*Plaintiffs,*

v.

KIIP, INC., a Delaware corporation,

*Defendant.*

No. 2019CH01695

**JURY TRIAL DEMANDED**

## CLASS ACTION COMPLAINT

Plaintiffs, Christine Farag and Jessica Vasil, bring this Class Action Complaint against Defendant, Kiip, Inc. ("Kiip" or "Defendant"), for secretly tracking cellphone users' private information without those users' consent. Plaintiffs allege as follows based on personal knowledge as to themselves and their own acts and experiences, and as to all other matters, upon information and belief, including an investigation by their attorneys.

## NATURE OF THE ACTION

1. Defendant Kiip is a mobile marketing company that displays advertisements on mobile devices through mobile applications, or "apps," installed on individuals' smartphones, including iPhones and Android devices. Defendant's advertising platform utilizes proprietary marketing technology to integrate with smart phone apps and seamlessly deliver ads to consumers.

2. Defendant created its advertising platform to allow app developers to monetize their apps through a wide variety of third-party advertisements that Defendant displays to the consumers while they use such apps. Because Defendant's marketing platform integrates with the software of

smart phone applications, Defendant's software has the ability to gather extensive information about consumers through their use of their cellphones, including personally sensitive information such as health statistics, purchasing activities, dietary profiles, and productivity goals, among other information.

3. Defendant uses the information it collects to custom-tailor ads to specific groups of app users located throughout the country, including ads on behalf of clients such as Coca-Cola, Marriott, and Home Depot.

4. However, Defendant's software often secretly extracts information about smartphone users without their consent. Indeed, as part of an attempt to improve its marketing capabilities and tailor ads to consumers, Defendant has accessed consumers' personal information by tracking and intercepting users' electronic communications without their knowledge or consent—even at times when those individuals' mobile devices were not in use.

5. Not only does Defendant fail to inform consumers about its invasive monitoring activities, Defendant also keeps its app developer partners in the dark about its unseemly and illegal conduct. Indeed, one such developer, Fitnesskeeper, Inc. ("Fitnesskeeper"), which operates the popular fitness app Runkeeper, terminated its relationship with Defendant and issued a public apology upon learning that Defendant was snooping on Runkeeper users by extracting their personal information and intercepting their electronic communications.[1]

6. The data that Defendant has collected from individuals' mobile devices without those individuals' consent includes consumers' personally identifying information, their current geographic location, and their individual cellphone device identifiers. Although this data is valuable to Defendant's marketing business, Defendant's conduct invaded consumers' privacy and

[1] Jason Jacobs, A Message to Our Users, Runkeeper Blog, http://blog.runkeeper.com/4714/a-message-to-our-users/ (last visited Oct. 12, 2016).

violated consumers' statutory and privacy rights, resulting in actual, concrete harm to individuals throughout the country.

7. In addition to violating consumers' privacy rights, Defendant's conduct has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, and the Illinois Eavesdropping Statute, 720 ILCS 5/14-1 *et seq.*

8. Accordingly, in order to redress these injuries, Plaintiffs bring this suit on their own behalf and on behalf of a nationwide class of similarly situated individuals, seeking an award of actual damages; injunctive relief prohibiting Defendant from monitoring, collecting, and transmitting consumers' information without their consent; equitable relief, including the disgorgement of any profits that Defendant derived from ill-gotten information; punitive damages; and reasonable attorneys' fees.

## PARTIES

9. Plaintiff Farag is a natural person whose personal information was collected, intercepted, and/or received by Defendant while she was using her cellphone in Cook County, Illinois.

10. Plaintiff Vasil is a natural person whose personal information was collected, intercepted, and/or received by Defendant while she was using her cellphone in Cook County, Illinois.

11. Defendant Kiip is a Delaware corporation with its principal place of business in San Francisco, California. Kiip is registered to do business in Illinois where it maintains offices, and it conducts business in Cook County and elsewhere throughout the United States.

