Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

Interim Class Counsel
(Additional counsel listed on signature page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE IPHONE APPLICATION LITIG.	CASE NO. 10-CV-05878-LHK JURY DEMAND FIRST CONSOLIDATED CLASS ACTION COMPLAINT FOR VIOLATIONS OF: 1. NEGLIGENCE; 2. COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030; 3. COMPUTER CRIME LAW, CAL. PENAL CODE § 502 4. TRESPASS TO CHATTEL; 5. CONSUMER LEGAL REMEDIES ACT, CAL. CIV. CODE § 1750; 6. UNFAIR COMPETITION, CAL. BUS. & PROF. CODE § 17200; 7. BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING; and 8. UNJUST ENRICHMENT

The persons designated below as plaintiffs ("Plaintiffs"), each on his or her own behalf and, collectively, on behalf of all others similarly situated (the putative "Class"), make the following allegations based on their personal knowledge of their own acts and observations and, otherwise, upon information and belief based on investigation of counsel.

I. NATURE OF THE CASE

1. Since Defendant Apple Inc. ("Apple") launched its mobile device business, it has maintained control of how the devices work, how consumers use them, and what happens when consumers use them—including functions that Apple controls, hidden from consumers' sight. Steve Jobs, Apple's founder and CEO, put it most succinctly: "Our job is to take responsibility for the complete user experience. And if it's not up to par, it's our fault, plain and simple." This responsibility has become the mantra for company executives and a major marketing theme. As recently as April 20, 2011, Chief Operating Officer Timothy Cook cited Apple's control of the user experience as a competitive differentiator, stating, "I think the user appreciates that Apple takes full responsibility for their experience . . . ."

2. This responsibility for the complete user experience begins with a consumer's purchase of a mobile device, designed and manufactured by Apple, that works the way Apple wants it to work. Whether an iPhone, iPod Touch, or iPad, (the "iDevices"), they all run Apple's proprietary iPhone operating system software ("iOS").

3. Apple's control extends to the approval and sale of software applications for the device ("apps") to the only marketplace Apple allows—the Apple App Store. No third-party app developer is permitted to sell an app in the App Store without entering into Apple's form iOS Developer Agreement. Every app in the App Store, whether sold to the consumer or offered as for "free," must be approved by Apple and be digitally signed by Apple. Apple trades on its control of the App Store, claiming to offer only apps that it has reviewed and found safe and appropriate. Apple has specifically represented to consumers that the App Store does not permits apps that "violate[] our developer guidelines," such as apps that contain pornography, violate user privacy, or hog bandwidth. See Fig 1.

Fig. 1

4. Finally, Apple controls the process for the development software as well—such as by requiring that developers buy and use Apple's software development kit and providing highly detailed guidelines for app development.

5. Apple uses the iDevices, the App Store, and the software development process to completely control the user experience by constructing the user's entire mobile computing environment, about which Apple has been highly secretive. Apple's control includes restrictions, such as blocking consumers from modifying devices or installing non-App-Store software, and blocking developers and researchers from publicly discussing Apple's standards for app development. It has frustrated inspection of its mobile environment by even prohibiting researchers from analyzing and publicly discussing device shortcomings such privacy flaws. Apple is so secretive about its agreements with app developers that its form contract only came to light last month, through a Freedom of Information Act request that a privacy organization, the Electronic Frontier Foundation, submitted to NASA.

6. Behind Apple's wall of control, it designs its mobile devices to be readily accessible to ad networks and Internet metrics companies to track consumers and access their personal information. These companies not only provide an important revenue source for app developers who provide "free" apps through the App Store, they also furnish the analytic data that demonstrates Apple's market leadership which it so often heralds in its quarterly investor conference calls. These companies, by helping finance third-party apps, gain access to consumers'

mobile devices to collect personal information they use to track and profile consumers, such as consumers' cellphone numbers, address books, unique device identifiers, and geolocation histories—highly personal details about who they are, who they know, and where they are.

7. Apple has a duty to its users that arises from law, the facts of its assertion of complete control and responsibility for the user experience, and its implied and express statements that it will protect the user, the user's personal information, and the security of the user's device. Unfortunately, Apple, having assumed that duty, has breached its duty by failing to fulfill even its most basic duty of care to protect the personal information of its users and security of their mobile devices. As a result of Apple's marketing and total control of the user experience, Apple has earned billions of dollars and created a market capitalization that has made it one of the most valuable companies in the world. This action seeks to hold Apple accountable to the standard imposed on it by law, and that it set for itself, to protect the privacy and security of its users.

II. PARTIES

A. Plaintiffs

8. Plaintiffs ("Plaintiffs") are United States' residents who use mobile devices manufactured by Defendant Apple, Inc. ("Apple") that operate using Apple's proprietary operating system, iOS ("iDevices"). Each Plaintiff downloaded to his or her iDevice and used one or more computer software applications, or apps, from the Apple App Store.

9. Plaintiff Jonathan Lalo downloaded and used numerous free and paid apps from the App Store during the Class Period.

10. Plaintiff Dustin Freeman downloaded and used numerous free and paid apps from the App Store during the Class Period.

11. Plaintiff Anthony Chiu downloaded and used numerous free and paid apps from the App Store during the Class Period.

12. Plaintiff Daniel Rodimer downloaded and used numerous free and paid apps from the App Store during the Class Period.

13. Plaintiff Jared Parsley downloaded and used numerous free and paid apps from

the App Store during the Class Period.

B. Defendant Apple

14. Defendant Apple, Inc. ("Apple") is a California corporation with its principal place of business at 1 Infinite Loop, Cupertino, California 95014. Apple is the maker of the Apple iPhone, iPad, and iPod Touch.

C. Tracking Defendants

15. Defendant Admob, Inc. ("Admob") is a company organized and existing under the laws of the State of Delaware, with its principal place of business located in San Mateo, California. AdWhirl is its wholly owned subsidiary. AdMob purports to be "the world's largest mobile advertising marketplace" offering "both advertisers and publishers the ability to target and personalize advertising to their customers in 150 countries."

16. Defendant Flurry, Inc. ("Flurry") is a Delaware corporation with its principal place of business located in San Francisco, California. Flurry is an advertising content and analytics provider for mobile device applications.

17. Defendant MobClix is a Delaware corporation with its principal place of business in Palo Alto, CA. Mobclix is an ad exchange provider for iPhone apps. Mobclix targets users based on location and the type of app to maximize the money that iPhone developers can make.

18. Defendant Pinch Media, Inc. ("Pinch Media") is a Delaware corporation with its principal place of business located in Hoboken, New Jersey. Pinch Media provides mobile advertising analytics services and partners with ad networks to deliver mobile advertising to mobile devices.

19. Defendant TrafficMarketplace.com. Inc. ("Trafficmarketplace.com") is a Delaware corporation with its principal place of business in El Segundo, CA. TrafficMarketplace.com is a mobile advertising network that purports to provide advertising network solutions for advertisers and publishers.

20. Defendant Mellenial Media ("Mellenial") is a Delaware corporation with is principal place of business in Baltimore, MD. Mellennial Media is an advertising content pro-

vider for mobile devices purporting to reach over 90 million unique mobile devices each month.

