

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

6 *Interim Class Counsel*
 (Additional counsel listed on signature page)
 7

8 **UNITED STATES DISTRICT COURT**
NORTHERN DISTRICT OF CALIFORNIA
 9 **SAN JOSE DIVISION**

10)	CASE NO. 10-CV-05878-LHK
11)	JURY DEMAND
12)	FIRST CONSOLIDATED CLASS
13)	ACTION COMPLAINT FOR
14)	VIOLATIONS OF:
15)	1. NEGLIGENCE;
16)	2. COMPUTER FRAUD AND ABUSE
17)	ACT, 18 U.S.C. § 1030;
18)	3. COMPUTER CRIME LAW,
19)	CAL. PENAL CODE § 502
20)	4. TRESPASS TO CHATTEL;
21)	5. CONSUMER LEGAL REMEDIES ACT,
22)	CAL. CIV. CODE § 1750;
23)	6. UNFAIR COMPETITION,
24)	CAL. BUS. & PROF. CODE § 17200;
25)	7. BREACH OF IMPLIED COVENANT OF
26)	GOOD FAITH AND FAIR DEALING; and
27)	8. UNJUST ENRICHMENT
28)	

1 The persons designated below as plaintiffs (“Plaintiffs”), each on his or her own behalf
2 and, collectively, on behalf of all others similarly situated (the putative “Class”), make the fol-
3 lowing allegations based on their personal knowledge of their own acts and observations and,
4 otherwise, upon information and belief based on investigation of counsel.

5 I. NATURE OF THE CASE

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

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

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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’

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

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

14 II. PARTIES

15 A. Plaintiffs

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

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

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

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

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

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

1 the App Store during the Class Period.

2 **B. Defendant Apple**

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

6 **C. Tracking Defendants**

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

12 16. Defendant Flurry, Inc. (“Flurry”) is a Delaware corporation with its principal
13 place of business located in San Francisco, California. Flurry is an advertising content and ana-
14 lytics provider for mobile device applications.

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

19 18. Defendant Pinch Media, Inc. (“Pinch Media”) is a Delaware corporation with its
20 principal place of business located in Hoboken, New Jersey. Pinch Media provides mobile ad-
21 vertising analytics services and partners with ad networks to deliver mobile advertising to mo-
22 bile devices.

23 19. Defendant TrafficMarketplace.com. Inc. (“Trafficmarketplace.com”) is a Dela-
24 ware corporation with its principal place of business in El Segundo, CA. TrafficMarket-
25 place.com is a mobile advertising network that purports to provide advertising network solu-
26 tions for advertisers and publishers.

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

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

3 21. Defendant AdMarval, Inc. (“AdMarval”) is a Delaware corporation with its
4 principal place of business in San Mateo, California. AdMarval is a mobile advertising pro-
5 vider that partners with other advertising networks to provide mobile advertising content to
6 mobile devices.

7 22. Defendant Quattro Wireless, Inc., (“Quattro”) has its principal place of business
8 in Waltham, MA. Quattro is a mobile advertising company purchased by Apple in January
9 2010 for \$300 million.

10 23. The defendants named above in paragraphs 15 through 22 collect personal in-
11 formation transmitted from users’ iDevices in order to either distribute or display advertise-
12 ments to users or provide metrics and analytics services used by third-party app developers and
13 online ad networks to track and measure user activity and are collectively referred to in this
14 complaint as the “Tracking Defendants.”

15 III. JURISDICTION AND VENUE

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

21 25. Venue is proper in this District under Title 28, United States Code, Section
22 1391(b) because Defendants’ improper conduct alleged in this complaint occurred in, was di-
23 rected from, and/or emanated from this judicial district. Five of the defendants are California
24 corporations with their principal places of business in this district.

25 IV. ALLEGATIONS OF FACT

26 A. The Sale and Use of iDevices

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

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

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

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

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

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

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

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

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

24 **B. Apple Controls Distribution of Apps for iDevices**

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

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

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

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

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

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

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

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

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

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

11 42. iDevice users are only allowed to download software specifically licensed by
12 Apple and available on the iDevice out of the box or through the App Store. If a user installs
13 any software not approved by Apple, the users’ warranty is voided. When a user installs Ap-
14 ple’s updates to the iDevice operating system, Apple takes the opportunity to erase any non-
15 licensed software on the device. Apple claims this control is necessary to ensure the “tightly in-
16 tegrated,” smooth functioning of the iDevice.