## JURISDICTION AND VENUE

12. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS

5/2-209 and in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant is registered to do business in Illinois and does business in Cook County, and because Defendant committed certain acts in Cook County that have given rise to the claims at issue in this case, as Defendant extracted personal data from Plaintiffs' cellphone communications and their phones were present in Cook County.

13. Venue is proper in this Court under 735 ILCS 5/2-101 because a substantial part of the events giving rise to the claims occurred in Cook County, as Defendant extracted personal data from Plaintiffs' cellphone communications and their phones were present in Cook County.

## COMMON ALLEGATIONS OF FACT

***Background in Mobile Advertising***

14. Software applications on mobile devices have created new challenges to consumer privacy. Many apps collect vast amounts of personal data and use intelligent tracking technologies to record user information, including individuals' interests, preferences, location, and health, among many other subjects.

15. Apps and their integrated technology also frequently track individuals' usage behavior, such as the length and frequency of an individual's use of an app, which allows companies to connect usage information with a specific customer account to build a profile of an individual user.

16. App users are often unaware of the threats to their privacy rights, because apps and the companies that develop them often fail to fully disclose the types and extent of data collected. Nonetheless, this data is extremely valuable—not just to businesses, but also to advertising companies such as Defendant.

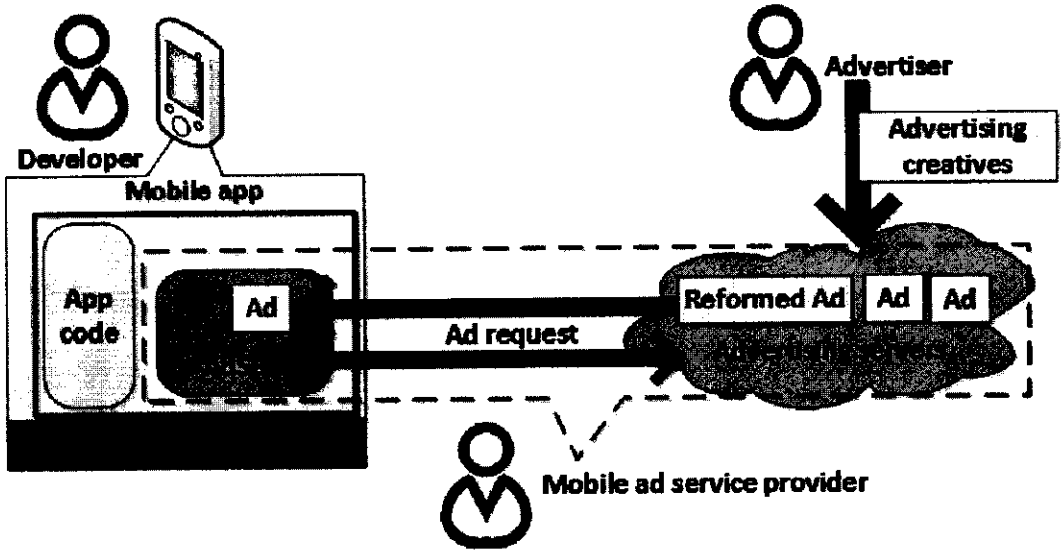
17. Although mobile app companies collect user information, in many cases user data

is also gathered by third-party software or technology integrated into a mobile app. When a consumer downloads, installs, and uses a mobile app on a smart phone, she usually does not know whether the app contains third-party technology that will collect or receive information about the user and her use of the app. Rarely, if ever, are consumers informed of the actual identity of such third parties.

***Third-Party Tracking***

18. Defendant provides a type of mobile advertising technology commonly referred to as a "third-party tracker." Third-party trackers like Defendant's monitor and record information about smartphone users, including how they use their smartphone and what their usage patterns are. They also collect more personal information, such as behavior patterns, interests, and data about the user's particular device.

19. A third-party tracker is not by itself a software app. Rather it is integrated into an existing mobile application. Once integrated, the third-party tracker can passively receive and actively extract data through the app, which is then sent to the tracker's advertising servers and is capable of being used to display ads to the app's user. (*See* Figure 1, below).