21. Defendant AdMarval, Inc. ("AdMarval") is a Delaware corporation with its principal place of business in San Mateo, California. AdMarval is a mobile advertising provider that partners with other advertising networks to provide mobile advertising content to mobile devices.

22. Defendant Quattro Wireless, Inc., ("Quattro") has its principal place of business in Waltham, MA. Quattro is a mobile advertising company purchased by Apple in January 2010 for $300 million.

23. The defendants named above in paragraphs 15 through 22 collect personal information transmitted from users' iDevices in order to either distribute or display advertisements to users or provide metrics and analytics services used by third-party app developers and online ad networks to track and measure user activity and are collectively referred to in this complaint as the "Tracking Defendants."

III. JURISDICTION AND VENUE

24. This Court has subject-matter jurisdiction over this action pursuant to Title 28, United States Code, Section 1331 and pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. Sections 1332(a) and (d), because the amount in controversy exceeds $5,000,000.00 exclusive of interest and costs, and more than two thirds of the members of the Class are citizens of states different from those of Defendants.

25. Venue is proper in this District under Title 28, United States Code, Section 1391(b) because Defendants' improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district. Five of the defendants are California corporations with their principal places of business in this district.

IV. ALLEGATIONS OF FACT

A. The Sale and Use of iDevices

26. Since Apple launched its mobile device business, it has sought to completely control the user experience by controlling all facets of the mobile environment and has differ-

entiated itself in the marketplace by advertising that it provides its customers a tightly integrated user experience. With this control comes responsibility, as acknowledged by Steve Jobs, Apple's founder and CEO, when he stated, "Our job is to take responsibility for the complete user experience. And if it's not up to par, it's our fault, plain and simple."

27. Apple's responsibility for the complete user experience begins with the consumers' purchase of a device designed and manufactured by Apple, and that works the way Apple wants it to work. Only Apple's iDevices may be licensed to use its iOS software. To date, almost 200 million iDevices have been sold worldwide.

28. Apple began marketing the iPhone mobile telephone on January 9, 2007, selling more than 108 million iPhones as of March 2011.

29. Similar to an iPhone but without cellular connectivity, the iPod Touch was marketed as a portable media player, personal digital assistant, and WIFI mobile platform that included the ability to run apps on the iOS operating system. Apple has sold 60 million iPod Touch units as of March 2011.

30. Apple subsequently introduced the iPad portable tablet computer, used primarily by users to view and listen to audio-visual and music content, play electronic games, and access the Internet. Apple has sold 19 million iPads as of March 2011.

31. The iPhone, iPad, and iPod Touch devices are designed by Apple, manufactured to Apple's specifications, and sold exclusively under the Apple brand.

32. The iDevices are mobile devices that are computers that operate using the iPhone operating system software known as iOS.

33. The iDevices utilize wireless access technology in the form of WIFI, GSM or CDMA protocols to access the Internet.

B. Apple Controls Distribution of Apps for iDevices

34. The iDevices enable the user to download apps that utilize an iDevice's Internet communications capability.

35. Apps may only be obtained from Apple's App Store application and website. Apple owns, controls, and operates the App Store, which it launched on July 10, 2008. As of

March 2011, consumers had downloaded 10 billion apps from the App Store. From the App Store, owners of an iDevice can purchase and install the software applications that are referred to herein as "apps."

36. Apple represents to every user of the App Store, pursuant to a click-through agreement requried to create a user App Store account: "Apple takes precautions — including administrative, technical, and physical measures — to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction."

37. Apple mobile devices and apps are now used by many consumers in almost all facets of their daily lives, for choosing restaurants or movies, making travel arrangements, conducting banking transactions, reading books and periodicals, and for many other purposes.

38. Apple has sought to make the App Store the exclusive marketplace for the purchase of software applications for iDevices. Apple has also sought to exercise tight control over what apps may be offered by the App Store. No developer is permitted to sell an app in the App Store without entering into Apple's form iOS Developer Agreement. Apple trades on its control of the App Store, claiming to offer only apps that it has reviewed and found safe and appropriate. Every app in the App Store, whether free or paid, must be approved by Apple and digitally signed by Apple. Apple has specifically represented to consumers that the App Store does not permit apps that "violate[] our developer guidelines" including apps containing pornography, apps that violate a users privacy, and apps that hog bandwidth.

39. Numerous apps available from the App Store are created by third-party developers. There are several hundred thousand third-party apps available at the App Store. Some of these are ostensibly free and some are sold for a fee. Apple distributes approved free apps through the App Store without charging the developer a fee. Apple also distributes approved apps for which the consumer is charged a price set by the developer; Apple collects the payment price through its revenue collection mechanism and retains 30 percent of the payment as its fee. Third-party apps include applications for business use, such as contact management and business expense tracking; personal finance use, such as trading; media, such as news outlets;

education, such as childbirth education and children's math learning; and entertainment, such as movie reviews and electronic games.

40. Other apps available from the App Store are developed by Apple, some of which are free to consumers and some of which are sold.

41. Apple exercises tight control over the types of apps it allows into the App Store. Whether an app is allowed to be sold in the App Store is completely at the discretion of Apple. Apple requires that proposed apps go through a rigorous approval process. Even if an app meets the "Program" requirements (as Apple describes it), the app can still be rejected by Apple for any reason at all. It is estimated that approximately 20 percent of all third-parties' requests to place their apps for sale in the App Store are rejected by Apple.

42. iDevice users are only allowed to download software specifically licensed by Apple and available on the iDevice out of the box or through the App Store. If a user installs any software not approved by Apple, the users' warranty is voided. When a user installs Apple's updates to the iDevice operating system, Apple takes the opportunity to erase any non-licensed software on the device. Apple claims this control is necessary to ensure the "tightly integrated," smooth functioning of the iDevice.

43. Even after a user downloads an approved app, Apple maintains control by requiring that the end-user license agreement for every third-party app include a clause giving Apple the ability to step into the shoes of the app developer and sue the end-user. Specifically, the iOS Developer Agreement states:

> **9. Third Party Beneficiary:** You and the end-user must acknowledge and agree that Apple, and Apple's subsidiaries, are third party beneficiaries of the EULA, and that, upon the end-user's acceptance of the terms and conditions of the EULA, Apple will have the right (and will be deemed to have accepted the right) to enforce the EULA against the end-user as a third party beneficiary thereof.

C. Apple Controls the Development Process for Apps Available on iDevices

44. In addition to controlling the characteristics and distribution of apps, described above, Apple exercises substantial control over their development and functionality.

45. A third party who wants to sell an App from the Apple App Store is required to

pay to enroll in the iPhone Developer Program.

46. The third party must also agree to the terms of Apple's iPhone Developer Program License Agreement ("iOS Developer Agreement"). The iOS is, by its terms, confidential, and prohibits the third party from making any public statements about the agreement, its terms and conditions, or the third party's relationship with Apple without Apple's prior written approval.

47. The third party must code the app using Apple's Software Development Kit software (SDK), which can only be installed on an Apple computer. An App developed using Apple's SDK will only function on iDevices and can only interact with the iDevice operating system and features in the ways permitted by the iOS Developer Agreement and SDK.

