

ORIGINAL

1 **MILBERG LLP**
2 JEFF S. WESTERMAN (SBN 94559)
3 jwesterman@milberg.com
4 SABRINA S. KIM (SBN 186242)
5 skim@milberg.com
6 One California Plaza
7 300 S. Grand Avenue, Suite 3900
8 Los Angeles, California 90071
9 Telephone: (213) 617-1200
10 Facsimile: (213) 617-1975

11 *Attorneys for Plaintiff*

12 [Additional Counsel Listed on Signature Page]

13 UNITED STATES DISTRICT COURT

14 NORTHERN DISTRICT OF CALIFORNIA

15 *cl*
16 ANTHONY CHIU, individually and on
17 behalf of all others similarly situated,

18 Plaintiff,

19 v.

20 APPLE, INC., a California Corporation, and
21 DOES 1 to 50 inclusive,

22 Defendants.

FILED

2011 JAN 27 P 2:18

Paed
SI

ADR

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
N.D. CA - SAN JOSE

99

E-filing

CV 11-00407

CASE NO. 11-00407

CLASS ACTION

HRL

COMPLAINT FOR:

1. Violations of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*;
2. Conversion;
3. Unjust Enrichment;
4. Violation of California Business and Professions Code § 17500 *et seq.*;
5. Violation of California Business and Professions Code § 17200 *et seq.*;
6. Violation of the Consumer Legal Remedies Act, California Civil Code § 1750;
7. Breach of Contract;
8. Breach of Implied Covenant of Good Faith and Fair Dealing;
9. Common Law Invasion of Privacy; and
10. Violation of Article I, Section 1 of the California Constitution.

JURY TRIAL DEMANDED

FAXED

1 Plaintiff Anthony Chiu (“Plaintiff” or “Mr. Chiu”) brings this action individually and on
2 behalf of a class of owners and users of mobile devices that run on Apple’s iPhone operating
3 system (“iOS”), including the Apple iPhone, iPad, and/or iPod Touch (collectively referred to as
4 the “mobile devices” or “Apple mobile devices”) who downloaded and used one or more
5 “applications,” as that term is defined herein, on their Apple mobile devices.

6 This case arises from Defendant Apple’s intentional and knowing transmission of data to
7 third parties that is used to identify Apple mobile device users and associate them with records
8 revealing the most intimate details of their lives, as reflected in their application usage and
9 activity, Internet browsing history and other personal data. This is done, without users’ consent
10 or knowledge, in violation of federal and state laws, and in breach of Apple’s purported
11 agreements with mobile device users. Plaintiff and the class seek damages and equitable relief.

12 Plaintiff alleges the following upon personal knowledge as to his own acts, and upon
13 information and belief based on the investigation conducted by Plaintiff’s counsel as to all other
14 matters.

15 **PARTIES**

16 1. Plaintiff Anthony Chiu is an individual who resides in Alameda, California. Mr.
17 Chiu is an owner and user of Apple’s iPhone who downloaded applications to his iPhone and
18 used them. The applications include: 360 App, camera+, soundhound, pageonce, trip tracker,
19 good guide, irecycle, iscopies, itriage, redlaser, key ring, repair pal, flixster, fandango, tv guide,
20 Netflix, stub hub, redbox, fring, whatsapp, pandora, hulu, dictionary.com, npr, poynt, point
21 inside, urbanspoon, kayak, taxi magic, and iheart radio.

22 2. Defendant Apple, Inc. (“Apple”) is a California corporation that is known
23 worldwide as an icon of personal computing. Apple has its principal place of business in this
24 District at 1 Infinite Loop, Cupertino, California 95014. Apple designs, manufactures and
25 markets, among other products, the iPhone, iPad, and iPod Touch, each of which runs on Apple’s
26 iOS. Apple also designs and manufactures a range of accessory, service and support offerings to
27 support the mobile devices, including its MobileMe subscription-based collection of online
28 services and software that automatically “pushes” or syncs new email, contacts, and calendar

1 events to the subscribers' iOS devices, Mac, and/or PC so that the devices "always stay in perfect
2 sync." Apple conducts business throughout California and the United States.

3 3. The true names and capacities, whether individual, corporate, associate or
4 otherwise, of each of the Defendants designated as a DOE are unknown to Plaintiff at this time
5 and therefore Plaintiff sues Defendants by such fictitious names, pursuant to California Civil
6 Code § 474. Plaintiff will ask leave of the Court to amend this Complaint to show the true
7 names and capacities of the DOE Defendants when that information is ascertained. Plaintiff is
8 informed and believes, and thereon alleges that each of the Defendants designated herein as a
9 DOE is legally responsible in some manner, for the performance of the acts and omissions
10 described below, and is liable for the events and happenings alleged and, in such manner,
11 proximately caused harm to Plaintiff as further alleged.

12 4. Defendant Apple, and the DOE Defendants, and each of them, are individually
13 sued as participants, co-conspirators, and aiders and abettors in the improper acts, plans,
14 schemes, and transactions that are the subject of this Complaint.

15 JURISDICTION AND VENUE

16 5. This Court has subject matter jurisdiction pursuant to the Class Action Fairness
17 Act of 2005, 28 U.S.C. § 1332 (a) and 1332 (d), because the amount in controversy exceeds
18 \$5,000,000.00 exclusive of interests and costs, and more than two-thirds of the members of the
19 Class are citizens of states different from that of Defendant. This Court also has federal question
20 jurisdiction as this Complaint alleges violations of the Stored Communications Act, 18 U.S.C.
21 § 2701 *et seq.*, (the "SCA").