**(Figure 1)**

20. Defendant and other third-party trackers use the information they collect to deliver advertisements and promotional offers based on user preferences, demographics, and geographic location, among other characteristics, and they often sell the information they collect to other companies. By design, third-party trackers, including Defendant's, gather extensive information in order to customize ads based on user preferences, behavior, and demographics, and they monetize aggregate user information by selling it to other third-parties.

21. Defendant's advertisements promote large corporate brands, and they are typically marketed to consumers as "rewards" within a mobile app when it is in use. Defendant ordinarily receives payment from such brands whenever an app user accepts or redeems such a "reward," which money Defendant then shares with the developer of the app in which the ad appeared.

***Defendant's Integration with the Runkeeper App***

22. At least as early as August 2014, Defendant partnered with Fitnesskeeper, the developer of the Runkeeper mobile app.

23. Runkeeper users initially must download the app to their smartphone or other mobile device. Once downloaded, the Runkeeper app allows its users to utilize their smartphones' geo-location capabilities to track how far and how fast they run during a workout. Runkeeper also allows users to save the routes they run and their best times on those routes in order to set goals for future runs or share their times with friends.

24. Based on a user's recorded runs and use of the Runkeeper app, the app provides the user with challenges and suggested workouts, tailored to the user in accordance with information gathered through the app.

25. On August 14, 2014, Defendant publicly announced that it had partnered with Runkeeper to deliver advertisements within the Runkeeper app.[2] Defendant's ads contained offers and promotions for various products, and were designed to appear at the moment a user completed a challenge or beat their best run time, so as to make the user feel as though they were being rewarded. (*See, e.g.,* Figure 2, below).

[2] Brittany Fleit, Runkeeper & Kiip Partner to Reward 34 Million Users, Kiip Blog, http://blog.kiip.me/advertising/runkeeper-kiip-partner/ (last visited Feb. 8, 2019).


**(Figure 2)**

26. Defendant has described its integration with Runkeeper as follows:

> [A]fter logging a workout and hitting various milestones (e.g., achieving a best new pace), users will be rewarded serendipitously. Rewards are fitness-related products, . . . "Runkeeper leverages Kiip's technology to give users the extra motivation to run faster or go the extra mile. By enabling brands to own millions of point-of-sweat moments, Kiip adds value to people's daily fitness routines through natural rewards."[3]

***Defendant's Advertising Platform Secretly Collects Users' Personal Data***

27. As with the Runkeeper app, Defendant's technology is designed to recognize when app users complete a milestone or reach an achievement within the app, and seize on that opportunity to deliver a promotion or offer on behalf of one of Defendant's clients.

28. Thus, by design, the defining feature of Defendant's marketing platform is its

[3] *Id.*

ability to monitor events in the lives of app users in real-time and detect when there will be a marketing opportunity for one of Defendant's clients. To determine when such an event has occurred and to deliver effective ads, Defendant partners with app developers like Fitnesskeeper to obtain continuous access to consumers' information and app usage activity.

29. The ads that Defendant shows to app users are not random. Defendant custom-tailors rewards and matches its clients' ads with certain app users based on its clients' target audience and desired demographics.

30. In order to determine whether its clients' products will appeal to certain app users, Defendant secretly collects and monitors users' personal information.

31. For instance, through the Runkeeper app, Defendant extracted app users' current geographic locations and cellphone device identifiers and had access to other personal information—even when the app was not in use and, more importantly, when users were not even using their respective phones. However, Defendant failed to obtain users' consent to do so.

32. Defendant designed and programmed its technology to covertly monitor app users without their consent and without the consent of its app partners in an effort to gain further marketing information about such users. Such activity involved intercepting the contents of consumers' electronic communications between them and their cellular service providers and between users and app developers, such as Fitnesskeeper.