48. In April of 2010, Apple amended its Developer Agreement purporting to ban apps from sending data to third-parties except for information directly necessary for the functionality of the App. Apple's revised Developer Agreement provides that "the use of third party software in Your Application to collect and send Device Data to a third party for processing or analysis is expressly prohibited."

D. Apple Has Failed To Use Its Control Over The iDevice, the Marketing of the Apps and the Programming of the Apps to Protect User Privacy and the Security of User Data.

49. As discussed above, Apple's control of the user experience includes restrictions, such as blocking consumers from modifying devices or installing non-App-store, and blocking developers and researchers from publicly discussing Apple's standards for app development, and even prohibiting researchers from analyzing and publicly discussing device shortcomings such privacy flaws.

50. As a direct consequence of the control exercised by Apple, plaintiffs and the Class cannot reasonably review the privacy effects of apps and must rely on Apple to fulfill its duty to do so.

51. Apple represents that it undertakes such a duty, representing that it reviews all apps available in its App Store and that it retains broad discretion to remove an App from the App Store.

52. A third party cannot upload an App for sale in the App Store until Apple digitally signs the App, thereby giving its approval for sale of the App through the App store.

53. Apple represents that an app may not access information from or about the user stored on the user's iDevice unless the information is necessary for the advertised functioning of the App.

54. Apple represents that it does not allow one app to access data stored by another App.

55. Apple represents that it does not allow an app to transmit data from a user's iDevice to other parties without the user's consent.

56. Apple does not review app source code, *i.e.* it does not review the code written by the developer in a programming language to inspect for that acquires users' personal information without the users' knowledge. Instead, Apple only reviews the executable file for the App, *i.e.*, the binary code that is executed by the iOS when the App is running. Thus, Apple's policy of reviewing only app executable files permits apps that subject consumers to privacy exploits and security vulnerabilities to be offered in the App Store.

57. Contrary to Apple's representations to consumers, Apple does not analyze the traffic generated by apps to detect apps that violate the privacy terms of the iOS Developer Agreement and Apple's commitments to users.

58. Contrary to such representations, without any permission from a consumer, Apple's design of the iDevice allows application developers to build apps that can easily access the following personally identifiable information on a consumer's iDevice:

a. *address book*, which includes names, phone numbers, email addresses, physical addresses, stored by the user; each entry also includes a notes field utilized by many users to store their own sensitive access-control, passcode, and account information;

b. *cellphone number*;

c. *file system*, consisting of any data files stored on the device, which could include information such as recent web searches, video viewing history, email host and login information (although not password and not email message content);

d. *geolocation*: in the */Library/Application Support/MobileSync/Backups/* folder on a user's iDevice, Apple maintains an unencrypted log of the user's movements, as often as 100 times a day, for up to a one-year period; Apple logs a user's geolocations even if the user has disabled the iDevice's GPS features, apparently by using cell transmitter tower signals to triangulate the user's location; Apple replicates this file on any computer with which the user synchs an iDevice;

e. *International Mobile Subscriber Identity (IMSI),* which remains unchanged even when a user changes devices and which reveals the user's country and mobile operator.

f. *keyboard cache*, which is a log of keystrokes intended to facilitate autocompletion assistance to the user, but which also includes any personal and confidential information the user types into the device;

g. *photographs*, which, by default, are stored with date and GPS coordinate information;

h. *SIM card serial number* (ICCID); and

i. *universally unique device identifier (UUID),* which Apple refers to as a *unique device identifier (UDID)*, a number that uniquely identifies the particular iDevice.

59. Nothing in the click-through agreement required App Store users would put a reasonable consumer on notice of the mechanism and manner by which the iDevice and apps allow users to be tracked and have their personal information shared.

60. For example, Apple understands the significance of identifiers such as its UDID in regards to users' privacy, as, internally, Apple claims that it treats UDID information as "personally identifiable information" because, if combined with other information, such as other information easily available on the iDevice, it can be used to personally identify a user. Further, the UDID is g*lobally* unique—no other device bears the same identifying number.

E. The Tracking Defendants Exploit the Access to Consumer Data That Apple Permits and By Doing So Create Additional Financial Incentives For Application Developers To Provide Additional Free and Paid Apps to iDevice Users Through the App Store

61. Notwithstanding Apple's control of the user experience, it designs its mobile devices to be very open when it comes to disclosing information about consumers to the Tracking Defendants, companies that incentivize application developers to provide the App Store with free apps for iDevices and provide Apple the metrics to support its claims of market leadership.

62. The personal and private information is of extreme interest to many advertising networks and web analytics companies, including the Tracking Defendants. For this reason, the Tracking Defendants pay to support app development, so that many apps are provided to consumers ostensibly "free" or at a lower cost.

63. When users download and install the apps on their iDevices, the Tracking Defendants' code accesses personal information on those devices without users' awareness or permission and transmits the information to the Tracking Defendants, supplying them with details such as consumers' cellphone numbers, address books, unique device identifiers, and geolocation histories—highly personal details about who the consumers are, who they know, what they do, and where they are.

64. Some Tracking Defendants pay app developers to include code that causes banner ads to be displayed when users run the apps. Those ads are then populated with content from the Tracking Defendants and provide the communications channel for the Tracking Defendants to acquire and upload users' personal information.

65. Prior to Apple's January 2010 acquisition of mobile advertising company, Quattro Wireless Network, Apple removed several apps from the App Store based on concerns over user privacy violations. These apps included: Aurora Feint, because it uploaded the consumers' contacts to the developer's server; MogoRoad, because of user complaints of unauthorized telephone calls from the developers' sales personnel; Storm8, because it harvested consumers' cellphone numbers and uploaded them without encryption; and Pinch Media, an analytics

framework for developers, because of its unauthorized collection of personal data and tracking.

66. In the wake of Apple's prohibition against sending user information to third parties (described above, paragraph 48), protests erupted from a number of third-party advertising networks and metrics/analytics companies (who have been receiving a steady flow of user data from iDevice and iPad apps). One prominent critic was the CEO of Google-owned AdMob. Following this criticism, Apple has taken no steps to actually implement its changed Developer Agreement or enforce it in any meaningful way.

67. As a result, the Tracking Defendants, through the apps with whom they had entered into relationships and to whom they had provided code, have continued to acquire details about consumers and to track consumers on an ongoing basis, across numerous applications, and tracking consumers when they accessed applications from different mobile devices.

68. With the personal information acquired, the Tracking Defendants used the information to compile—in addition to the types of information listed in paragraph 58, above—personal, private, and sensitive information that included consumers' video application viewing choices, web browsing activities, and their and personal characteristics such as gender, age, race, family status, education level, geographic location, and household income, even though the Tracking Defendants require none of this information to provide the user services for which they were marketed.

69. The Tracking Defendants acquired personal information and compiled profiles that were unnecessary to the apps' stated functions but were useful to the Tracking Defendants in their commercial compilation, use, and sale of consumers' personal information.

70. Because of Apple's and the Tracking Defendants' control and coding, consumers are unable to detect, manage, or avoid this collection and transmittal of information.

