EXHIBIT A

Majed Nachawati
mn@fnlawfirm.com
FEARS | NACHAWATI LAW FIRM
4925 Greenville Avenue, Suite 715
Dallas, Texas 75206
Telephone: (214) 890-0711
Facsimile: (214) 890-0712

Jeremy R. Wilson
jeremy@wilsontrosclair.com
WILSON TROSCLAIR & LOVINS, P.L.L.C.
302 N. Market Street, Suite 510
Dallas, Texas 75202
Telephone: (214) 484-1930
Facsimile: (214) 276-1475

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

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DUSTIN FREEMAN, JARED PARSLEY, COLE PARR, and PRECIOUS ARRINGTON on Behalf of Themselves and All Others Similarly Situated

Plaintiffs,

v.

APPLE, INC., a Delaware Corporation; GOGII, INC., a Delaware Corporation; PANDORA MEDIA, INC., a California Corporation; BACKFLIP STUDIOS, INC., a Delaware Corporation; THE WEATHER CHANNEL, INC., a Georgia Corporation; DICTIONARY.COM, LLC, a California Corporation; OUTFIT7 LTD., a Foreign Corporation, ROOM CANDY, INC., a California Corporation, SUNSTORM INTERACTIVE, INC., an Indiana Corporation,

Defendants.

CASE NO. CV10 5881

COMPLAINT – CLASS ACTION

JURY TRIAL DEMAND

(1) Violation of CFAA, 18 U.S.C. § 1030;
(2) Violation of CLRA, Civ. Code § 1750, *et seq.*;
(3) Violation of California's Computer Crime Law, Penal Code § 502, *et seq.*;
(4) Violation of Bus. and Profs. Code § 17200, *et seq.*;
(5) Trespass;
(6) Conversion; and
(7) Unjust Enrichment.

On behalf of themselves and all others similarly situated, Plaintiffs, DUSTIN FREEMAN, JARED PARSLEY, COLE PARR, and PRECIOUS ARRINGTON sue Defendants, APPLE, INC., GOGII, INC., PANDORA INC., BACKFLIP STUDIOS, INC., THE WEATHER CHANNEL, INC., DICTIONARY.COM, LLC, OUTFIT7, LTD., ROOM CANDY, INC., and SUNSTORM INTERACTIVE, INC., and in support thereof, state:

This is a class action. Plaintiffs bring this action on their own behalf and on behalf of all similarly situated individuals.

I.

SUMMARY OF THE CASE

1. This lawsuit involves the intentional interception, by Defendants, of Plaintiffs' personally identifying information ("PII"). Defendants accomplish this by using iPhone and iPad mobile device applications ("Apps"). Defendants capture Plaintiffs' devices Unique Device ID ("UDID") – the unique identifying number that Apple, Inc. ("Apple") assigns to each of its iPhones and iPads – and transmits that information along with the devices' location data to third-party advertisers. Apple, as a joint venturer with the remaining Defendants, aids and abets this intentional taking and transmitting of Plaintiffs' PII. All of this is done without Plaintiffs' consent and in violation of their legal rights. Plaintiffs bring this lawsuit to rectify this wrong being systematically perpetrated upon them.

II.

INTRADISTRICT ASSIGNMENT

2. Defendant Apple, Inc.'s principle executive offices and headquarters are located in this District at 1 Infinite Loop, Cupertino, California 95014. Intradistrict assignment to the San Jose Division is proper.

III.

PARTIES

3. Plaintiff, DUSTIN FREEMAN, is a resident of Arlington in Tarrant County, Texas. At all times relevant to this action, Plaintiff FREEMAN has owned an iPhone and had the following iPhone Apps installed on his iPhone: Pandora, Paper Toss, and Weather Channel.

4. Plaintiff, JARED PARSLEY, is a resident of Royce City in Hunt County, Texas. At all times relevant to this action, Plaintiff PARSLEY has owned an iPhone and had the following iPhone Apps installed on his iPhone: Pandora, Paper Toss and TextPlus 4.