33. Defendant also designed and programmed its marketing platform to integrate the information it obtained through covert means with the information it obtained overtly through its partnerships with app developers, like Fitnesskeeper, in order to build consumer marketing profiles. Defendant's marketing platform then transmitted the contents of the unauthorized user information to its servers for its own use.

34. Defendant never obtained consent from any Runkeeper users before intercepting, monitoring, collecting, and transmitting their personal information. To the contrary, Defendant concealed its actual data collection policies from the public and its business partner apps, including Runkeeper, knowing that consumers would resist disclosing personal information when not using an app and when their phones are not in use.

***Government Inquiry Finds that Defendant's Technology Raises Privacy Concerns***

35. On May 10, 2016, the Norwegian Consumer Council—a Norwegian government agency and consumer protection organization—filed a complaint regarding Defendant and Runkeeper with the Norwegian Data Protection Authority.

36. The complaint was based on a study of privacy risks in mobile apps performed by SINTEF, an independent scientific and industrial research organization.[4] For the study, SINTEF analyzed different popular mobile apps for smartphones to determine what personal information those apps were collecting and revealing about their users.

37. Among the mobile apps, the study focused on Runkeeper and a number of other fitness and sports apps due to the "vulnerability in fitness and sports apps as they often contain health-related data."[5] Specifically, the Norwegian Consumer Council determined that Runkeeper "generates extensive personal data, such as location in combination with time as well as information about the user's physical fitness, health and training habits." [6]

38. SINTEF's study further found that much of this information is obtained by

---

[4] Antoine Pultier et al., SINTEF, Privacy in Mobile Apps: Measuring Privacy Risks in Mobile Apps (2016), *available at* http://www.academia.edu/22037218/Privacy_in_Mobile_Apps_Measuring_Privacy_Risks_in_Mobile_Apps.

[5] *Id.* at 12.

[6] Norwegian Consumer Council, Complaint Concerning the Mobile App Runkeeper 3 (2016), *available at* http://fbrno.climg.no/wp-content/uploads/2016/05/2016-05-10-Complaint-runkeeper-ENG.pdf (hereinafter "Consumer Council Complaint").

Defendant and similar third-party trackers, who "have access to important information about the phone and its user, such as the device identifier."[7]

39. A device identifier is a serial-like identifier for a particular cellphone. Tracking companies such as Defendant use these device identifiers for marketing purposes. The use of these identifiers poses a greater risk than tracking technologies typically used on PC web browsers, because the numbers are difficult or impossible to delete and can be tied to other personal data.

40. Most importantly, however, the SINTEF study found that the Runkeeper application, when integrated with Defendant's technology, "tracks the [user's] GPS position even when the phone is not in use." As a result, "The users can [] be geo-tracked whenever the [smartphone's] GPS function is turned on."

41. This finding resulted from the testers' "48 hour analysis." For this phase of the testing, the testers installed Runkeeper on a smartphone and monitored the phone for 48 hours without ever actually using it. During this period, the testers did not unlock the phone's screen, meaning that the phone was idle and its screen was black. Even though the cellphone tested was not in use over the entire 48-hour period, the testers found that Defendant repeatedly collected information through the Runkeeper app.

42. Based on its finding that "the [Runkeeper] app collects location data and other personal information when the mobile phone and app are not in use," the Norwegian Consumer Council found it problematic that "this personal data is transferred to a third party [Kiip] when the app is not in use."

43. Defendant failed to obtain consent from the consumers whose information it collected. Because users were entirely unaware that their data was being extracted and transferred

[7] Pultier, *supra* note 4, at 13.

from their smartphone communications when the Runkeeper app was not in use—and even when the phone was not in use—there was a complete "lack of consent regarding the collection and sharing of location data . . . ."[8]

***Fitnesskeeper Ends its Relationship with Defendant and Apologizes to Consumers***

44. Shortly after the Norwegian Consumer Council observed in its complaint that "we cannot see that the app at any point – in the app itself, in the terms of use, privacy policy or on its website – makes the user aware that location or other personal data is collected when the mobile phone is not in use or when the user is not involved in a training session, nor that this data is forwarded to a third party [i.e., Defendant],"[9] Fitnesskeeper terminated its relationship with Defendant's advertising service and formally apologized to consumers for Defendant's untoward conduct.