71. Apple is aware that apps are providing a conduit for the Tracking Defendants to acquire consumers' personal information with consumers' knowledge or consent.

72. However, because consumers are unaware of the Tracking Defendants, they cannot complain to Apple about particular apps and request that Apple remove the apps from the App Store.

73. Apple has continued to allow app developers to run their apps on its iOS platform and failed to void the licensing agreements application developers, even after it received notice of Tracking Defendants' practices.

F. Privacy Interests and Consent

74. Plaintiffs in this action consider the information from and about themselves on their iDevices to be personal and private information.

75. Consumers using iDevices that download apps from the App Store would reasonably consider information from and about themselves stored on their iDevices to be personal and private information that they would not expected to be collected and used by third parties without the consumers' express consent.

76. Plaintiffs did not expect, receive notice of, or consent to the Tracking Defendants tracking of their App use. Plaintiffs did not expect, receive notice of, or consent to the Tracking Defendants acquisition of Plaintiffs' personally identifiable information.

77. The Tracking Defendants activities were in conflict with the privacy policies and/or terms of use of the Apple App store.

78. The Tracking Defendants actions exceeded the scope of any authorization that could have been granted by Plaintiffs at the time of downloading and using apps.

79. Plaintiffs consider information about their mobile communications to be in the nature of confidential information.

80. Plaintiffs consider information about any website they visit, or apps they download, to be in the nature of confidential information that they do not expect to be shared with an unaffiliated company.

81. The Tracking Defendants sell users' personal information to, or purchase and merge with user's personal information, other personal information about the same users that is available in the commercial, secondary information market, which the traffickers take substantial efforts to shield from the public eye. The Tracking Defendants and other parties to the information market use the merger of personal information to effectively or actually de-anonymize consumers.

82. Plaintiffs did not consent to being personally identified to the Tracking Defendants or for their personally identifiable information to be shared with and used on behalf of the Tracking Defendants.

83. The Tracking Defendants actions were knowing, surreptitious, and without notice and so were conducted without authorization and exceeding authorization.

84. The Tracking Defendants misappropriated Plaintiffs' personal information.

85. Consumers routinely engage in online economic exchanges with the websites they visit by exchanging their personal information for the websites' content and services, thereby reducing the costs consumers would otherwise have to pay. The transactions are value-for-value exchanges. This value-for-value exchange takes place particularly when an app is supported by advertising revenue, such as revenue the Tracking Defendants pay app developers.

86. Because, as alleged herein, the Tracking Defendants engaged in undisclosed and inadequately disclosed data collection from consumers, those consumers did not receive the full value of their exchanges. In essence, Tracking Defendants raised the price consumers paid to use the app but, instead of telling consumers or the website, Tracking Defendants simply reach around (or through) the website and into consumers' pockets, extracting their undisclosed premium in the form of consumers' information.

87. Because Tracking Defendants imposed an undisclosed cost on consumers, by taking more information than they were entitled to take, Tracking Defendants' practices imposed economic costs on consumers.

88. The scarcity of consumer information increases its value. The Tracking Defendants devalued consumers' information by taking and propagating it.

89. The undisclosed privacy and information transfer consequences of Tracking Defendants' practices imposed costs on consumers in the form of the loss of the opportunity to have entered into value-for-value exchanges with other app providers whose business practices better conformed to consumers' expectations. Thus, the Tracking Defendants' failure adequately to disclose the information practices and using their lack of disclosure as a cover for

taking consumers' information, the Tracking Defendants imposed opportunity costs on consumers.

90. Likewise, Tracking Defendants' lack of disclosure coupled with their taking of information imposed costs on consumers who would otherwise have exercised their rights to utilize the economic value of their information by declining to exchange it with Tracking Defendants or any other app provider.

91. Consumers' information, which they use as an asset of economic value in the ways described above, has discernable value as an asset in the information marketplace, where consumers may market their own information.

92. The Tracking Defendants' conduct alleged in this complaint constituted an ongoing course of conduct that harmed Plaintiff and consumers in general, and caused them to incur financial losses.

93. The Tracking Defendants deprived Plaintiffs of and/or diminished the economic value of their personal information.

94. The Tracking Defendants used Plaintiffs' personal information for their own economic benefit.

95. Plaintiffs' experiences are typical of the experiences of Class Members.

96. The aggregated loss and damage sustained by the Class, as defined herein, includes economic loss with an aggregated value of at least $5,000 during a one-year period.

97. The Tracking Defendants perpetrated the acts and omissions set forth in this complaint through an organized campaign of deployment, which constituted a single act.

98. Plaintiffs and Class Members have been harmed by the Tracking Defendants deceptive acquisition of their personal information in the loss of their rights to use, share, and maintain the confidentiality of their information, each according to his or her own discretion.

V. CLASS ALLEGATIONS

99. Pursuant to the Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a class action on behalf of themselves and all others similarly situated as members of the Class, defined as follows:

> All persons residing in the United States who have downloaded software from the App Store on a mobile device that runs Apple's iOS, (iPhone, iPad and/or iPod Touch), from December 1, 2008 to the date of the filing of this Complaint.

100. Excluded from the Class are Defendants, their legal representatives, assigns, and successors, and any entities in which Defendants have controlling interests. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

101. The "Class Period" is December 1, 2008 to the present.

102. Plaintiffs reserve the right to revise this definition of the Class based on facts learned in the course of litigating this matter.

103. The Class consists of millions of individuals and other entities, making joinder impractical.

104. The claims of Plaintiffs are typical of the claims of all other Class Members.

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

106. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

107. 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.

108. Defendants have acted and failed to act on grounds generally applicable to Plaintiffs and other Class Members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members.

109. The factual and legal bases of Defendants' liability to Plaintiff and other Class Members are the same, resulting in injury to Plaintiff and all of the other Class Members. Plain-

tiff and other Class Members have all suffered harm and damages as a result of Defendants' wrongful conduct.

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

a. whether Defendants, without authorization, tracked and compiled information to which Class Members enjoyed rights of possession superior to those of Defendants;

b. whether Defendants, without authorization, created personally identifiable profiles of Class Members;

c. Whether Defendants violated the statutes and common laws alleged herein;

d. Whether Defendants misappropriated valuable information assets of Class Members;

e. Whether Defendants caused economic harm to Class Members;

f. Whether Apple violated its own Terms and Privacy Policies by sharing and causing to be shared Plaintiffs' personal information with Tracking Defendants;

g. Whether Defendants created or caused or facilitated the creation of personally identifiable consumer profiles of Class Members;

h. Whether Defendants continue to retain and/or sell, valuable information assets from and about Class Members;

i. What uses of such information were exercised and continue to be exercised by Defendants;

j. Whether Defendants breached their contracts, and if so, the appropriate measure of damages and remedies against Defendants for such breaches;

k. Whether Defendants invaded and caused the invasion of the privacy of Class Members; and

l. Whether Defendants have been unjustly enriched.