5. Plaintiff, COLE PARR, is a resident of Dallas in Dallas County, Texas. At all times relevant to this action, Plaintiff PARR has owned an iPhone and had the following iPhone Apps installed on his iPhone: Pimple Popper Lite, Pandora, Dictionary.com, Pumpkin Maker and Talking Tom Cat.

6. Plaintiff, PRECIOUS ARRINGTON, is a resident of Palmdale, California. At all times relevant to this action, Plaintiff ARRINGTON has owned an iPhone and had the following iPhone Apps installed on her iPhone: Pandora and Paper Toss.

7. Defendant, APPLE, INC. ("Apple"), is a California Corporation with its principal place of business in Cupertino, California. Apple manufactures and sells the popular mobile phone, the iPhone, as well as the iPad.

8. Defendant, GOGII, INC. ("Gogii"), is a Delaware Corporation with its principal place of business at 13160 Mindanao Way, Ste. 233, Marina Del Rey, California 90292. Defendant, Gogii, is the maker of the mobile device application ("App"), Textplus4.

9. Defendant, PANDORA MEDIA, INC., is a Delaware Corporation with its principal place of business at 2101 Webster Street, Ste. 1650, Oakland,

California 94612. Defendant, Pandora, is the maker of the iPhone App, Pandora.

10. Defendant, BACKFLIP STUDIOS, INC., is a Delaware Corporation with its principal place of business in Boulder, Colorado. Defendant, Backflip Studios Inc., is the maker of the iPhone App, Paper Toss.

11. Defendant, THE WEATHER CHANNEL, INC., is a Georgia Corporation with its principal place of business at 300 Interstate North Parkway SE, Atlanta, Georgia 30339-2403. Defendant, The Weather Channel, Inc., is the maker of the iPhone App, Weather Channel.

12. Defendant, DICTIONARY.COM, LLC, is a California Corporation with its principal place of business at 555 12th Street, Ste. 100, Oakland, California 94607. Defendant, Dictionary.com, LLC, is the maker of the iPhone App, Dictionary.com.

13. Defendant, OUTFIT7 LTD., is Slovenia limited company with its principal place of business at Palo Alto, California. Defendant, Outfit7 Ltd., is the maker of the iPhone App, Talking Tom Cat.

14. Defendant, ROOM CANDY, INC., is a California corporation with its principal place of business in San Marino, California. Defendant, Room Candy, Inc., is the maker of the iPhone App, Pimple Popper Lite.

15. Defendant, SUNSTORM INTERACTIVE, INC., is an Indiana corporation with its principal place of business at 9643 Oakhaven Court, Indianapolis, Indiana 46256. Defendant, Sunstorm Interactive, is the maker of the iPhone App, Pumpkin Maker.

IV.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this matter pursuant to 28 U.S.C. §1332 (federal diversity jurisdiction), as one or more members of the proposed class are residents of a different state from Defendants and the amount in

controversy likely exceeds the jurisdictional amount required by that code section. This Court has jurisdiction pursuant to 28 U.S.C. §1331 (federal question jurisdiction), as it involves allegations of violation of federal law. This Court has pendent jurisdiction of all alleged state law claims.

17. Venue is appropriate in this District because Defendant Apple, as well as certain members of the proposed class, are residents of this District and Defendants have committed torts within the Northern District of California.

18. Each of the Defendants in this action, other than Defendant Apple, sells or provides its mobile device application ("Apps") to any iPhone and iPad user who wishes to download them from the iTunes App Store. Each Defendant, other than Apple, has thus marketed and sold its product within the State of California and, upon information and belief, has sold or provided its products to millions of California residents. Furthermore, each non-California Defendant has contracted with a California company, Defendant Apple, to sell products on a nationwide basis. Defendant Apple is a resident of the State of California and is a resident of this District.

19. Thus, for those Defendants not residing within the State of California, there exist sufficient minimum contacts with the State of California, such that hailing them to answer for their violations of Plaintiffs' legal rights in the State of California does not offend traditional notions of fair play and substantial justice.