22 6. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391 as
23 Defendant Apple's principal executive office and headquarters are located in California.

24 FACTUAL ALLEGATIONS

25 APPLE MOBILE DEVICES AND APPS

26 7. On January 9, 2007, Apple entered the cellular telephone market with the
27 introduction of its now-iconic and ubiquitous iPhone. Possessing many of the capabilities of an
28 internet-connected laptop computer in a sleek, compact device, the iPhone quickly became one

1 of the most popular and influential devices in the smartphone market; Apple sold more than 59
2 million iPhones in fewer than four years. Apple has since expanded its product line to include the
3 iPod Touch and the iPad, both of which run the same iOS software and share many of the same
4 hardware features as the iPhone.

5 8. Apple offers apps for its mobile devices on an Apple-sponsored website, known
6 as the “App Store,” which was launched on July 10, 2008. The App Store is linked to Apple’s
7 iTunes application. An application or “app” is a software program that runs on a computer or
8 mobile device. iTunes is Apple’s proprietary digital media player application, designated by
9 Apple for playing and organizing Apple’s digital music and video files, and is also an interface
10 to manage the contents on Apple’s iOS products. Apple advertises the App Store as “the
11 ultimate source for mobile apps — 300,000 and counting in practically every category.” As of
12 January 22, 2011, Apple announced *via* its “10 Billion App Countdown” that the App Store had
13 over 10 billion downloads. *See* Apple Inc., [http://www.apple.com/itunes/10-billion-app-](http://www.apple.com/itunes/10-billion-app-countdown/)
14 [countdown/](http://www.apple.com/itunes/10-billion-app-countdown/) (last visited Jan. 22, 2011).

15 9. Some apps, such as “Safari” and “Maps,” are offered directly by Apple. Others
16 are offered by third-party app developers who have contracted with Apple to sell their apps *via*
17 the App Store for use on Apple’s mobile devices. Apple generally takes 30% of revenues from
18 the app sales, while the remaining 70% goes to the seller or owner of the app.

19 **UDIDS AND OTHER PERSONAL DATA**

20 10. Apple equips each mobile device with a unique, application-visible serial number
21 called a Unique Device Identifier (“UDID”). Apple allows the UDID to be displayed to
22 application developers, and allows the downloaded applications access to the user’s browsing
23 history each time the user clicks on an advertisement or application appearing on their mobile
24 device. There is no way to block the visibility of the UDID to any installed applications, nor is
25 there any mechanism to prevent the transmission of the UDID, and other information obtained
26 from the mobile device, to third parties in the current version of Apple’s operating system. The
27 commercial collection of data from the mobile devices through invisible and intrusive techniques
28 has become big business at the expense of the users’ privacy as the application developers use

1 the UDID themselves, and/or sell them to tracking companies as they would any other
2 commodity.

3 11. Consequently, anyone who has used a mobile device to browse the Internet to
4 obtain advice about hemorrhoids, sexually transmitted disease, abortion, drug rehabilitation, or
5 care for elderly; to search for jobs, seek out new romantic partners, engage in political activity; in
6 fact, to do more or less anything; can be reasonably sure that the browsing history created by
7 such investigation has been incorporated into a detailed dossier for sale to marketers.

8 12. The spying on mobile device users by observing and remembering the user's
9 clicks, combining it with the user's UDID, and building and selling detailed profiles of the
10 identified user's online activities and interests, allows the online marketers chilling access to the
11 most intimate details of the user's life, in order to exploit this otherwise private information to
12 commercial advantage. One data aggregator, Audience Science, states that its work involves
13 "recording billions of behavioral events daily and reaching over 385 million unique Internet
14 users" and then making such data available to its clients: "web publishers, marketers, networks,
15 exchanges, and agencies[,] to create intelligent audience segments to connect people with
16 relevant advertising driving the transition to data-driven audience marketing online." See
17 MediaPost, [http://mediapost.com/events/?/showID/OMMAGlobalNewYork.09.NewYorkCity/
18 type/Exhibitor/itemID/647/OMMAGlobalNewYork-Exhibitors%20and%20Sponsors.html](http://mediapost.com/events/?/showID/OMMAGlobalNewYork.09.NewYorkCity/type/Exhibitor/itemID/647/OMMAGlobalNewYork-Exhibitors%20and%20Sponsors.html) (last
19 visited Jan. 24, 2011).

20 13. On December 17, 2010, the *Wall Street Journal* published an article entitled,
21 "*Your Apps Are Watching You*" that detailed the effect of Apple's blanket disclosure of its
22 mobile device users' UDIDs, combined with the release of other personal information such as
23 user name and password, contacts (collected from the phone's address book, which contains
24 names, users' phone numbers and email addresses, as well as a "notes field," in which many
25 users store sensitive data such as door security codes or bank accounts), age and gender, phone
26 numbers, current location, and in some cases, even the owner's real name, obtained from the
27
28

1 mobile device.¹ The *Wall Street Journal* investigated the transmissions of 101 popular mobile
2 device apps—games and other software applications for iPhone and Android phones— and
3 concluded that 56 out of the 101, or over half, transmitted the UDID that had been wrongfully
4 disclosed to other companies without the users’ awareness or consent. The article cited multiple
5 marketers that touted the high market value of this information in targeting consumers based on
6 the data mined from their iOS mobile device giving credence to the statement, “the more
7 information that is known about a consumer, the more a company will pay to deliver a precisely-
8 targeted advertisement to him.” Federal Trade Commission Preliminary Staff Report, *Protecting*
9 *Consumer Privacy in an Era of Rapid Change*, (Dec. 2010) at 24 (“FTC Report”).