111. The questions of law and fact common to Class Members predominate over any

questions affecting only individual members, and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

VI. CLAIMS FOR RELIEF

112. Based on the foregoing allegations, Plaintiffs' claims for relief include the following:

FIRST CLAIM FOR RELIEF

Negligence, as to Defendant Apple

113. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

114. As set forth above, Apple owed a duty to Plaintiffs and Class Members.

115. Apple breached its duty by designing iDevices so that the Tracking Defendants could acquire personal information without consumers' knowledge or permission, by failing to review and remove privacy-violating apps from the App Store, and by constructing and controlling consumers' user experience and mobile environment so that consumers could not reasonably avoid such privacy-affecting actions.

116. Apple failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiff and Class Members' personal information, privacy rights, and security.

117. Apple's failure to fulfill its commitments included Apple's practice of capturing frequent and detailed information about iDevice users' locations for up to one year, including the locations of iDevice users who had utilized Apple's prescribed functioning for disabling Global Positioning System services, maintaining records of such location histories on users' iDevices, transferring such location history files to users' replacement iDevices, transferring such location history files to other computers with which users synchronized their iDevices, and storing such location history files in accessible, unencrypted form, without providing notice to users or obtaining users' consent, and where consumers had no reasonable means to become aware of such practice or to manage it, and where such practice placed users at unreasonable risk of capture and misuse of such highly detailed and personal information, and where a reasonable consumer would consider such a practice unexpected, objectionable, and shocking to

the conscience of a reasonable person.

118. Apple's unencrypted storage on iDevices and computers with which they were synchronized the information described in paragraph 118, above, was negligent.

119. Plaintiffs and Class Members were harmed as a result of Apples breaches of its duty, and Apple proximately caused such harms.

SECOND CLAIM FOR RELIEF

Violations of the Computer Fraud and Abuse Act, 18 U.S.C § 1030, *et seq.*

as to All Defendants

120. Plaintiffs incorporates the above allegations by reference as if fully set forth herein.

121. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

122. Tracking Defendants violated 18 U.S.C. 1030 by intentionally accessing Plaintiffs' and Class Members' iDevices without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

123. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA."

124. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

125. Apple violated the CFAA in that it caused the transmission to users' iDevices, either by native installation or iOs upgrade, of code that caused users' iDevices to maintain, synchronize, and retain detailed, unencrypted location history files.

126. Each of Plaintiffs and Class Members' mobile devices is a "protected computer

. . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

127. The Tracking Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command to be downloaded to Plaintiffs' Apple mobile devices, which are protected computers as defined above.

128. The Tracking Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs' and Class Members' protected Apple mobile devices without authorization, and as a result of such conduct, recklessly caused damage to Plaintiffs' and Class Members Apple mobile devices by impairing the integrity of data and/or system and/or information.

129. The Tracking Defendants violated 18 U.S.C. § 1030 (a)(5)(A)(iii) by intentionally accessing Plaintiffs' and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

130. Plaintiffs and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

131. Plaintiffs and Class Members have suffered loss by reason of these violations, as defined in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

132. Plaintiffs and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

133. Apple and the Tracking Defendants are jointly and severally liable for the violations of the Computer Fraud and Abuse Act alleged herein.

134. As a result of these takings, Tracking Defendants' conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

135. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, the right of privacy.

136. Tracking Defendants' unlawful access to Plaintiffs' and Class Members' computers and electronic communications has caused Plaintiffs and Class Members irreparable injury. Unless restrained and enjoined, Tracking Defendants will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

137. Each Defendant is jointly and severally liable for the conduct alleged hereunder of any other Defendants and/or Defendants.

THIRD CLAIM FOR RELIEF

Violations of the Computer Crime Law, California Penal Code § 502, *et seq.*

as to All Defendants

138. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

139. The Tracking Defendants violated California Penal Code § 502 by knowingly accessing, copying, using, made use of, interfering, and/or altering, data belonging to Plaintiffs and Class Members.

140. Apple violated California Penal Code § 502 in that it caused the transmission to users' iDevices, either by native installation or iOs upgrade, of code, that caused users' iDevices to maintain, synchronize, and retain detailed, unencrypted location history files.

141. The Tracking Defendants violated California Penal Code section 502(c)(1) by knowingly accessing and without permission altering and making use of data from Plaintiffs' and Class Members' computers in order to devise and execute business practices to deceive Plaintiffs and Class Members into surrendering private electronic communications and activities for Defendants' financial gain, and to wrongfully obtain valuable private data from Plaintiffs.

142. The Tracking Defendants violated California Penal Code section 502(c)(2) by knowingly accessing and without permission taking, or making use of data from Plaintiffs' and

Class Members' computers.

143. Tracking Defendants violated California Penal Code section 502(c)(3) by knowingly and without permission using and causing to be used Plaintiffs' and Class Members' computer services.

144. Tracking Defendants violated California Penal Code section 502(c)(4) by knowingly accessing and, without permission, adding and/or altering the data from Plaintiffs' and Class Members' computers, that is, application code installed on such computers.

145. Tracking Defendants violated California Penal Code section 502(c)(5) by knowingly and without permission disrupting or causing the disruption of Plaintiffs' and Class Members' computer services or denying or causing the denial of computer services to Plaintiffs and the Class.

146. Tracking Defendants violated California Penal Code section 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' computers, computer system, and/or computer network.

147. Tracking Defendants violated California Penal Code section 502(c)(7) by knowingly and without permission accessing or causing to be accessed Plaintiffs and Class Members' computers, computer systems, and/or computer networks.

148. Tracking Defendants violated California Penal Code section 502(c)(8) by knowingly introducing a computer contaminant into the Plaintiffs' and Class Members' computers, computer systems, and/or computer networks, and doing so to obtain data from Plaintiffs' and Class Members iDevices.

149. Plaintiffs and Class Members have also suffered irreparable injury from these unauthorized acts of disclosure in that their information has been harvested, retained, and used by Tracking Defendants, and which information continues to be retained and used by Tracking Defendants; due to the continuing threat of such injury and, in addition, the threat that Tracking Defendants will transfer Plaintiffs and Class Members' information to yet other third parties, Plaintiffs and Class Members have no adequate remedy at law, entitling them to injunctive relief.

150. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

151. As a direct and proximate result of Tracking Defendants' unlawful conduct within the meaning of California Penal Code section 502, Tracking Defendants have caused loss to Plaintiffs and Class Members in an amount to be proven at trial. Plaintiffs and Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code section 502(e).

152. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

153. Plaintiffs and Class Members have suffered irreparable and incalculable harm and injuries from Tracking Defendants' violations. The harm will continue unless Tracking Defendants are enjoined from further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

154. Further, such harms will continue unless Defendant Apple is enjoined from providing iDevices and apps and engaging in business practices in the App Store that facilitate Tracking Defendants' wrongful acts.

155. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code section 502(e)(4) because Tracking Defendants's violation were willful and, on information and belief, Tracking Defendants is guilty of oppression, fraud, or malice as defined in Cal. Civil Code section 3294.

156. Tracking Defendants' unlawful access to Plaintiffs' and Class Members' computers and electronic communications has caused them irreparable injury. Unless restrained and enjoined, Tracking Defendants will continue to commit such acts. Plaintiffs and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs and Class Members to remedies including injunctive relief as provided by California Penal Code section 502(e).