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

21 **9. Third Party Beneficiary:** You and the end-user must acknowledge
22 and agree that Apple, and Apple's subsidiaries, are third party beneficiar-
23 ies of the EULA, and that, upon the end-user's acceptance of the terms
24 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.

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

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

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

1 pay to enroll in the iPhone Developer Program.

2 46. The third party must also agree to the terms of Apple's iPhone Developer Pro-
3 gram License Agreement ("iOS Developer Agreement"). The iOS is, by its terms, confidential,
4 and prohibits the third party from making any public statements about the agreement, its terms
5 and conditions, or the third party's relationship with Apple without Apple's prior written ap-
6 proval.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 b. *cellphone number*;

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

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

7 e. *International Mobile Subscriber Identity (IMSI)*, which remains un-
8 changed even when a user changes devices and which reveals the user’s country and mobile
9 operator.

10 f. *keyboard cache*, which is a log of keystrokes intended to facilitate auto-
11 completion assistance to the user, but which also includes any personal and confidential infor-
12 mation the user types into the device;

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

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

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

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

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

1 **E. The Tracking Defendants Exploit the Access to Consumer Data That Apple Per-**
2 **mits and By Doing So Create Additional Financial Incentives For Application De-**
3 **velopers To Provide Additional Free and Paid Apps to iDevice Users Through the**
4 **App Store**

5 61. Notwithstanding Apple’s control of the user experience, it designs its mobile
6 devices to be very open when it comes to disclosing information about consumers to the Track-
7 ing Defendants, companies that incentivize application developers to provide the App Store
8 with free apps for iDevices and provide Apple the metrics to support its claims of market lead-
9 ership.

10 62. The personal and private information is of extreme interest to many advertising
11 networks and web analytics companies, including the Tracking Defendants. For this reason, the
12 Tracking Defendants pay to support app development, so that many apps are provided to con-
13 sumers ostensibly “free” or at a lower cost.

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

20 64. Some Tracking Defendants pay app developers to include code that causes ban-
21 ner ads to be displayed when users run the apps. Those ads are then populated with content
22 from the Tracking Defendants and provide the communications channel for the Tracking De-
23 fendants to acquire and upload users’ personal information.

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

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

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

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

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

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

22 70. Because of Apple’s and the Tracking Defendants’ control and coding, consum-
23 ers are unable to detect, manage, or avoid this collection and transmittal of information.

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

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

1 73. Apple has continued to allow app developers to run their apps on its iOS plat-
2 form and failed to void the licensing agreements application developers, even after it received
3 notice of Tracking Defendants’ practices.

4 **F. Privacy Interests and Consent**

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

7 75. Consumers using iDevices that download apps from the App Store would rea-
8 sonably consider information from and about themselves stored on their iDevices to be per-
9 sonal and private information that they would not expected to be collected and used by third
10 parties without the consumers’ express consent.

11 76. Plaintiffs did not expect, receive notice of, or consent to the Tracking Defen-
12 dants tracking of their App use. Plaintiffs did not expect, receive notice of, or consent to the
13 Tracking Defendants acquisition of Plaintiffs’ personally identifiable information.

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

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

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

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

23 81. The Tracking Defendants sell users’ personal information to, or purchase and
24 merge with user’s personal information, other personal information about the same users that is
25 available in the commercial, secondary information market, which the traffickers take substan-
26 tial efforts to shield from the public eye. The Tracking Defendants and other parties to the in-
27 formation market use the merger of personal information to effectively or actually de-
28 anonymize consumers.

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

4 83. The Tracking Defendants actions were knowing, surreptitious, and without no-
5 tice and so were conducted without authorization and exceeding authorization.

6 84. The Tracking Defendants misappropriated Plaintiffs' personal information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 **V. CLASS ALLEGATIONS**

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

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

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

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

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

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

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

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

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

21 107. The class treatment of common questions of law and fact is superior to multiple
22 individual actions or piecemeal litigation in that it conserves the resources of the courts and the
23 litigants, and promotes consistency and efficiency of adjudication.