10 14. Eric Smith, Director of Information Security and Networking at Bucknell
11 University, published a research paper on October 1, 2010, entitled, “*iPhone Applications &*
12 *Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers*
13 *(UDIDs)*,” in which he presented the results of his investigation into Apple’s disclosure of
14 UDIDs and other personal information from the users’ mobile devices, and the consequent
15 collection and dissemination of such personal information (where and how the personal
16 information is being shared, with whom, and how it is being used).² Smith found that a
17 substantial number of applications collect both the phone’s UDID and some form of user login
18 data which ties to a stored user account, and that 68% of the evaluated apps silently transmitted
19 the UDID back to a remote server owned either by the app developer or an advertising partner.
20 Such entities inherently have the ability to tie a UDID to a real-world identity, and combined
21 with other widespread data collection of information mined from the mobile devices, can lead to
22 effective real-time user tracking of location and activity. Such data collection can also open the
23 door to specific harms associated with the misuse of the user’s personal data, such as economic
24 injury resulting from identity theft; unwanted commercial intrusions into their daily lives by

25 _____
26 ¹ Available at http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html?mod=what_they_know (last visited 1/20/11).

27 ² Available at [http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-](http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf)
28 [Issues.pdf](http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf)

1 unwanted solicitations; unwanted exposure of sensitive data relating to the personal health or
2 financial condition of the user which could lead to reputational harm, including the fear of being
3 monitored or simply having private information made public; or actual physical harm, and even
4 risks to physical security. In plain English: an advertiser can know, in real-world terms, exactly
5 what a particular mobile device was used to search for on a given day, where the search was
6 conducted from, and, assuming that the mobile device was used by its owner, the advertiser
7 would know the identity of the person. Few, if any, consumers would knowingly consent to such
8 exposure, and even the government would not have such unlimited access to personal
9 information unless it first obtained a warrant.

10 15. By collecting personal information from the mobile devices “[w]ebsites and stores
11 can, therefore, easily buy and sell information on visitors with the intention of merging
12 behavioral with demographic and geographic data in ways that will create social categories that
13 advertisers covet and target with ads tailored to them or people like them.” Joseph Turow,
14 Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, *Americans Reject
15 Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), available at
16 <http://ssrn.com/abstract=1478214>.

17 16. As one researcher put it, “[a]n advertiser or other entity who wants to track user
18 behaviors and patterns online could not ask for a better identifier than one that is guaranteed by
19 the hardware manufacturer to be unique to a single device. Indeed, “[The UDID] is effectively a
20 ‘supercookie,’ says Vishal Gurbuxani, co-founder of Mobclix Inc., an exchange for mobile
21 advertisers” See Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, Wall St. J.,
22 Dec. 17, 2010.³ A cookie is a device stored on a users’ computer that enables the tracking of a
23 users’ browsing history. Another marketer stated:

24 “The great thing about mobile is you can’t clear a UDID like you can a cookie,”
25 says Meghan O’Holleran of Traffic Marketplace, an Internet ad network that is
26 expanding into mobile apps. “That’s how *we track everything*.” Ms. O’Holleran
27 says Traffic Marketplace, a unit of Epic Media Group, monitors Smartphone users
28 whenever it can. *‘We watch what apps you download, how frequently you use*

28 ³ See *supra* note 1.

1 *them, how much time you spend on them, how deep into the app you go,* she
2 says.

3 *Id.* [Emphasis added.]

4 17. Among the companies receiving the personalized profiles is one owned by Apple
5 itself, Quattro Wireless, which uses the information to target advertisements through Apple's
6 lucrative iAd system. Apple boasts that "[w]ith iAd, you can now reach the Apple audience in
7 their favorite apps anytime, anywhere with unmatched impact and precision," and urges
8 marketers to:

9 Get Started Today

10 Learn how you can advertise on the iAd Network and *reach the most engaged*
11 *audience in mobile.* Contact an iAd sales executive today.

12 See Apple Inc., <http://advertising.apple.com/developers/> (last visited Jan. 22, 2011). [Emphasis
13 added.]

14 **APPLE'S RELEASE OF ITS USERS' PERSONAL DATA VIOLATES ITS OWN PRIVACY POLICY**

15 18. Apple's privacy policy is opaque and confusing, but one thing is clear: it does not
16 inform mobile device users that by providing application developers with their UDID, Apple
17 enables them to put a name to highly personal and in many cases, embarrassing information,
18 derived from app downloading activity and usage, and Internet browsing history, that would
19 otherwise be anonymous. On the contrary, the Apple Privacy Policy contains a section entitled,
20 "How we use your personal information," and the enumeration of ways the information is being
21 used does not include giving third parties unfettered access to mobile device users' personally
22 identifiable information. Rather, the policy states that, "[p]ersonal information will *only* be
23 shared by Apple to provide or improve our products, services and advertising; *it will not be*
24 *shared* with third parties for their marketing purposes." (Emphasis added.)