V.

STATEMENT OF FACTS

20. This is a consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

21. The basis for Plaintiffs' claims rest on Defendants' use of an intrusive tracking scheme implemented through the use of mobile device Apps on

Plaintiffs' iPhones and iPads.

22. Apps are computer programs that users can download and install on their mobile computer devices, including iPhones and iPads.

23. While Apps have been available for some time, it was with the introduction of Apple's iPhone in 2007 that Apps propelled themselves into a position of prominence in the daily lives of many mobile device users.

24. With features more like a laptop than a mobile phone, the iPhone enabled millions of mobile phone users to more effectively and more intuitively access the Internet and perform the computer functions that have become increasingly important in today's world. In addition, the iPhone features numerous games and other forms of entertainment for its users.

25. Unlike most earlier mobile phones, the iPhone allows users to install after-market programs, called Apps, onto their mobile device. This allows users, such as Plaintiffs, to customize their iPhones to perform functions other than those that the phones could perform when they were initially sold to the consumers.

26. Numerous other mobile device manufacturers have followed Apple's lead in allowing the installation of Apps on their users' mobile devices.

27. From the beginning, Apple has retained significant control over the software that users can place on their iPhones. Apple claims that this control is necessary to ensure smooth functioning of the iPhone. For instance, iPhone users are only allowed to download software specifically licensed by Apple. If a user installs any software not approved by Apple, the users' warranty is voided. If the user updates the operating system on their iPhone, the non-licensed software is erased by Apple.

28. Apple also retains a significant amount of control over the types of Apps it allows into its newly created market place. Whether an App is allowed to

be sold in the App Store is completely at the discretion of Apple. Apple requires that proposed Apps go through a rigorous approval process. Even if an App meets the "Program" requirements (as Apple describes it) the App can still be rejected by Apple for any reason at all. It is estimated that approximately twenty percent (20%) of all requests to place Apps for sale in the iTunes App Store are rejected by Apple. In exchange for Apple agreeing to allow the App developer to participate in its "Program," Apple retains thirty percent (30%) of all revenues from sales of the App.

29. Apple also exercises a significant amount of control over the functionality of the Apps that it allows into its "Program." For instance, Apple restricts how Apps interact with the iPhone's operating system and restricts Apps from disabling certain safety features of the iPhone.

30. Despite Apple's restrictions, Apple's App Store has been a huge success. As of October 20, 2010, there were at least 300,000 third-party applications officially available on the App Store, with over seven (7) billion total downloads. Market researcher, Gartner Inc., estimates that world-wide App sales this year will total $6.7 billion.

31. Apple's iPhone has also succeeded in helping to bring hand-held computing to the masses. Approximately fifty-nine (59) million people now have an iPhone. With the subsequent introduction of its iPad (estimated sales of 8.5 million in 2010), Apple has obtained a remarkable reach for its products.

32. Thanks in part to the iPhone's tremendous commercial success, mobile devices (including iPhones and iPads) are now used by many consumers in almost all facets of their daily lives, from choosing a restaurant, to making travel arrangements, to conducting bank transactions. Most consumers carry their mobile devices with them everywhere they go. While this convenience is valuable to consumers, so is the information that consumers put into their mobile devices.

33. Because Apps are software that users, such as Plaintiffs, download and install on their iPhone (which is a hand-held computer), Apps have access to a huge amount of information about a mobile device user. Apps can have access to such items as a mobile device's contacts list, username and password, and perhaps most importantly—the user's location information. Plaintiffs in this action consider the information on their phone to be personal and private information.

34. All of this information, however, is of extreme interest to many advertising networks. This information is also highly valuable. It is for this reason that many Apps are given away for free by the developer—just so that the App developer can sell advertising space on its App. Some advertising networks pay App developers to place banner ads within their Apps. Those ads are then populated with content from the third-party advertising network. In the process, those third-party advertisers are able to access various pieces of information from the user's iPhone, supposedly in order to serve ads to the App user that are more likely to be of interest to them.