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

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

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

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

6 a. whether Defendants, without authorization, tracked and compiled infor-
7 mation to which Class Members enjoyed rights of possession superior to those of Defendants;

8 b. whether Defendants, without authorization, created personally identifi-
9 able profiles of Class Members;

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

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

14 e. Whether Defendants caused economic harm to Class Members;

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

17 g. Whether Defendants created or caused or facilitated the creation of per-
18 sonally identifiable consumer profiles of Class Members;

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

21 i. What uses of such information were exercised and continue to be exer-
22 cised by Defendants;

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

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

27 l. Whether Defendants have been unjustly enriched.

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

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

3 **VI. CLAIMS FOR RELIEF**

4 112. Based on the foregoing allegations, Plaintiffs' claims for relief include the fol-
5 lowing:

6 **FIRST CLAIM FOR RELIEF**

7 **Negligence, as to Defendant Apple**

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

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

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

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

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

1 the conscience of a reasonable person.

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

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

6 **SECOND CLAIM FOR RELIEF**

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

8 **as to All Defendants**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 133. Apple and the Tracking Defendants are jointly and severally liable for the viola-
25 tions of the Computer Fraud and Abuse Act alleged herein.

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

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

3 136. Tracking Defendants' unlawful access to Plaintiffs' and Class Members' com-
4 puters and electronic communications has caused Plaintiffs and Class Members irreparable in-
5 jury. Unless restrained and enjoined, Tracking Defendants will continue to commit such acts.
6 Plaintiff's and Class Members' remedy at law is not adequate to compensate it for these in-
7 flicted and threatened injuries, entitling Plaintiff and Class Members to remedies including in-
8 junctive relief as provided by 18 U.S.C. § 1030(g).

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

11 **THIRD CLAIM FOR RELIEF**

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

13 **as to All Defendants**

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

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

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

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

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

1 Class Members' computers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 **FOURTH CLAIM FOR RELIEF**

2 **Trespass to Chattel, as to All Defendants**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 their iDevices;

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

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

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

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

10 **FIFTH CLAIM FOR RELIEF**

11 **Violations of the Consumer Legal Remedies Act, California Civil Code § 1750, et seq.**

12 **as to Defendant Apple**

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

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

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

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

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

4 **SIXTH CLAIM FOR RELIEF**

5 **Violations of the Unfair Competition Law (UCL)**

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

7 **as to All Defendants**

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

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

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

19 **A. Unlawful Business Act and Practices**

20 186. Defendants' business acts and practices are unlawful, in part, because they vio-
21 late California Business and Professions Code, Section 17500, *et seq.*, which prohibits false ad-
22 vertising, in that they were untrue and misleading statements relating to Defendants' perform-
23 ance of services and provision of goods and with the intent to induce consumers to enter into
24 obligations relating to such services, and regarding which statements Defendants knew or
25 which, and by the exercise of reasonable care Defendants should have known, were untrue and
26 misleading.

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

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

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

9 189. Defendants are therefore in violation of the unlawful prong of the Unfair Com-
10 petition Law.

11 **B. Unfair Business Act and Practices**

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

16 191. Defendants' conduct lacks reasonable and legitimate justification in that Defen-
17 dants have benefited from such conduct and practices while Plaintiff and the Class members
18 have been misled as to the nature and integrity of Defendants' products and services and have,
19 in fact, suffered material disadvantage regarding their interests in the privacy and confidential-
20 ity of their personal information. Defendants' conduct offends public policy in California teth-
21 ered to the Consumer Legal Remedies Act, the state constitutional right of privacy, and Cali-
22 fornia statutes' recognition of the need for consumers to be information and equipped to protect
23 their own privacy interests, such as California Civil Code, Section 1798.8, such that consumers
24 may make informed decisions in their choices of merchants and other means of safeguarding
25 their privacy.

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

1 defendants were conducting themselves in a manner adverse to their commitments and users' in-
2 terests, through the undisclosed functions of iDevices and apps and the related conduct of the
3 Tracking Defendants. Defendants are therefore in violation of the unfairness prong of the Un-
4 fair Competition Law.

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

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

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

14 SEVENTH CLAIM FOR RELIEF

15 Breach of Implied Covenant of Good Faith and Fair Dealing

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

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

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

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

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

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

10 201. The contract is a form contract, the terms of which Plaintiffs are deemed to have
11 accepted once Plaintiffs and the Class signed up with Apple. The contract purports to give dis-
12 cretion to Apple relating to Apple's protection of users' privacy. Apple is subject to an obliga-
13 tion to exercise that discretion in good faith. The covenant of good faith and fair dealing is
14 breached when a party to a contract uses discretion conferred by the contract to act dishonestly
15 or to act outside of accepted commercial practices. Apple breached its implied covenant of
16 good faith and fair dealing by exercising bad faith in using its discretionary rights to deliber-
17 ately, routinely, and systematically make Plaintiffs' personal information available to third par-
18 ties.