25 19. Similarly, Apple spokesman Tom Neumayr states, "[Apple has] created strong
26 privacy protections for our customers, especially regarding location-based data. Privacy and
27
28

1 trust are vitally important,” See Scott Thurm & Yukari Iwanti Kane, *Your Apps Are Watching*
2 *You*, Wall St. J., Dec. 17, 2010.⁴

3 20. It is now widely accepted that such privacy policies are ineffective when it comes
4 to providing consumers with useful and accurate information about how their personal
5 information will be collected and used. In a preliminary staff report prepared by the Federal
6 Trade Commission, entitled, *Protecting Consumer Privacy in an Era of Rapid Change*, the
7 Federal Trade Commission stated that, “[T]he notice-and-choice model, as implemented, has led
8 to long, incomprehensible privacy policies that consumers typically do not read, let alone
9 understand” and that are wholly inadequate in an age in which companies “collect and use
10 consumers’ information in ways that often are invisible to consumers.” FTC Report at iii. The
11 FTC also found that “privacy notices are often opaque, lack uniformity, and are too long and
12 difficult to navigate. Too frequently they bury disclosures of important information. . . . A
13 particularly strong illustration of where privacy policies have been ineffective is in the mobile
14 context where, because of the small size of the device, a privacy notice can be spread out over
15 100 separate screens. Indeed, it is difficult to imagine consumers scrolling through each screen
16 or making informed choices based on the information contained in them.” *Id.* at 70. See also,
17 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S L.J. &
18 Pol’y for Info. Soc’y 543, 565 (2008) (estimating that it would take consumers hundreds of hours
19 to read the privacy policies they might typically encounter in one year on the Internet).

20 21. Research confirms that consumers almost never get past the first few sentences of
21 privacy policies or terms of service, if they read them at all, and that, moreover, when they see
22 the hyperlinked words “Privacy Policy” on a Web site, they assume that they mean that their
23 information is not being collected or shared, even if the policy says just the opposite. See Turow,
24 *supra* ¶ 15. This is especially so when the first few sentences of the privacy policy evince
25 concern for maintaining the users privacy. The take-it-or-leave-it Apple “privacy policy” ---
26 which would be more aptly named a “disclosure policy” --- is no exception. The first sentence:

27 _____
28 ⁴ See *supra* note 1.

1 “Your privacy policy is important to us.” To the right of that sentence sits the “TRUSTe
2 Certified Privacy” logo --- a sure sign to most consumers that Apple is guarding their personal
3 information:



4
5
6 Apple Inc. has been awarded TRUSTe’s Privacy Seal signifying that this privacy
7 policy and practices have been reviewed by TRUSTe for compliance with
8 TRUSTe’s program requirements including transparency, accountability and choice
9 regarding the collection and use of your personal information. The TRUSTe
10 program does not cover information that may be collected through downloadable
11 software. If you have questions or complaints regarding our privacy policy or
12 practices, please contact us at privacy@apple.com. If you are not satisfied with
13 our response you can contact [TRUSTe here](#).

14 22. Moreover, Apple’s “privacy policy” misleadingly states that, “[i]f we do combine
15 non-personal information with personal information the combined information will be treated as
16 personal information for as long as it remains combined.” This falsely suggests that Apple
17 protects the mobile device users’ personal information from disclosure, when in fact it does not
18 and misleadingly suggests that personally identifiable information is substantively different from
19 non-personally identifiable information when in practice, this distinction is irrelevant to privacy
20 issues:

21 Data privacy historically has been thought of in terms of *personally identifying*
22 *information* (alternatively called *personally identifiable or individually*
23 *identifiable* information or referred to simply as *PII*). Attention had been focused
24 on personal data that could identify an individual person --- by data elements such
25 as the person’s name, postal address, email address, social security number or
26 driver’s license number --- as opposed to aggregate data, which may be useful to
27 companies but not reveal anything in particular about any individual user, or data
28 unique to a person that could distinguish that person from someone else, but not
29 reveal a person’s identity (such as cookie data that shows almost everything about
30 a user’s use of a site except who that user is. . . . The Federal Trade Commission
31 noted in a 2009 report, however, that changes in data collection and use practices
32 and new technologies increasingly make the distinction between PII and non-PII
33 less meaningful. . . . As technologies improve, it is assumed that it will be easier
34 to actually identify a specific person based on data that to date has been
35 considered non-PII or pseudonymous. . . .

36 Even where data itself is anonymous or pseudonymous, it can become identifiable
37 when combined and linked together. . . . Thus, distinctions between PII and non-
38 PII may not have any bearing on the particular privacy risks at issue. . . . For all
39 these reasons, the FTC has suggested that, at least in the context of behavioral

1 advertising, the relevant criteria is *whether information reasonably could be*
2 *associated with a particular consumer or device*, not whether it is PII or non-PII.

3 The increased use of third party cookies, the use of cookies for increasingly more
4 sensitive data and the practice of some sites in combining information voluntarily
5 obtained with data collected through cookies and other technical means have
6 blurred the difference between personally identifying information and non-PII.
7 Ian C. Ballon, *E-Commerce and Internet Law: Treatise With Forms*, 26.01 Data
8 Privacy Law - In General, at pp. 26-7 - 26-9, and 26.03 Web Beacons, Cookies
9 and Other Online Data Gathering Mechanisms, at pp. 26-20 - 26-21 (2d ed. West
10 2009).

11 **CLASS ACTION ALLEGATIONS**

12 23. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23 on behalf of a Class
13 defined as follows: All Apple customers who reside in the United States and who, any time after
14 July 10, 2008, have downloaded and used an application on their iPhone, iPad and/or iPod
15 Touch.