157. Each Defendant is jointly and severally liable for the conduct alleged hereunder of any other Defendants and/or Defendants.

FOURTH CLAIM FOR RELIEF

Trespass to Chattel, as to All Defendants

158. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

159. The common law prohibits the intentional intermeddling with personal property, including a iDevice, in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

160. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiffs and Class Members, Defendants dispossessed Plaintiffs and Class Members from use and/or access to their iDevices, or parts of them, by obfuscating iDevice functions and the execution of privacy-affecting code. Further, these acts impaired the use, value, and quality of Plaintiffs and Class Members' iDevices. Defendants' acts constituted an intentional interference with the use and enjoyment of the iDevices. By the acts described above, Defendants repeatedly and persistently engaged in trespass to personal property in violation of the common law.

161. Without Plaintiffs and Class Members' consent, or in excess of any consent given, Defendants knowingly and intentionally accessed and/or caused the access to Plaintiffs' and Class Members' property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property and causing injury to Plaintiffs and the members of the Class.

162. Defendants engaged in deception and concealment to gain access to Plaintiffs and Class Members' iDevices.

163. Defendants engaged in the following conduct with respect to Plaintiffs and Class Members' iDevices: Defendants accessed and obtained control over iDevices; Defendants caused the installation of code on the hard drives of the iDevices; Defendants programmed the operation of its code to circumvent the iDevice owners' privacy and security controls, to remain beyond their control, and to continue function and operate without notice to them or consent from Plaintiff and Class Members.

164. All these acts described above were acts in excess of any authority any user

granted when visiting websites and none of these acts was in furtherance of users' uses of iDevices or apps. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and Class Members may have granted to the Defendants did not apply to Defendants's conduct.

165. Defendants's installation and operation of its program used, interfered, and/or intermeddled with Plaintiffs' and Class Members' iDevice systems. Such use, interference and/or intermeddling was without Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class Members' consent.

166. Defendants's installation and operation of its program constitutes trespass, nuisance, and an interference with Class Members' chattels, to wit, their iDevices.

167. Defendants's installation and operation of its program impaired the condition and value of Class Members' iDevices.

168. Defendants trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and Class Members.

169. As a direct and proximate result of Defendants's trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiffs and Class Members' property, Defendants has injured and impaired in the condition and value of Class Members' iDevices, as follows:

170. by consuming the resources of and/or degrading the performance of Plaintiffs' and Class Members' iDevices (including hard drive space, memory, processing cycles, and Internet connectivity);

171. by diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiffs' and Class Members' iDevices;

172. by devaluing, interfering with, and/or diminishing Plaintiffs' and Class Members' possessory interest in their iDevices;

173. by altering and controlling the functioning of Plaintiffs' and Class Members' iDevices;

174. by infringing on Plaintiffs' and Class Members' right to exclude others from

their iDevices;

175. by infringing on Plaintiffs' and Class Members' right to determine, as owners of their iDevices, which program functionality should be installed and operating on their iDevices;

176. by compromising the integrity, security, and ownership of Class Members' iDevices; and

177. by forcing Plaintiffs' and Class Members' to expend money, time, and resources in order to remove the program installed on their iDevices without notice or consent.

178. Each Defendant is jointly and severally liable for the conduct alleged hereunder of any other Defendants and/or Defendants.

FIFTH CLAIM FOR RELIEF

Violations of the Consumer Legal Remedies Act, California Civil Code § 1750, *et seq.* as to Defendant Apple

179. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

180. In violation of Civil Code section 1750, et seq. (the "CLRA"), Defendant Apple has engaged and is engaging in unfair and deceptive acts and practices in the course of transactions with Plaintiffs, and such transactions are intended to and have resulted in the sales of services to consumers. Plaintiffs and the Class Members are "consumers" as that term is used in the CLRA because they sought or acquired Defendant's good or services for personal, family, or household purposes, including Apple's iDevices. Defendant's past and ongoing acts and practices include but are not limited to Defendant's representation that is goods or services were of a particular standard, quality, and grade when in fact, they were of another; in particular, Apple purported to control the user experience in using the iDevices so that users could reasonably expect Apple to take responsibility for protecting their privacy and security when using the iDevice, including use of the iDevice with apps downloaded from the App Store.

181. Defendant's violations of Civil Code § 1770 have caused damage to Plaintiffs and the other Class Members and threaten additional injury if the violations continue. This damage includes the privacy and economic consequences set forth above.

182. Plaintiffs assert that their first complaint filings constituted fulfillment of their

notification burden under section 1782 and that Defendant has not adequately responded within the required 30 days, and Plaintiffs therefore request all relief to which they are justly entitled under Civil Code, Section 1780, in an amount to be determined at trial.

SIXTH CLAIM FOR RELIEF

Violations of the Unfair Competition Law (UCL)

California Business and Professions Code § 17200, *et seq.*

as to All Defendants

183. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

184. In violation of California Business and Professions Code, Section 17200 *et seq.*, Defendants' conduct in this regard is ongoing and includes, but is not limited to, statements made by Defendants and Defendants' omissions, including Apple's privacy and security commitments and all Defendants' failure to disclosure their business conduct, and as otherwise set forth above.

185. By engaging in the above-described acts and practices, Defendants have committed one or more acts of unfair competition within the meaning of the Unfair Competition Law and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and property—specifically, personal information; the private and secure use of the iDevices and apps; and the opportunity cost of having installed and used Apple's iDevices and software.

A. Unlawful Business Act and Practices

186. Defendants' business acts and practices are unlawful, in part, because they violate California Business and Professions Code, Section 17500, *et seq.*, which prohibits false advertising, in that they were untrue and misleading statements relating to Defendants' performance of services and provision of goods and with the intent to induce consumers to enter into obligations relating to such services, and regarding which statements Defendants knew or which, and by the exercise of reasonable care Defendants should have known, were untrue and misleading.

187. Defendants' business acts and practices are also unlawful in that, as set forth herein, they violate the Consumer Legal Remedies Act, California Civil Code, Section 1750, *et*

seq.; the Computer Crimes Law, California Penal Code, Section 502, *et seq.*; False Advertising, California Business and Professions Code, Section 17500; and the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030, *et. seq.*

188. Defendants' business acts and practices are also unlawful in that they violate the California Constitution, Article I, Section 1, which articulates the inalienable right to pursue and obtain privacy, in that Defendants interfered with and obstructed users' rights and reasonable expectations regarding their privacy, particularly in light of promises by Defendants as an inducement for users to purchase iDevices and download apps.

189. Defendants are therefore in violation of the unlawful prong of the Unfair Competition Law.

B. Unfair Business Act and Practices

190. Defendants' business acts and practices are unfair because they have caused harm and injury-in-fact to Plaintiff and Class Members and for which Defendants have no justification other than to increase, beyond what Defendants would have otherwise realized, its information assets supportive of its advertising revenue.

191. Defendants' conduct lacks reasonable and legitimate justification in that Defendants have benefited from such conduct and practices while Plaintiff and the Class members have been misled as to the nature and integrity of Defendants' products and services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendants' conduct offends public policy in California tethered to the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes' recognition of the need for consumers to be information and equipped to protect their own privacy interests, such as California Civil Code, Section 1798.8, such that consumers may make informed decisions in their choices of merchants and other means of safeguarding their privacy.