45. On May 17, 2016, the founder and CEO of Runkeeper, Jason Jacobs, issued a written, public apology in response to the Norwegian Consumer Council's complaint and the SINTEF study.[10] His apology, posted on the Runkeeper website, refers to Defendant and states that users' location data was unexpectedly being extracted from consumers' cellphones and received by Defendant. Jacobs further stated that Runkeeper had decided to remove Kiip's technology from its app going forward.

***Allegations Specific to Plaintiffs***

46. Plaintiffs downloaded and used the Runkeeper app on their smartphones while Defendant's third-party tracker was integrated with the app.

47. During their use of the Runkeeper app, Plaintiffs' cellphones communicated with

[8] Consumer Council Complaint at 3.
[9] *Id.* at 4.
[10] Jason Jacobs, A Message to Our Users, Runkeeper Blog, http://blog.runkeeper.com/4714/a-message-to-our-users/ (last visited Feb. 8, 2019).

their cellular service providers and the Fitnesskeeper servers, providing their geo-location information and device identifiers to Runkeeper along with other personal information about themselves.

48. Defendant intercepted, collected, and received the personal information Plaintiffs provided through the Runkeeper app and stored it on their servers. However, Plaintiffs were unaware that Defendant's third-party tracker was integrated with the Runkeeper app and that it was intercepting their communications and collecting their information.

49. Plaintiffs were also unaware that Defendant's third-party tracker was intercepting their phones' electronic communications and collecting their personal information, including their geo-location and device identifiers, while they were not using the Runkeeper app, and even when they were not using their respective cellphones, because Defendant never informed them as such.

50. Plaintiffs never provided consent to Defendant to monitor, intercept, collect, and transmit their personal information while they were not using the Runkeeper app, and especially not when they were not using their respective cellphones.

51. Plaintiffs would never have downloaded or used Runkeeper had they known that Defendant would monitor, intercept, collect, and transmit their information when they were not using the Runkeeper app, and even while their respective cellphones were not in use.

## CLASS ACTION ALLEGATIONS

52. Pursuant to 735 ILCS 5/2-801, Plaintiffs bring this action on their own behalf and on behalf of a nationwide class (the "Class") defined as follows:

> The Class: All people in the United States and its territories who used a mobile app integrated with Defendant's advertising platform during the applicable limitations period.

53. Excluded from the Class are any members of the judiciary assigned to preside over

this matter; any officer, director, or employee of Defendant; and any immediate family member of such officer, director, or employee.

54. Upon information and belief, there are at least thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable.

55. Plaintiffs' claims are typical of the claims of the members of the Class they seek to represent, because the factual and legal bases of Defendant's liability to Plaintiffs and the other members of the Class are the same, and because Defendant's conduct has resulted in similar injuries to Plaintiffs and to all of the other members of the Class. As alleged herein, Plaintiffs and the other members of the Class they seek to represent have all suffered harm and an invasion of privacy as a result of Defendant's unlawful and wrongful conduct.

56. There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class members include, but are not limited to, the following:

(a) Whether Defendant failed to obtain the Class members' consent to intercept and extract personal information, including their location data;

(b) Whether Defendant's conduct violated the Computer Fraud and Abuse Act;

(c) Whether Defendant's conduct violated the Illinois Eavesdropping Statute;

(d) Whether Defendant acted negligently regarding Plaintiffs' and the Class members' personal information;

(e) Whether Defendant breach its implied contracts with Plaintiffs and the Class members.

(f) Whether Defendant was unjustly enriched by receipt of the Class members'

data.

57. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive, and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

58. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class they seek to represent. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither of the Plaintiffs nor their counsel has any interest adverse to those of the other Class members.