16 24. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of
17 Defendants or any employees, officers, or directors of Defendants; legal representatives,
18 successors, or assigns of Defendants; and any justice, judge or magistrate judge of the United
19 States who may hear the case, and all persons related to any such judicial officer, as defined in
20 28 U.S.C. § 455(b).

21 25. **Numerosity**. The Class members are so numerous and dispersed nationwide that
22 joinder of all members is impracticable. Upon information and belief, the Class members
23 number in the hundreds of thousands, if not millions. The exact number of Class members is
24 unknown, but can be determined from Defendants' computerized and other records. Plaintiff
25 reasonably estimates and believes that there are thousands of persons in the Class.

26 26. **Commonality**. There are numerous and substantial questions of law and fact that
27 are common to all members of the Class, which predominate over any question affecting only
28 individual Class members. The members of the Class were and continue to be subjected to the
same practices of the Defendants. The common questions and issues raised by Plaintiff's claims
include:

(a) whether Defendants shared Plaintiff's and the Class's personal
information with third-party advertisers and online tracking companies;

1 (b) whether Plaintiff consented to Defendants' sharing of Plaintiff's personal
2 information with third-party advertisers and online tracking companies;

3 (c) whether Apple violated its own Terms and Privacy Policies by sharing of
4 Plaintiff's personal information with app developers, third-party advertisers, and online tracking
5 companies;

6 (d) whether Defendants breached their contracts, and if so, the appropriate
7 measure of damages and remedies against Defendants for such breaches;

8 (e) whether Defendants breached the covenants of good faith and fair dealing,
9 and if so, the appropriate measure of damages and remedies against Defendants for such breach;

10 (f) whether Defendants have violated the SCA; California Business and
11 Professions Code § 17200 *et seq.*; California Business and Professions Code § 17500 *et seq.*;
12 Consumer Legal Remedies Act, California Civil Code § 1750; Article I, Section 1 of the
13 California Constitution; and other violations of common law;

14 (g) whether Plaintiff and the Class have been damaged as a result of
15 Defendants' alleged violations as alleged herein; and, if so, the appropriate relief for Defendants'
16 violations; and

17 (h) whether Defendants have been unjustly enriched as a result of its unlawful
18 conduct, and, if so, whether Defendants should disgorge inequitably obtained money that they
19 have been unjustly enriched by; and, the nature and extent of any other remedies, and injunctive
20 relief, to which Plaintiff and the Class are entitled.

21 27. **Typicality.** Plaintiff's claims are typical of the claims of all of the other members
22 of the Class, because his claims are based on the same legal and remedial theories as the claims
23 of the Class and arise from the same course of conduct by Defendants.

24 28. **Adequacy.** Plaintiff will fairly and adequately protect the interests of all
25 members of the class in the prosecution of this Action and in the administration of all matters
26 relating to the claims stated herein. Plaintiff is similarly situated with, and has suffered similar
27 injuries as, the members of the Class he seeks to represent. Plaintiff has retained counsel
28

1 experienced in handling class action lawsuits. Neither Plaintiff nor his counsel have any interest
2 that might cause them not to vigorously pursue this action.

3 29. **Superiority.** A class action is superior to other available methods for the fair and
4 efficient adjudication of the controversy, since individual joinder of the Class members is
5 impracticable. Even if individual Class members were able to afford individual litigation, it
6 would be unduly burdensome to the Courts in which the individual litigation would proceed.
7 Defendants have subjected the Class to the same violations as referenced herein. Accordingly,
8 class certification is appropriate under Rule 23 because common issues of law and fact regarding
9 Defendants' uniform violations predominate over individual issues, and class certification is a
10 superior method of resolving these claims. No unusual difficulties are likely to be encountered
11 in the management of this action as a class action. Defendants acted and continue to act in a
12 manner that is generally applicable to all members of the Class, making final injunctive relief
13 appropriate.

14 **FIRST CAUSE OF ACTION**
15 **(Stored Communications Act, 18 U.S.C. § 2701 et seq.)**

16 30. Plaintiff hereby incorporates by reference the allegations contained in all of the
17 preceding paragraphs of this complaint.

18 31. Defendants provide electronic communication services to the public *via* their
19 Apple mobile devices and/or apps. 18 U.S.C. § 2510(15).

20 32. Defendants provide remote computing service to the public because they provide
21 computer storage and processing services by means of an electronic communications system. 18
22 U.S.C. § 2711(2).

23 33. Defendants carry and maintain their users' UDIDs solely for the purpose of
24 providing storage and computer processing services to its users. Defendants are not authorized
25 to access this information for purposes other than providing storage and computer processing.
26 18 U.S.C. § 2702(a)(2).

27 34. Mobile device users' UDID and personal information as stored by Defendants are
28 electronic communications within the meaning of 18 U.S.C. § 2510 (12).

1 35. Defendants hold their users' UDID and personal information in electronic storage
2 within the meaning of 18 U.S.C. § 2510(17).

3 36. In relevant part, 18 U.S.C. § 2701(a)(1)-(2) of the SCA provide that an offense is
4 committed by anyone who: "(1) intentionally accesses without authorization a facility through
5 which electronic communication service is provided; or (2) intentionally exceeds an
6 authorization to access that facility; and thereby obtains . . . [an] electronic communication while
7 it is in electronic storage in such system."