35. Considering that mobile advertising is projected to be $1.5 billion a year industry by 2016, advertisers, website publishers, and ad networks are seeking ways to better track their web users and find out more about them. The ultimate goal of many advertising networks is to ascertain the identity of particular users so that advertisements can be tailored to their specific likes and dislikes.

36. Browser cookies are the traditional method used by advertisers to track web users' activities. But browser cookies have a large hurdle when it comes to an advertiser's ability to track a viewer – users often delete them because they do not want advertising companies to have information about them.

37. Defendants, however, have found their solution – the Unique Device ID ("UDID") that Apple assigns to every iPhone and iPad it manufactures. Ap-

ple's UDID is an example of a computing device ID generally known as a global unique identifier ("GUID"). A GUID is a string of electronically readable characters and/or numbers that is stored in a particular device or file (*e.g.*, piece of hardware, copy of software, database, user account) for purposes of subsequently identifying the device or file. Thus, a GUID is similar to a serial number in that it is so unique that it reliably distinguishes the particular device, software copy, file, or database from others, regardless of the operating environment.

38. Because the UDID is unique to each iPhone and iPad, it is an attractive feature for third-party advertisers looking for a means of reliably tracking a mobile device users' online activities. Because the UDID is not alterable or deletable by a iPhone or iPad user, some have referred to the UDID as a "supercookie." While not technically correct (because the UDID is on the device from the time of its manufacturing), this description aptly summarizes the desirability of access to the UDID from an advertising perspective.

39. Apple's UDID is concerning for several reasons. First, unlike with desktop computers, mobile devices travel most everywhere with the user. Also, mobile devices tend to be unique to an individual. While someone might borrow someone's mobile device briefly, it is unusual for individuals to frequently trade mobile devices with someone they know.

40. Furthermore, unlike a desktop computer, the iPhone and iPad come equipped with the tools necessary to determine their geographic location. Thus, being able to identify a unique device, and combining that information with the devices' geographic location, gives the advertiser a huge amount of information about the user of a mobile device. From the perspective of advertisers engaged in surreptitious tracking, this is a perfect means of tracking mobile device users' interests and likes on the Internet.

41. Apple certainly understands the significance of its UDID and users'

privacy, as, internally, Apple claims that it treats UDID information as "personally identifiable information" because, if combined with other information, it can be used to personally identify a user.

42. Unfortunately, however, unlike with browser cookies, Apple does not provide users any way to delete or restrict access to their devices' UDIDs. Traditional efforts to prevent Internet tracking, such as deleting cookies, have no effect on Apps' access to an iPhone's or iPad's UDID.

43. Apple has, however, recognized that it could go further to protect its users' private information from being shared with third parties. Thus, in April of 2010, Apple amended its Developer Agreement purporting to ban Apps from sending data to third-parties except for information directly necessary for the functionality of the App. Apple's revised Developer Agreement provides that "the use of third party software in Your Application to collect and send Device Data to a third party for processing or analysis is expressly prohibited."

44. This change prompted a number of third-party advertising networks (who have been receiving a steady flow of user data from iPhone and iPad Apps) to protest. One prominent critic was the CEO of AdMob. It appears that, as a result of this criticism, Apple has taken no steps to actually implement its changed Developer Agreement or enforce it in any meaningful way.

45. In this lawsuit, each of the non-Apple Defendants, through the use of Apps placed on Plaintiffs' mobile devices, accessed Plaintiffs' UDID and location information and transmitted that information to numerous third-party ad networks.

46. The general practice engaged in by Defendants was recently confirmed by Eric Smith, Assistant Director of Information Security and Networking at Bucknell University in Lewisburg, Pennsylvania and reported in his research report entitled, "iPhone Applications & Privacy Issues: An Analysis

of Application Transmission of iPhone Unique Device Identifiers (UDID's)" (last accessed December 19, 2010), online: http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf;

47. Further, the *Wall Street Journal*, as reported in the article "Your Apps Are Watching You," Scott Thurm and Yukari Iwatani Kane (December 18, 2010) independently confirmed that each non-Apple Defendant systematically uses its iPhone App to obtain iPhone users' UDID and location data and transmit it to multiple third parties.