59. Defendant has acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

**COUNT I**
**Violation of the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030, et seq.)**

60. Plaintiffs incorporate by reference all of the foregoing allegations as if fully set forth herein.

61. A party violates the CFAA when it intentionally accesses a computer without authorization, or in excess of its authorization, in order to obtain anything of value, or obtains *any information* from any protected computer. 18 U.S.C. § 1030(a)(2)(C), (a)(4).

62. Plaintiffs' personal smart phone devices are "protected computers" under the

CFAA, because such devices constitute high-speed data processing devices that perform logical, arithmetic, and storage functions which are used for interstate or foreign commerce or communication.

63. In violation(s) of 18 U.S.C. § 1030(a)(2)(C) and/or § 1030(a)(4), Defendant intentionally accessed Plaintiffs' protected computers, *i.e.* smartphone devices, in order to obtain valuable information therefrom that it sold to advertisers.

64. Defendant obtained an aggregate value of its use of such information which exceeded $5,000 in any one-year period.

65. Defendant's conduct also constituted damage to ten (10) or more protected computers in any one-year period.

66. As a result of Defendant's conduct and violations of the CFAA, Plaintiffs have suffered actual harm in the form of actual monetary damages, pecuniary losses, and other harms, including an invasion of their privacy, loss of control over their personal information, diminution of the value of their personal privacy, and interference with the unrestricted use of their mobile devices, all of which have ascertainable value to be proven at trial.

## COUNT II
## Violation of the Illinois Eavesdropping Statute (720 ILCS 5/14-1, et seq.)

67. Plaintiffs incorporate by reference all of the foregoing allegations as if fully set forth herein.

68. A person violates the Illinois Eavesdropping Statute where he or she "knowingly and intentionally . . . [i]ntercepts, records, or transcribes, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication . . . ." 720 ILCS 5/14-2(a).

69. The Illinois Eavesdropping Statute broadly defines "private electronic

communication" to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS 5/14-1(e).

70. The mobile devices of Plaintiffs and the other Class members transmitted data and information to mobile app developers and their cellular service providers through the use of the app on their respective smartphones, constituting "electronic communications" under Section 14-2(a) of the Illinois Eavesdropping Statute.

71. By designing and programming its third-party tracker to contemporaneously monitor, intercept, record, and transfer the contents of electronic communications sent by the mobile devices of Plaintiffs and the other Class members, Defendant intentionally and knowingly intercepted and recorded "private electronic communications" in violation of Section 14-2 of the Illinois Eavesdropping Statute.

72. Such electronic communications intercepted by Defendant included non-tracking data such as device identifiers and other private and/or personal communications that Plaintiffs intentionally provided to mobile app developers, their service providers, and/or other apps authorized by Plaintiffs to access such electronic communications, even when the Plaintiffs' phones were not in active use. Defendant intercepted these communications at the same time the subject electronic communications were intentionally transmitted to authorized parties.

73. Plaintiff and the other Class members intended and believed that the information they provided through their smartphone apps would be private. Indeed, their usage information reveals personal information and their device identifiers can be used to trace electronic

communications to their respective mobile devices to determine their individual identities.

74. Plaintiffs and the other Class members expected that such information would remain private and/or would not be transmitted to an unknown third-party entity like Defendant while they were not using apps on their respective smartphones, and especially when they were not even using their mobile devices at all. Plaintiffs and the other Class members reasonably expected that such information would not be used or collected by unknown third-parties in ways that exceeded the scope of their consent.

75. Defendant failed to notify or inform Plaintiffs and the other Class members that it was monitoring and intercepting their personal and private non-tracking data while they were not using apps on their smartphones and/or while their mobile devices were inactive. Therefore, there was no reason for them to believe that anyone was accessing or intercepting their private electronic communications during times when they were not using the app or even using their mobile devices.

76. Neither of the Plaintiffs nor any of the other members of the Class consented to Defendant's interception or use of their private electronic communications. Nor could they have consented—Defendant never sought to obtain consent from Plaintiffs or the other Class members, and each unlawful interception occurred without their knowledge and while they were not using apps on their smartphones, including while they were not even using their respective mobile devices at all.