8 37. Defendants intentionally exceeded their authorization to access and control
9 confidential and private information relating to Plaintiff's and the Class's electronic
10 communications in violation of 18 U.S.C. § 2701 *et seq.* of the SCA.

11 38. In relevant part, 18 U.S.C. § 2702(a)(1)-(2) of the SCA provides that a person or
12 entity shall not: "(1) . . . knowingly divulge to any person or entity the contents of a
13 communication . . . ; and (2) . . . shall not knowingly divulge to any person or entity the contents
14 of any communication"

15 39. Section 2707 of the SCA provides for a civil cause of action and allows for
16 damages, and declaratory and equitable relief.

17 40. Defendants knowingly, willfully, unlawfully, and intentionally without
18 authorization divulged confidential and private information relating to Plaintiff's electronic
19 communications in violation of 18 U.S.C. § 2701 *et seq.* of the SCA.

20 41. Defendants engage in the foregoing acts without obtaining the lawful consent of
21 the user. 18 U.S.C. § 2702(b)(3).

22 42. By engaging in the foregoing acts, Defendants knowingly divulge the contents of
23 communication carried and maintained by Defendants on behalf of and received by
24 transmissions from their users in violation of 18 U.S.C. § 2702(a)(2).

25 Plaintiff and the Class are entitled to statutory damages of no less than \$1,000.00 (one thousand
26 dollars) per violation. Because Defendants' violations were willful and intentional, Plaintiff and
27 the Class are entitled to recover punitive damages as provided by 18 U.S.C. § 2702(c).

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

**SECOND CAUSE OF ACTION
(Conversion)**

43. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

44. Plaintiff's personally identifiable information – including full name, email address, mailing address, telephone number, and credit card number – is valuable property owned by Plaintiff.

45. Defendants unlawfully exercised dominion over said property and thereby converted Plaintiff's and the Class members' respective personal information by providing it to third parties in violation of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and in violation of its contracts with Plaintiff and the respective class members.

46. Plaintiff and the Class were damaged thereby.

**THIRD CAUSE OF ACTION
(Unjust Enrichment)**

47. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

48. By engaging in the conduct described in this Complaint, Defendants have knowingly obtained benefits from Plaintiff under circumstances that make it inequitable and unjust for Defendants to retain them.

49. Defendants have received a benefit from Plaintiff and Defendants have received and retained money from advertisers and other third parties as a result of sharing the personal information of Defendants' users' with those advertisers without Plaintiff's knowledge or consent as alleged in this Complaint.

50. Plaintiff did not expect that Defendants would seek to gain commercial advantage from third parties by using his personal information without his consent.

51. Defendants knowingly used Plaintiff's personal information without his knowledge or consent to gain commercial advantage from third parties and had full knowledge of the benefits they have received from Plaintiff. If Plaintiff had known Defendants were not

1 keeping his personal information from third parties, he would not have consented and
2 Defendants would not have gained commercial advantage from third parties.

3 52. Defendants will be unjustly enriched if Defendants are permitted to retain the
4 money paid to them by third parties, or resulting from the commercial advantage they gained, in
5 exchange for Plaintiff's personal information.

6 53. Defendants should be required to provide restitution of all money obtained from
7 their unlawful conduct.

8 54. Plaintiff and the Members of the Class are entitled to an award of compensatory
9 and punitive damages in an amount to be determined at trial or to the imposition of a
10 constructive trust upon the wrongful revenues and/or profits obtained by and benefits conferred
11 upon Defendants as a result of the wrongful actions as alleged in this complaint.

12 55. Plaintiff and the Class have no remedy at law to prevent Defendants from
13 continuing the inequitable conduct alleged in this complaint and the continued unjust retention of
14 the money Defendants received from third-party advertisers.

15 **FOURTH CAUSE OF ACTION**
16 **(Violation Of California Business and Professions Code § 17500, et seq.**
17 **Untrue and Misleading Statements)**

18 56. Plaintiff hereby incorporates by reference the allegations contained in all of the
19 preceding paragraphs of this Complaint.

20 57. Plaintiff asserts this cause of action against Defendants for violations of
21 California Business and Professions Code § 17500 et seq. for untrue and misleading statements.

22 58. At all relevant times, Defendants engaged in a scheme of offering its Apple
23 mobile device and app services to Plaintiff by way of, *inter alia*, commercial marketing and
24 advertising, the World Wide Web (Internet), product packaging and labeling, and other
25 promotional materials. These materials misrepresented and/or omitted the truth about the extent
26 to which Defendants would share valuable personal information with third parties. Defendants
27 knew, or should have known, that these statements were deceptive, misleading, or untrue.

28 59. Said advertisements and inducements were made within the State of California
and come within the definition of advertising as contained in Business and Professions Code

1 § 17500 *et seq.* in that such promotional materials were intended as inducements to purchase and
2 use products and services offered by Defendants and are statements disseminated by Defendants
3 to Plaintiff and were intended to reach Plaintiff. Defendants knew, or should have known, that
4 these statements were misleading and deceptive.

5 60. In furtherance of said plan and scheme, Defendants have prepared and distributed
6 within the State of California *via* commercial marketing and advertising, the World Wide Web
7 (Internet), product packaging and labeling, and other promotional materials, statements that
8 misleadingly and deceptively represent the truth about personal information that Apple mobile
9 device and app users entrust to Defendants.