48. None of the Defendants adequately informed Plaintiffs of their practices, and none of the Defendants obtained Plaintiffs' consent to do so.

49. Apple's 159-page, single spaced terms of service states: "By using any location-based services on your iPhone, you agree and consent to Apple's and its partners and licensees' transmission, collection, maintenance, processing, and use of your location data to provide such products and services." The iPad terms of service is nearly identical.

50. The following Apps, however, do not provide location based-services:

a. Paper Toss is a mobile device application owned by Defendant, Backflip Studios, Inc. Paper Toss is a gaming application that allows users to "throw" virtual paper balls into a digital wastebasket target. Paper Toss shares its UDID and/or users' Location (City, ZIP Code and Latitude/Longitude) with numerous third parties, including ad networks. No location based service is involved.

b. TextPlus4 is a mobile device application owned by Defendant, GOGII, Inc. TextPlus4 is a messaging application that allows users to send and receive text and picture messages. TextPlus 4 shares its users' UDID, Age, Gender, and and/or Location (ZIP Code) with

numerous third parties, including ad networks. No location based service is involved.

c. Dictionary.com is a mobile device application owned by Defendant, Dictionary.com, LLC. Dictionary.com is a reference application that allows users to look up the definition of various words and phrases. Dictionary.com shares its users' UDID and/or Location (City and ZIP Code) with numerous third parties, including ad networks. No location based service is involved.

d. Pandora is a mobile device application owned by Defendant, Pandora Media, Inc. Pandora is a music application that allows users to access, stream and download digital music files. Pandora shares its users' UDID and Age, Gender, and/or Location (City, ZIP Code and DMA Code) with third parties, including ad networks. No location based service is involved.

e. Talking Tom Cat is a mobile device application owned by Defendant, Outfit7 Ltd. Talking Tom Cat is an entertainment application that allows users to interact with a virtual pet cat that responds to touch and repeats everything said by the user with a funny voice. Talking Tom Cat shares its users' UDID and/or Location (ZIP Code), Phone ID, Username and Password with third parties, including ad networks. No location based service is involved.

f. Pumpkin Maker is a mobile device application owned by Defendant Sunstorm Interactive, Inc. Pumpkin Maker is a gaming application that allows users to carve virtual Jack-O-Lanterns and apply various Halloween themed backgrounds. Pumpkin Maker shares its users' UDID and/or Location (City, DMA2 Code and Latitude/Longitude) with third parties, including ad networks. No location based service

is involved.

51. There are simply no location based services involved in these Apps that would justify access to Plaintiffs' location data. When this information is combined with Plaintiffs' UDID information, it becomes personally identifying information. None of these Defendants adequately disclose to Plaintiffs that they are transmitting such information to third-party advertising networks.

52. In fact, prior to the Wall Street Journal report referenced above, the following Defendants did not have any privacy policy at all: BACKFLIP STUDIOS, INC. (Paper Toss App), OUTFIT7 LTD. (Talking Tom Cat), ROOM CANDY, INC. (Pimple Popper), and SUNSTORM INTERACTIVE, INC., (Pumpkin Maker).

53. The remaining non-Apple Defendant, the Weather Channel does appear to provide some location based services through its App, but still fails to sufficiently warn Plaintiffs that they are transmitting location data in conjunction with Plaintiffs' UDID to multiple third parties.

54. The UDID and location information obtained by each non-Apple Defendant was sent to multiple third-party advertising networks (in the case of Defendant Pandora, eight third parties).

55. As discussed above, Apple considers users' UDID information to be personally identifying information. By attempting to change its App Development criteria, Apple demonstrated that it is aware of the dangers posed by transmission of user data to third parties. Apple has simply failed to follow through on that conviction.