77. Due to Defendant's unlawful conduct, Plaintiffs and the other Class members are entitled to an award of actual damages pursuant to § 14-6(b); injunctive relief as the Court deems appropriate pursuant to § 14-6(a); and an award of punitive damages pursuant to § 14-6(c).

## COUNT III
## Common Law Negligence

78. Plaintiffs incorporate by reference all of the foregoing allegations as if fully set

forth herein.

79. Defendant assumed a duty of care owed to the Class members users when it provided software that Defendant knew would be installed on the Class members' mobile devices; Defendant knew and could reasonably foresee that this would enable its advertising platform to access, monitor, collect, and transmit individuals' sensitive personal information.

80. Defendant's duty of care obligated it to exercise reasonable care by (1) informing smartphone users (either directly or through its app developer partners) that it could and actually was accessing, monitoring, collecting, and transmitting individuals' sensitive personal information; (2) obtaining permission or valid consent to access, monitor, collect, and transmit individuals' sensitive personal information in accordance with mobile marketing industry standards; and (3) safeguarding users' personal information and preventing unauthorized disclosure to third-parties.

81. Defendant breached its duty of care owed to the Class members as described herein by, among other things, intentionally misrepresenting the nature of its software and data collection practices despite knowledge that Plaintiffs and the other Class members would rely on such misrepresentations; failing to obtain valid consent or permission from smartphone users before intercepting their electronic communications or accessing, monitoring, collecting, and transmitting their personal information; intentionally concealing its data collection activities from the public and even from its app developer partners; and selling or licensing user data to other advertisers and third-parties without authorization.

82. As a direct and proximate result of Defendant's misconduct described herein, Plaintiffs and the other Class members have suffered actual monetary damages, pecuniary losses, and other harms, including an invasion of their privacy, loss of control over their personal

information, diminution of the value of their personal privacy, and interference with the unrestricted use of their mobile devices, all of which have ascertainable value to be proven at trial.

**COUNT IV**
**Negligence *Per Se***

83. Plaintiffs incorporate by reference all of the foregoing allegations as if fully set forth herein.

84. Defendant owed a duty of care to the Class members when it provided software that Defendant knew would be installed on the Class members' mobile devices; Defendant knew and could reasonably foresee that this would enable its advertising platform to access, monitor, collect, and transmit individuals' sensitive personal information.

85. Defendant's conduct in covertly intercepting Plaintiffs' intentional electronic communications constitutes a breach of the duties of care prescribed by the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., and the Illinois Eavesdropping Statute, 720 ILCS 5/14-1 et seq., respectively, resulting in harm to Plaintiffs.

86. The harm that Defendant caused to Plaintiffs and the other members of the Class resulted from the types of occurrences these statutes were designed to prevent.

87. Plaintiffs and the other Class members are the types of persons for whose protection those statutes were adopted.

88. As a direct and proximate result of Defendant's misconduct described herein, Plaintiffs and the other Class members have suffered actual monetary damages, pecuniary losses, and other harms, including an invasion of their privacy, loss of control over their personal information, diminution of the value of their personal privacy, and interference with the unrestricted use of their mobile devices, all of which have ascertainable value to be proven at trial.

**COUNT V**

**Breach of Implied Contract**

89. Plaintiffs incorporate by reference all of the foregoing allegations as if fully set forth herein.

90. Through their conduct and actions, Plaintiffs and the other members of the Class entered into implied contracts in law and in fact with Defendant. Specifically, when Plaintiffs and the other members of the Class downloaded smartphone apps to their respective mobile devices and used the apps, with which Defendant had integrated its third-party tracking software and advertising platform, Plaintiffs and the other members of the Class entered into implied contracts with Defendant.

91. Under these implied contracts, Plaintiffs and the other members of the Class reached a meeting of the minds and mutual understanding with Defendant that Plaintiffs and the other members of the Class would provide some personal information, device data, and usage data through their actual use of the smartphone apps, and in exchange Defendant implicitly agreed that it would only access, monitor, collect, and transmit individuals' personal information and data in accordance with users' expectations, mobile marketing industry standards, and the terms of the applicable terms of use and privacy policy.