10 61. Consumers, including Plaintiff, were among the intended targets of such
11 representations.

12 62. The above acts of Defendants, in disseminating said misleading and deceptive
13 statements throughout the State of California to consumers, including Plaintiff, were and are
14 likely to deceive reasonable consumers, including Plaintiff, by obfuscating the truth about
15 Defendants' use of their personal information.

16 63. As a result of the above violations, Plaintiff has suffered injury in fact and lost
17 money or property. Plaintiff and the Members of the Class, pursuant to Business and Professions
18 Code § 17535, are entitled to an order of this Court enjoining such future conduct on the part of
19 Defendants, and such other orders and judgments that may be necessary to return Defendants'
20 ill-gotten gains and restore to any person in interest any money paid for Defendants' services as a
21 result of the wrongful conduct of Defendants.

22 **FIFTH CAUSE OF ACTION**
23 **(Violation Of California Business And Professions Code § 17200 *et seq.***
24 **Unfair Competition)**

25 64. Plaintiff hereby incorporates by reference the allegations contained in all of the
26 preceding paragraphs of this complaint.
27
28

1 65. At all relevant times, Defendants engaged, and continue to engage, in unfair,
2 unlawful, and fraudulent business practices in California by engaging in the misconduct detailed
3 above.

4 66. Defendants misled consumers by continuously and falsely representing during the
5 Class Period that they would not make personally identifiable information available to third
6 parties without the consent of Plaintiff when in fact it secretly provided such information to third
7 parties as alleged herein.

8 67. Defendants engaged in these unfair and fraudulent practices to increase their
9 profits. The business practices alleged above are unlawful under § 17200 *et seq.* because they
10 violate § 17500 *et seq.*, the Stored Communications Act, and the California Consumer Legal
11 Remedies Act, among others.

12 68. Had Plaintiff known that Defendants would share his personally identifiable
13 information with third parties, he would not have purchased or used Defendants' services,
14 which in turn, forced him to relinquish, for free, valuable personal information. As a result of
15 Defendants' acts of unfair competition, Plaintiff and the Members of the Class have suffered, and
16 continues to suffer, injury in fact and have lost money and/or property as a result of such
17 fraudulent, unfair, and/or unlawful business practices, in an amount that will be proven at trial,
18 but which is in excess of the jurisdictional minimum of this Court.

19 69. The aforementioned practices that Defendants have used, and continue to use to
20 their significant gain, also constitute unlawful competition and provide an unlawful advantage
21 over Defendants' competitors, as well as injury to Plaintiff.

22 70. Plaintiff seeks full restitution and disgorgement of money, as necessary and
23 according to proof, to restore to Plaintiff the value of all personal information that Defendants
24 unlawfully converted by means of the unfair and/or fraudulent business practices complained of
25 herein, plus interest thereon.

26 71. Plaintiff seeks an injunction to prohibit Defendants from continuing to engage in
27 the unfair trade practices complained of herein. Cal. Bus. & Prof. Code § 17203. The acts
28 complained of herein occurred, at least in part, within the Class Period.

1 79. By engaging in the actions, misrepresentations, and misconduct set forth in this
2 Complaint, Defendants violated, and continue to violate, § 1770(a)(7) by misrepresenting the
3 service is of a particular standard, quality, or grade.

4 80. By engaging in the actions, misrepresentations, and misconduct set forth in this
5 complaint, Defendants violated, and continue to violate, § 1770(a)(9) by advertising services
6 with intent not to sell them as advertised.

7 81. By engaging in the actions, misrepresentations, and misconduct set forth in this
8 complaint, Defendants violated, and continue to violate, § 1770(a)(16) by misrepresenting that a
9 subject of a transaction has been supplied in accordance with a previous representation when
10 they have not.

11 82. Plaintiff requests that this Court enjoin Defendants from continuing to employ the
12 unlawful methods, acts, and practices alleged herein pursuant to California Civil Code
13 § 1780(a)(2). If Defendants are not restrained from engaging in these types of practices in the
14 future, Plaintiff and the Class will continue to suffer harm.

15 **SEVENTH CAUSE OF ACTION**
16 **(Breach of Contract)**

17 83. Plaintiff hereby incorporates by reference the allegations contained in all of the
18 preceding paragraphs of this complaint.

19 84. Plaintiff submits personal information to Apple and Apple promises that it will
20 not share this information with third-party advertisers or applications developers without
21 Plaintiff's consent, and the consent of each Class member, respectively.

22 85. The Apple Privacy Policy states that Apple will not divulge personal information
23 to outside advertising companies without the user's consent. Despite this promise, Apple did in
24 fact knowingly share users' personal information with outside advertisers and application
25 developers in violation of its own Agreement with its users.

26 86. Plaintiff never consented to the sharing of his personal information to third-party
27 advertisers and/or application developers.

28 87. Plaintiff has performed his obligations under the contract.

1 88. Apple materially breached its contractual obligations through its conduct as
2 alleged herein, including its transmission of Plaintiff's personal information to third-party
3 advertisers and application developers, as well as Plaintiff's UDID without consent.

4 89. Plaintiff and the Class have been damaged as a direct and proximate result of
5 Apple's breach of their agreements with Plaintiff and the Members of the Class.

6 **EIGHTH CAUSE OF ACTION**
7 **(Breach of Implied Covenant of Good Faith and Fair Dealing)**

8 90. Plaintiff hereby incorporates by reference the allegations contained in all of the
9 preceding paragraphs of this complaint.