56. Plaintiffs and members of the proposed class were harmed by Defendants' actions in that their personal, private information was obtained without their knowledge or consent. Plaintiffs and members of the proposed class were harmed in that their personal property – their computer – was hijacked by

Defendants and turned into a device capable of spying on their every online move.

57. Plaintiffs' valuable UDID information, demographic information, location information, as well as their application usage habits is a valuable commodity that they could have sold to research firms. Plaintiffs also consider this information to be personal and private. Such information was taken from them without their knowledge or consent. Plaintiffs should be compensated for this harm. Plaintiffs are entitled to compensation for this invasion of their privacy.

58. Each of the non-Apple Defendants is liable to Plaintiffs for violation of their statutory and common-law rights. Defendant Apple, by exercising significant control over App developers and sharing profits with them, has created a "community of interest" with the other Defendants to render them joint venturers, who are responsible for each other's torts. Defendant Apple has also aided and abetted the remaining Defendants in the commission of their legal wrongs against Plaintiffs and the proposed class. Based on the above, Apple has acted sufficiently in concert with the remaining Defendants to impose liability.

59. Plaintiffs and members of the proposed class bring this action to redress this illegal and intrusive scheme designed by Defendants to intrude into their personal lives and collect personal information about them.

60. Plaintiffs seek damages for their injuries, an injunction to protect those not yet harmed by these illegal activities, and, where legally available, attorneys' fees and other costs associated with the bringing of this action.

Defendant Apple Aided and Abetted the Other Defendants

61. Defendant Apple knew or should have known the other Defendants' conduct constituted a breach of those Defendants' duties to Plaintiffs and the Class.

62. Defendant Apple gave substantial assistance to the other Defendants in committing the acts alleged in this Complaint. Furthermore, Apple had a duty to Plaintiffs and the Class to take steps to prevent such harm.

63. Such conduct by Apple constitutes Aiding and Abetting pursuant to California law and imposes liability on Defendant Apple for the other Defendant's torts, as outlined below.

Defendant Apple is in a Joint Venture with the Other Defendants

64. Defendant Apple's conduct and that of the remaining Defendants constitutes an undertaking by two or more persons jointly to carry out a single business enterprise for profit.

65. By reviewing each App, setting the conditions for and requirements for Apps to be sold and partnering with the above-named App developers in the sale of those Apps, Apple has created a "community of interest" in a common undertaking of which each partner has or exercises the right of control and direction of the undertaking.

66. By sharing the profits of all App sales of the other Defendants' applications through the iTunes App store, Apple is a joint venture with each of the remaining Defendants.

67. All members of a joint venture are jointly and severally liable for injuries resulting from the tortious conduct of one of the joint venturers, Apple is thus legally responsible for the tortuous conduct alleged in each of the Counts.

VI.

CLASS ACTION ALLEGATIONS

68. Pursuant to Fed. R. Civ. P. 23(b)(3), and 23(b)(2) Plaintiffs bring this action on behalf of themselves, and all others similarly situated, as representatives of the following class (the "Class"):

> Each and every individual in the United States of America who has placed one of Defendants' iPhone Apps or iPad Apps

on their iPhone or iPad in the four years preceding the filing of this lawsuit (the "Class").

Excluded from the class are Defendants as well as all employees of this Court, including, but not limited to, Judges, Magistrate Judges, clerks and court staff and personnel of the United States District Courts of the Northern District of California, the United States Court of Appeals for the Ninth Circuit and the United States Supreme Court; their spouses and any minor children living in their households and other persons within a third degree of relationship to any such Federal Judge; and finally, the entire jury venire called to for jury service in relation to this lawsuit. Also excluded from the class are any attorneys or other employees of any law firms hired, retained and/or appointed by or on behalf of the named Plaintiffs to represent the named Plaintiffs and any/or any proposed class members or proposed class in this lawsuit.

Furthermore, to the extent that undersigned counsel has any legal interest to damages or other monetary relief, or other relief due to the putative class (or any other rights as potential putative class members), arising as a result of the causes of action asserted in this litigation, such interest is hereby disclaimed by undersigned counsel.