19 202. Plaintiffs have performed all, or substantially all, of the of the obligations im-
20 posed on them under contract, whereas Apple has acted in a manner as to evade the spirit of the
21 contract, in particular by deliberately, routinely, and systematically without notifying Plaintiffs'
22 of its disclosure of Plaintiffs' personal information to Tracking Defendants. Such actions repre-
23 sent a fundamental wrong that is clearly beyond the reasonable expectation of the parties. Ap-
24 ple's causing the disclosure of such information to the Tracking Defendants is not in accor-
25 dance with the reasonable expectations of the parties and evidences a dishonest motive.

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

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

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

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

13 **EIGHTH CLAIM FOR RELIEF**

14 **Unjust Enrichment, as to Tracking Defendants**

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

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

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

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

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

1 **VII. DEMAND FOR RELIEF**

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

- 4 A. certify this case as a Class action on behalf of the Class defined above, appoint
5 Plaintiff as Class representative, and appoint his counsel as Class counsel;
- 6 B. declare that Defendants’ actions violate the statutes and common-law jurispru-
7 dence set forth above;
- 8 C. award injunctive and equitable relief as applicable to the Class *mutatis mutandis*,
9 including:
- 10 i. prohibiting Defendants from engaging in the acts alleged above;
 - 11 ii. requiring Defendants to provide reasonable notice and choice to con-
12 sumers regarding Defendants’ data collection, profiling, merger, and
13 deanonymization activities;
 - 14 iii. requiring Defendants to disgorge to Plaintiffs and Class Members or
15 to whomever the Court deems appropriate all of Defendants’ ill-
16 gotten gains;
 - 17 iv. requiring Defendants to delete all data from and about Plaintiffs and
18 Class Members that it collected and/or acquired from third parties
19 through the acts alleged above;
 - 20 v. requiring Defendants to provide Plaintiffs and other Class Mem-
21 bers reasonable means to decline, permanently, participation in
22 Defendants’ collection of data from and about them;
 - 23 vi. enjoining Apple from acquiring, retaining, and transferring,
24 whether in encrypted or unencrypted form, users’ detailed loca-
25 tion history;
 - 26 vii. requiring Apple to seek express consent from Plaintiffs and other
27 Class Members to capture, retain, and transfer location history in-
28 formation and, otherwise, to purge such information from all

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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.

1 Date: April 20, 2011

Respectfully submitted,

2
3 KAMBERLAW, LLC

4 By: s/Scott A. Kamber

5 Scott A. Kamber (*pro hac vice*)

6 KAMBERLAW, LLC

Interim Class Counsel

7 SCOTT A. KAMBER (*pro hac vice*)

8 DAVID A. STAMPLEY (*pro hac vice*)

9 *skamber@kamberlaw.com*

dstampley@kamberlaw.com

10 KAMBERLAW, LLC

11 100 Wall Street, 23rd Floor

New York, New York 10005

12 Telephone: (212) 920-3072

13 Facsimile: (212) 202-6364

14 DEBORAH KRAVITZ (SBN 275661)

15 (N.D. Cal. admission pending)

16 *dkravitz@kamberlaw.com*

17 KamberLaw, LLP

18 141 North St.

19 Healdsburg, California 95448

20 Telephone: (707) 820-4247

21 Facsimile: (212) 202-6364

22 AVI KREITENBERG (SBN 266571)

23 KAMBERLAW, LLP

24 1180 South Beverly Drive, Suite 601

25 Los Angeles, CA 90035

26 Telephone: (310) 400-1050

27 Facsimile: (310) 400-1056

28 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

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

3 JEFF S. WESTERMAN
4 jwesterman@milberg.com
5 MILBERG LLP
6 One California Plaza
7 300 South Grand Avenue, Ste 3900
8 Los Angeles, California 90071
9 Telephone: (213) 617-1200
10 Facsimilie: (213) 617-1975