92. Defendant breached its agreements with Plaintiffs and the other members of the Class by, among other things, failing to obtain valid consent or permission from the Class members before intercepting their electronic communications and/or accessing, monitoring, collecting, and transmitting their personal information; concealing its data collection activities from the public and even from its app developer partners; and selling or licensing user information and data to other advertisers and third-parties without authorization.

93. Indeed, as the Norwegian Consumer Council observed in its complaint, "we cannot

see that the app at any point – in the app itself, in the terms of use, privacy policy or on its website – makes the user aware that location or other personal data is collected when the mobile phone is not in use or when the user is not involved in a training session, nor that this data is forwarded to a third party [i.e., Defendant]," (Consumer Council Complaint, at 4).

94. As a direct and proximate result of Defendant's breach of its implied agreements, Plaintiffs and the other Class members have suffered actual monetary damages, pecuniary losses, and other harms, including an invasion of their privacy, loss of control over their personal information, diminution of the value of their personal privacy, and interference with the unrestricted use of their mobile devices, all of which have ascertainable value to be proven at trial.

**COUNT VI**
**Unjust Enrichment**

95. Plaintiffs incorporate by reference all of the foregoing allegations as if fully set forth herein.

96. As explained above, Defendant monitored, collected, received, and transmitted the usage data and geo-location information of Plaintiffs and the other members of the Class without their knowledge or consent.

97. To the extent that Defendant collected or received Plaintiffs' and the other Class members' personal information and geo-location data, Defendant has retained a benefit to the detriment of Plaintiffs and the other Class members. This benefit is measurable by the monetary value of the Plaintiffs' and the other Class members' information. Defendant appreciates or has knowledge of such benefit.

98. Further, to the extent that Defendant received advertising revenue as a result of information obtained improperly from Plaintiffs and the other members of the Class, and/or to the extent that Defendant transmitted or sold Plaintiffs' and the other Class members' information and

geo-location data, in whole or in part, to a third-party, Defendant has retained a benefit to the detriment of Plaintiffs and the other Class members. Defendant appreciates or has knowledge of such benefit, which is measurable by the revenue Defendant received.

99. Because Plaintiffs and the other Class members would never have downloaded and used apps containing Defendant's software had they known that such information would be improperly collected by third-parties like Defendant who were unauthorized to gather such information, Defendant has unjustly received and retained a benefit as a result of its conduct.

100. As explained above, Defendant was not authorized and did not have consent to collect this information, and Defendant's retention of this benefit violates fundamental principles of justice, equity, and good conscience.

101. Defendant has been enriched, and it would be unjust to allow Defendant to retain the enrichment.

102. Plaintiffs are therefore entitled to an award of damages in the amount by which Defendant was unjustly enriched and an order requiring Defendant to disgorge any profits or other benefit it has retained.

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the other Class members, pray for the following relief:

A. an order certifying the proposed Class as defined above and appointing Plaintiffs as the class representatives;

B. an award of actual damages under Counts I – V in an amount to be determined at trial;

C. disgorgement or restitution under Count VI in an amount to be determined at trial;

D. injunctive relief under Count II;

E. an award of punitive damages under Count II;

F. an award of reasonable attorneys' fees and other costs; and

G. such other and further relief as the Court deems reasonable and just.

**JURY DEMAND**

Plaintiffs request a trial by jury of all claims that can be so tried.

Dated: February 8, 2019

CHRISTINE FARAG and JESSICA VASIL, individually and on behalf of a class of similarly situated individuals

By: */s/ Paul T. Geske*
One of Plaintiffs' Attorneys

Myles McGuire
Paul T. Geske
Timothy P. Kingsbury
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
pgeske@mcgpc.com
tkingsbury@mcgpc.com

*Attorneys for Plaintiffs*