10 91. As set forth in the Sixth Cause of Action, Plaintiff submits personal information
11 to Apple and Apple promises in its Privacy Policy that it will not share this information with
12 third-party advertisers or applications developers without Plaintiff's consent, and the consent of
13 each Class member, respectively.

14 92. A covenant of good faith and fair dealing, which imposes upon each party to a
15 contract a duty of good faith and fair dealing in its performance, is implied in every contract,
16 including the Agreement that embodies the relationship between Apple and its users.

17 93. Good faith and fair dealing is an element imposed by common law or statute as an
18 element of every contract under the laws of every state. Under the covenant of good faith and
19 fair dealing, both parties to a contract impliedly promise not to violate the spirit of the bargain
20 and not to intentionally do anything to injure the other party's right to receive the benefits of the
21 contract.

22 94. Plaintiff reasonably relied upon Apple to act in good faith both with regard to the
23 contract and in the methods and manner in which it carries out the contract terms. Bad faith can
24 violate the spirit of the Agreement and may be overt or may consist of inaction. Apple's inaction
25 in failing to adequately notify Plaintiff of the release of personal information to outside
26 advertisers and application developers evidences bad faith and ill motive.

27 95. The contract is a form contract, the terms of which Plaintiff is deemed to have
28 accepted once Plaintiff and the Class signed up with Apple. The contract purports to give

1 discretion to Apple relating to Apple's protection of users' privacy. Apple is subject to an
2 obligation to exercise that discretion in good faith. The covenant of good faith and fair dealing is
3 breached when a party to a contract uses discretion conferred by the contract to act dishonestly or
4 to act outside of accepted commercial practices. Apple breached its implied covenant of good
5 faith and fair dealing by exercising bad faith in using its discretionary rights to deliberately,
6 routinely, and systematically make Plaintiff's personal information available to third parties.

7 96. Plaintiff has performed all, or substantially all, of the obligations imposed on him
8 under the contract, whereas Apple has acted in a manner as to evade the spirit of the contract, in
9 particular by deliberately, routinely, and systematically without notifying Plaintiff of its
10 disclosure of his personal information to third-party advertisers. Such actions represent a
11 fundamental wrong that is clearly beyond the reasonable expectations of the parties. Apple's
12 disclosure of such information to third party advertisers and tracking companies is not in
13 accordance with the reasonable expectations of the parties and evidences a dishonest purpose.

14 97. Apple's ill motive is further evidenced by its failure to obtain Plaintiff's consent
15 in its data mining efforts while at the same time consciously and deliberately utilizing data
16 mining to automatically and without notice providing user information to third-party advertisers
17 and Internet tracking companies. Apple profits from advertising revenues derived from its data
18 mining efforts from Plaintiff and the Class.

19 98. The obligation imposed by the implied covenant of good faith and fair dealing is
20 an obligation to refrain from opportunistic behavior. Apple has breached the implied covenant
21 of good faith and fair dealing in the Agreement through its policies and practices as alleged
22 herein. Plaintiff and the Class have sustained damages and seek a determination that the policies
23 and procedures of Apple are not consonant with Apple's implied duties of good faith and fair
24 dealing.

25 **NINTH CAUSE OF ACTION**
26 **(Common Law Invasion Of Privacy)**

27 99. Plaintiff hereby incorporates by reference the allegations contained in all of the
28 preceding paragraphs of this complaint.

1 **REQUEST FOR RELIEF**

2 WHEREFORE, Plaintiff Anthony Chiu, on behalf of himself and the Class, requests the
3 following relief:

4 A. An order certifying that this action is properly brought and may be maintained as
5 a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiff be appointed
6 as Class Representative, and that Plaintiff's counsel be appointed Class Counsel;

7 B. An award of damages, except as to the CLRA claim as alleged above in
8 paragraphs 75-84;

9 C. Restitution of all monies unjustly obtained or to be obtained from Plaintiff and
10 members of the Class;

11 D. Declaratory and injunctive relief;

12 E. An award of reasonable attorneys' fees and costs; and

13 F. Such other relief at law or equity as this court may deem just and proper.

14 **DEMAND FOR JURY TRIAL**

15 Plaintiff hereby demands trial of his claims by jury to the extent authorized by law.

16 DATED: January 27, 2011

17 **MILBERG LLP**
18 **JEFF S. WESTERMAN**
19 **SABRINA S. KIM**

20 
21 _____
22 **JEFF S. WESTERMAN**

23 One California Plaza
24 300 S. Grand Avenue, Suite 3900
25 Los Angeles, CA 90071
26 Telephone: (213) 617-1200
27 Facsimile: (213) 617-1975
28 E-mail: jwesterman@milberg.com
skim@milberg.com

Attorneys for Plaintiff

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

MILBERG LLP
SANFORD P. DUMAIN
PETER E. SEIDMAN
ANDREI V. RADO
ANNE MARIE VU (SBN 238771)
One Pennsylvania Plaza, 49th Floor
New York, NY 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229
E-mail: sdumain@milberg.com
pseidman@milberg.com
arado@milberg.com
avu@milberg.com

Attorneys for Plaintiff

REESE RICHMAN LLP
MICHAEL R. REESE (SBN 206773)
KIM RICHMAN
875 Avenue of the Americas, 18th Floor
New York, NY 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272
E-mail: mreese@reese-richman.com
krichman@reese-richman.com

Attorneys for Plaintiff