11 PETER E. SEIDMAN
12 ANDREI V. RADO
13 ANNE MARIE VU (Bar No. 238771)
14 pseidman@milberg.com
15 arado@milberg.com
16 avu@milberg.com
17 MILBERG LLP
18 One Pennsylvania Plaza, 49th Floor
19 New York, New York 10119
20 Telephone: (212) 594-5300
21 Facsimile: (212) 868-1229

22 JEREMY WILSON
23 jeremy@wtfirm.com
24 WILSON TROSCLAIR & LOVINS
25 302 N. Market Street, Suite 501
26 Dallas, Texas 75202
27 Telephone: (214) 430-1930

28 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

1 JOSEPH H. MALLEY
malleylaw@gmail.com
2 LAW OFFICE OF JOSEPH H. MALLEY
1045 North Zang Blvd.
3 Dallas, Texas 75208
Telephone: (214) 943-6100
4

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

10 NABIL MAJED NACHAWATI, II
11 *mn@fnlawfirm.com*
FEARS NACHAWATI
12 4925 Greenville Avenue, Suite 715
Dallas, Texas 75206
13 Telephone: (214) 890-0711
14 Facsimile: (214) 890-0712

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

21 Counsel for Plaintiffs
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

1 RICHARD A. LOCKRIDGE
2 ROBERT K. SHELQUIST
3 rlockridge@locklaw.com
4 rshelquist@locklaw.com
5 LOCKRIDGE GRINDAL NAUEN P.L.L.P.
6 100 Washington Avenue S., Suite 2200
7 Minneapolis, MN 55401
8 Telephone: (612) 339-6900
9 Facsimile: (612) 339-0981

10 JEFF S. WESTERMAN
11 jwesterman@milberg.com
12 MILBERG LLP
13 One California Plaza
14 300 South Grand Avenue, Ste 3900
15 Los Angeles, California 90071
16 Telephone: (213) 617-1200
17 Facsimilie: (213) 617-1975

18 PETER E. SEIDMAN
19 ANDREI V. RADO
20 ANNE MARIE VU (Bar No. 238771)
21 pseidman@milberg.com
22 arado@milberg.com
23 avu@milberg.com
24 MILBERG LLP
25 One Pennsylvania Plaza, 49th Floor
26 New York, New York 10119
27 Telephone: (212) 594-5300
28 Facsimile: (212) 868-1229

JEREMY WILSON
jeremy@wtfirm.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

1 Telephone: (415) 568-2555

2 Facsimile: (415) 568-2556

3 Plaintiffs' Liaison Counsel

4
5
6 JOSEPH H. MALLEY

malleylaw@gmail.com

7 LAW OFFICE OF JOSEPH H. MALLEY

1045 North Zang Blvd.

8 Dallas, Texas 75208

9 Telephone: (214) 943-6100

10 DAVID C. PARISI (SBN 162248)

SUZANNE HAVENS BECKMAN (SBN 188814)

11 *dcparsi@parisihavens.com*

12 *shavens@parisihavens.com*

PARISI & HAVENS LLP

13 15233 Valleyheart Drive

Sherman Oaks, California 91403

14 Telephone: (818) 990-1299

15 Facsimile: (818) 501-7852

16 NABIL MAJED NACHAWATI, II

17 *mn@fnlawfirm.com*

FEARS NACHAWATI

4925 Greenville Avenue, Suite 715

18 Dallas, Texas 75206

19 Telephone: (214) 890-0711

Facsimile: (214) 890-0712

20 MICHAEL R. REESE (Bar No. 206773)

21 KIM RICHMAN

22 *mreese@reeserichman.com*

krichman@reeserichman.com

REESE RICHMAN LLP

23 875 Avenue of the Americas, 18th Floor

New York, NY 10001

24 Telephone: (212) 579-4625

25 Facsimile: (212) 253-4272

26 Counsel for Plaintiffs

1 **CERTIFICATE OF SERVICE**

2

3 I, David Stampley, an attorney, hereby certify that on April 21, 2011, I caused the above

4 ***First Consolidated Complaint***, to be served by causing true and accurate copies of such

5 documents to be electronically filed and transmitted to counsel of record through the Court’s

6 CM/ECF electronic filing system.

7

8 Date: April 21, 2011

8 Respectfully submitted,

9

10 KAMBERLAW, LLC

11 By: s/David A. Stampley

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28