192. In addition, Defendants' *modus operandi* constitutes a sharp practice in that Defendants knew and should have known that consumers care about the status of personal information and privacy but are unlikely to be aware of and able to detect the means by which De-

fendants were conducting themselves in a manner adverse to their commitments and users' interests, through the undisclosed functions of iDevices and apps and the related conduct of the Tracking Defendants. Defendants are therefore in violation of the unfairness prong of the Unfair Competition Law.

193. Defendants' acts and practices were fraudulent within the meaning of the Unfair Competition Law because they were likely to mislead the members of the public to whom they were directed.

194. Apple's practice of capturing, storing, and transferring through synchronization to other computers highly detailed and personal records of users' location histories of long duration, and storing such information in unencrypted form, was in violation of the unfairness prong of the Unfair Competition Law.

195. Each Defendant is jointly and severally liable for the conduct alleged hereunder of any other Defendants and/or Defendants.

SEVENTH CLAIM FOR RELIEF

Breach of Implied Covenant of Good Faith and Fair Dealing

196. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs in this complaint.

197. As set forth above, Plaintiffs submit personal information to Apple and such information is stored on Plaintiffs' iDevices, and Apple promises in its Privacy Policy that it will not share this information with third-party advertisers or applications developers without Plaintiffs' consent, and the consent of each Class Member, respectively, and promises in its App Store click-through agreement to protect users' privacy.

198. A covenant of good faith and fair dealing, which imposes upon each party to a contract a duty of good faith and fair dealing in its performance, is implied in every contract, including their agreement in the transactions for acquisitions of iDevices and apps that embodies the relationship between Apple and its users.

199. Good faith and fair dealing is an element imposed by common law or statute as an element of every contract under the laws of every state. Under the covenant of good faith

and fair dealing, both parties to a contract impliedly promise not to violate the spirit of the bargain and not to intentionally do anything to injure the other party's right to receive the benefits of the contract.

200. Plaintiffs reasonably relied upon Apple to act in good faith with regard to the contract and in the methods and manner in which it carries out the contract terms. Bad faith can violate the spirit of their agreements and may be overt or may consist of inaction. Apple's inaction in failing to adequately notify Plaintiffs of the release of their personal information to the Tracking Defendants and application developers and depriving Plaintiffs of the means to become aware of such information taking evidences bad faith and ill motive.

201. The contract is a form contract, the terms of which Plaintiffs are deemed to have accepted once Plaintiffs and the Class signed up with Apple. The contract purports to give discretion to Apple relating to Apple's protection of users' privacy. Apple is subject to an obligation to exercise that discretion in good faith. The covenant of good faith and fair dealing is breached when a party to a contract uses discretion conferred by the contract to act dishonestly or to act outside of accepted commercial practices. Apple breached its implied covenant of good faith and fair dealing by exercising bad faith in using its discretionary rights to deliberately, routinely, and systematically make Plaintiffs' personal information available to third parties.

202. Plaintiffs have performed all, or substantially all, of the of the obligations imposed on them under contract, whereas Apple has acted in a manner as to evade the spirit of the contract, in particular by deliberately, routinely, and systematically without notifying Plaintiffs' of its disclosure of Plaintiffs' personal information to Tracking Defendants. Such actions represent a fundamental wrong that is clearly beyond the reasonable expectation of the parties. Apple's causing the disclosure of such information to the Tracking Defendants is not in accordance with the reasonable expectations of the parties and evidences a dishonest motive.

203. Apple's ill motive is further evidenced by its failure to obtain Plaintiffs' consent in data mining efforts while at the same time consciously and deliberately facilitating data mining to automatically and without notice provide user information the Tracking Defendants.

Apple profits from advertising revenues derived from its data mining efforts from Plaintiffs and the Class.

204. The obligation imposed by the implied covenant of good faith and fair dealing is an obligation to refrain from opportunistic behavior. Apple has breached the implied covenant of good faith and fair dealing in their agreement through its policies and practices as alleged herein. Plaintiffs and the Class have sustained damages and seek a determination that the policies and procedures of Apple are not consonant with Apple's implied duties of good faith and fair dealing.

205. Apple's capture, retention, and transfer through synchronization of uses' detailed location histories, even when such users had disable GPS services on their iDevices, and storing such location histories in unencrypted form, was a breach of the implied covenant of good faith and fair dealing

EIGHTH CLAIM FOR RELIEF

Unjust Enrichment, as to Tracking Defendants

206. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

207. Plaintiffs and the Class have conferred a benefit upon the Tracking Defendants which have, directly or indirectly, received and retained personal information of Plaintiffs and Class Members, as set forth herein. Defendants have received and retained information that is otherwise private, confidential, and not of public record, and/or have received revenue from the provision, use, and or trafficking in the sale of such information.

208. Defendants appreciate and/or have knowledge of said benefit.

209. Under principles of equity and good conscience, the Tracking Defendants should not be permitted to retain the information and/or revenue that they acquired by virtue of their unlawful conduct. All funds, revenue, and benefits received by them rightfully belong to Plaintiffs and the Class, which the Tracking Defendants have unjustly received as a result of their actions.

210. Plaintiffs and Class Members have no adequate remedy at law.

VII. DEMAND FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendants and that the Court may:

A. certify this case as a Class action on behalf of the Class defined above, appoint Plaintiff as Class representative, and appoint his counsel as Class counsel;

B. declare that Defendants' actions violate the statutes and common-law jurisprudence set forth above;

C. award injunctive and equitable relief as applicable to the Class *mutatis mutandis*, including:

i. prohibiting Defendants from engaging in the acts alleged above;

ii. requiring Defendants to provide reasonable notice and choice to consumers regarding Defendants' data collection, profiling, merger, and deanonymization activities;

iii. requiring Defendants to disgorge to Plaintiffs and Class Members or to whomever the Court deems appropriate all of Defendants' ill-gotten gains;

iv. requiring Defendants to delete all data from and about Plaintiffs and Class Members that it collected and/or acquired from third parties through the acts alleged above;

v. requiring Defendants to provide Plaintiffs and other Class Members reasonable means to decline, permanently, participation in Defendants' collection of data from and about them;

vi. enjoining Apple from acquiring, retaining, and transferring, whether in encrypted or unencrypted form, users' detailed location history;

vii. requiring Apple to seek express consent from Plaintiffs and other Class Members to capture, retain, and transfer location history information and, otherwise, to purge such information from all

resident systems and identify parties that have accessed such information on users' iDevices and synchronized devices;

viii. awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired by Defendants through the wrongful conduct alleged above; and

ix. ordering an accounting and constructive trust to be imposed on the data from and about Plaintiffs and Class Members and on funds or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;

D. award damages, including statutory damages where applicable, to Plaintiffs and Class Members in an amount to be determined at trial;

E. award restitution against Defendants for all money to which Plaintiffs and the Class are entitled in equity;

F. restrain, by preliminary and permanent injunction, Defendants, its officers, agents, servants, employees, and attorneys, and those participating with them in active concert, from identifying Plaintiffs and Class Members online, whether by personal or pseudonymous identifiers, and from monitoring, accessing, collecting, transmitting, and merging with data from other sources any information from or about Plaintiff and Class Members;

G. award Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees; pre- and post-judgment interest to the extent allowable; restitution; disgorgement and other equitable relief as the Court deems proper; compensatory damages sustained by Plaintiffs and the Class; statutory damages, including punitive damages; and permanent injunctive relief prohibiting Defendant from engaging in the conduct and practices complained of herein; and

for such other and further relief as this Court deems just and proper.