69. The requirements of Fed. R. Civ. P. 23 are met in this case. The Class, as defined, is so numerous that joinder of all members is impracticable. Although discovery will be necessary to establish the exact size of the class, it is likely, based on the nature of Defendants' businesses, that it numbers in the millions.

70. There are questions of fact and law common to the Class as defined, which common questions predominate over any questions affecting only individual members. The common questions include:

a. whether Defendants, as a regular practice, obtained and disseminated the class' personally identifiable information without their knowledge and consent, or beyond the scope of their consent;

b. whether Defendants failed to disclose material terms regarding the collection and dissemination of the class' personally identifiable information;

c. what use was made of the class' personally identifiable information, including to whom the information was sold for a profit;

d. whether Defendants used iPhone Apps or iPad Apps to send Plaintiffs' UDID, location, and/or Username/password information to third parties; and

e. whether Plaintiffs' personally identifiable information was used to track their activity.

71. Plaintiffs can and will fairly and adequately represent and protect the interests of the Class as defined and have no interests that conflict with the interests of the Class. This is so because:

a. All of the questions of law and fact regarding the liability of the Defendants are common to the class and predominate over any individual issues that may exist, such that by prevailing on their own claims, Plaintiffs will necessarily establish the liability of the Defendants to all class members;

b. Without the representation provided by Plaintiffs, it is unlikely that any class members would receive legal representation to obtain the remedies specified by relevant statutes and the common law;

c. Plaintiffs have retained competent attorneys who are experienced in the conduct of class actions. Plaintiffs and their counsel have the necessary resources to adequately and vigorously litigate this class action, and Plaintiffs and their counsel are aware of their fiduciary responsibility to the class members and are determined to diligently discharge those duties to obtain the best possible recovery for the Class.

72. Defendants' actions have affected numerous consumers in a similar way. The class action is superior to any other method for remedying Defendant's actions given that common questions of fact and law predominate. Class treatment is likewise indicated to ensure optimal compensation for the Class and limiting the expense and judicial resources associated with thousands of potential claims.

VII.

CAUSES OF ACTION

COUNT I – COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

(By Plaintiffs Against All Defendants)

73. Plaintiffs incorporate by reference each proceeding and succeeding paragraph as though set forth fully at length herein.

74. By accessing and transmitting Plaintiffs' UDID and location data on the computers of Plaintiffs and members of the class, Defendants have accessed Plaintiffs' computers, in the course of interstate commerce and/or communication, in excess of the authorization provided by Plaintiffs as described in 18 U.S.C. § 1030(a)(2)(C).

75. Defendants violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing Plaintiffs' and members of the class's computers without authorization and/or by exceeding the scope of that authorization.

76. Plaintiffs' computers, and those of the class, are protected computers pursuant to 18 U.S.C. § 1030(e)(2)(B).

77. Defendants thus further violated the Act by causing the transmission of a program, information, code or command and as a result caused harm aggregating at least $5,000 in value.

78. Defendants' actions were knowing and/or reckless and, as outlined above, caused harm to Plaintiffs and members of the proposed class.

79. Plaintiffs seek recovery for this loss, as well as injunctive relief, to prevent future harm.

COUNT II – CONSUMER LEGAL REMEDIES ACT,
CAL. CIV. CODE § 1750, ET SEQ.
(By Plaintiffs Against All Defendants)

80. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

81. In violation of Civil Code section 1750, et. seq. (the "CLRA"), Defendants have engaged in and are engaging in unfair and deceptive acts and practices in the course of transactions with Plaintiffs, and such transactions are intended to and have resulted in the sales of services to consumers. Plaintiffs and the Class Members are "consumers" as that term is used in the CLRA because they sought or acquired Defendants' good or services for personal, family, or household purposes. Defendants' past and ongoing acts and practices include but are not limited to:

a) Defendants' representations that their services have characteristics, uses, and benefits that they do not have, in violation of Civil Code § 1770(a)(5);

b) Defendants' representations that their services are of a particular standard, quality and grade but are of another standard quality and grade, in violation of Civil Code § 1770(a)(7); and

c) Defendants' advertisement of services with the intent not to sell those services as advertised, in violation of Civil Code § 1770(a)(9).