Date: April 20, 2011

Respectfully submitted,

KAMBERLAW, LLC

By: s/Scott A. Kamber

Scott A. Kamber (*pro hac vice*)
KAMBERLAW, LLC
Interim Class Counsel

SCOTT A. KAMBER (*pro hac vice*)
DAVID A. STAMPLEY (*pro hac vice*)
skamber@kamberlaw.com
dstampley@kamberlaw.com
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

DEBORAH KRAVITZ (SBN 275661)
(N.D. Cal. admission pending)
dkravitz@kamberlaw.com
KamberLaw, LLP
141 North St.
Healdsburg, California 95448
Telephone: (707) 820-4247
Facsimile: (212) 202-6364

AVI KREITENBERG (SBN 266571)
KAMBERLAW, LLP
1180 South Beverly Drive, Suite 601
Los Angeles, CA 90035
Telephone: (310) 400-1050
Facsimile: (310) 400-1056

Interim Class Counsel

RICHARD A. LOCKRIDGE
ROBERT K. SHELQUIST
rlockridge@locklaw.com
rshelquist@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401

Telephone: (612) 339-6900
Facsimile: (612) 339-0981

JEFF S. WESTERMAN
jwesterman@milberg.com
MILBERG LLP
One California Plaza
300 South Grand Avenue, Ste 3900
Los Angeles, California 90071
Telephone: (213) 617-1200
Facsimilie: (213) 617-1975

PETER E. SEIDMAN
ANDREI V. RADO
ANNE MARIE VU (Bar No. 238771)
pseidman@milberg.com
arado@milberg.com
avu@milberg.com
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

JEREMY WILSON
jeremy@wtlfirm.com
WILSON TROSCLAIR & LOVINS
302 N. Market Street, Suite 501
Dallas, Texas 75202
Telephone: (214) 430-1930

Plaintiffs' Executive Committee

WILLIAM AUDET
JONAS P. MANN
MICHAEL A. MCSHANE
AUDET & PARTNERS LLP
221 Main Street, Suite 1460
San Francisco, California 94105
Telephone: (415) 568-2555
Facsimile: (415) 568-2556

Plaintiffs' Liaison Counsel

JOSEPH H. MALLEY
malleylaw@gmail.com
LAW OFFICE OF JOSEPH H. MALLEY
1045 North Zang Blvd.
Dallas, Texas 75208
Telephone: (214) 943-6100

DAVID C. PARISI (SBN 162248)
SUZANNE HAVENS BECKMAN (SBN 188814)
dcparisi@parisihavens.com
shavens@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299
Facsimile: (818) 501-7852

NABIL MAJED NACHAWATI, II
mn@fnlawfirm.com
FEARS NACHAWATI
4925 Greenville Avenue, Suite 715
Dallas, Texas 75206
Telephone: (214) 890-0711
Facsimile: (214) 890-0712

MICHAEL R. REESE (Bar No. 206773)
KIM RICHMAN
mreese@reeserichman.com
krichman@reeserichman.com
REESE RICHMAN LLP
875 Avenue of the Americas, 18th Floor
New York, NY 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272

Counsel for Plaintiffs

JURY TRIAL DEMAND

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

Date: April 20, 2011

Respectfully submitted,

KAMBERLAW, LLC

By: s/Scott A. Kamber

Scott A. Kamber (*pro hac vice*)
KAMBERLAW, LLC
Interim Class Counsel

SCOTT A. KAMBER (*pro hac vice*)
DAVID A. STAMPLEY (*pro hac vice*)
skamber@kamberlaw.com
dstampley@kamberlaw.com
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

DEBORAH KRAVITZ (SBN 275661)
(N.D. Cal. admission pending)
dkravitz@kamberlaw.com
KamberLaw, LLP
141 North St.
Healdsburg, California 95448
Telephone: (707) 820-4247
Facsimile: (212) 202-6364

AVI KREITENBERG (SBN 266571)
KAMBERLAW, LLP
1180 South Beverly Drive, Suite 601
Los Angeles, CA 90035
Telephone: (310) 400-1050
Facsimile: (310) 400-1056

Interim Class Counsel

RICHARD A. LOCKRIDGE
ROBERT K. SHELQUIST
rlockridge@locklaw.com
rshelquist@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

JEFF S. WESTERMAN
jwesterman@milberg.com
MILBERG LLP
One California Plaza
300 South Grand Avenue, Ste 3900
Los Angeles, California 90071
Telephone: (213) 617-1200
Facsimilie: (213) 617-1975

PETER E. SEIDMAN
ANDREI V. RADO
ANNE MARIE VU (Bar No. 238771)
pseidman@milberg.com
arado@milberg.com
avu@milberg.com
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

JEREMY WILSON
jeremy@wtlfirm.com
WILSON TROSCLAIR & LOVINS
302 N. Market Street, Suite 501
Dallas, Texas 75202
Telephone: (214) 430-1930

Plaintiffs' Executive Committee

WILLIAM AUDET
JONAS P. MANN
MICHAEL A. MCSHANE
AUDET & PARTNERS LLP
221 Main Street, Suite 1460
San Francisco, California 94105

Telephone: (415) 568-2555
Facsimile: (415) 568-2556

Plaintiffs' Liaison Counsel

JOSEPH H. MALLEY
malleylaw@gmail.com
LAW OFFICE OF JOSEPH H. MALLEY
1045 North Zang Blvd.
Dallas, Texas 75208
Telephone: (214) 943-6100

DAVID C. PARISI (SBN 162248)
SUZANNE HAVENS BECKMAN (SBN 188814)
dcparisi@parisihavens.com
shavens@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299
Facsimile: (818) 501-7852

NABIL MAJED NACHAWATI, II
mn@fnlawfirm.com
FEARS NACHAWATI
4925 Greenville Avenue, Suite 715
Dallas, Texas 75206
Telephone: (214) 890-0711
Facsimile: (214) 890-0712

MICHAEL R. REESE (Bar No. 206773)
KIM RICHMAN
mreese@reeserichman.com
krichman@reeserichman.com
REESE RICHMAN LLP
875 Avenue of the Americas, 18th Floor
New York, NY 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I, David Stampley, an attorney, hereby certify that on April 21, 2011, I caused the above ***First Consolidated Complaint***, to be served by causing true and accurate copies of such documents to be electronically filed and transmitted to counsel of record through the Court's CM/ECF electronic filing system.

Date: April 21, 2011

Respectfully submitted,

KAMBERLAW, LLC

By: s/David A. Stampley