82. Defendants' violations of Civil Code § 1770 have caused damage to Plaintiffs and the other Class members and threaten additional injury if the violations continue. This damage includes the losses set forth above.

83. At this time, Plaintiffs only seek injunctive relief for Defendants' violations of this statute. Pursuant to California Civil Code Section 1782, and to the extent that this complaint is not sufficient written notice, Plaintiffs will notify Defendants in writing of the particular violations of Civil Code Section 1770 and

demand that Defendants rectify the problems associated with their behavior detailed above, which acts and practices are in violation of Civil Code § 1770.

84. If Defendants fail to respond adequately to Plaintiffs' above described demand within 30 days of Plaintiffs' notice, pursuant to California Civil Code, Section 1782(b), Plaintiffs will amend the complaint to request damages and other relief, as permitted by Civil Code, Section 1780.

COUNT III - CALIFORNIA'S COMPUTER CRIME LAW, CAL. PENAL CODE § 502

(By Plaintiffs Against All Defendants)

85. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

86. The California Computer Crime Law, California Penal Code § 502, referred to as "CCCL" regulates "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."

87. Defendants violated California Penal Code § 502 by knowingly accessing, copying, using, made use of, interfering, and/or altering, data belonging to Plaintiffs and Class members: (1) in and from the State of California; (2) in the home states of the Plaintiffs; and (3) in the state in which the servers that provided the communication link between Plaintiffs and the websites they interacted with were located.

88. Pursuant to California Penal Code § 502(b)(1), "Access means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network."

89. Pursuant to California Penal Code § 502(b)(6), "Data means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or

as stored in the memory of the computer or in transit or presented on a display device."

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

91. Defendants have violated California Penal Code § 502(c)(2) by knowingly accessing and without permission, taking, or making use of data from Plaintiffs' computers.

92. Defendants have violated California Penal Code § 502(c)(3) by knowingly and without permission, using and causing to be used Plaintiffs' computer services.

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

94. Defendants have violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' computer, computer system, and/or computer network.

95. California Penal Code § 502(j) states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

96. Plaintiffs have also suffered irreparable injury from these unauthorized acts of disclosure, to wit: their personal, private, and sensitive

electronic data was obtained and used by Defendants. Due to the continuing threat of such injury, Plaintiffs have no adequate remedy at law, entitling Plaintiffs to injunctive relief.

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

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

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

COUNT IV – UNFAIR COMPETITION LAW,
CAL. BUS. & PROF. CODE § 17200
(By Plaintiffs Against All Defendants)

100. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

101. In violation of California Business and Professions Code § 17200 et. seq. (the "UCL"), Defendants' conduct in this regard is ongoing and includes, but is not limited to, unfair, unlawful and fraudulent conduct.

102. By engaging in the above-described acts and practices, Defendants have committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and/or property—specifically, personal information.

103. Defendants' business acts and practices are unlawful, in part,

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

104. Defendants' business acts and practices are also unlawful in that they violate the California Consumer Legal Remedies Act, 1750, *et seq.*, California Penal Code section 502, and Title 18, United States Code, Section 1030. Defendants are therefore in violation of the "unlawful" prong of the UCL.

105. Defendants' business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiffs and Class Members and for which Defendants has no justification other than to increase, beyond what Defendants would have otherwise realized, their profit in fees from advertisers and their information assets through the acquisition of consumers' personal information. Defendants' conduct lacks reasonable and legitimate justification in that Defendants have benefited from such conduct and practices while Plaintiffs and the Class Members have been misled as to the nature and integrity of Defendants' services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendants' conduct offends public policy in California tethered to the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material information that enables them to safeguard their own privacy interests, including California Civil Code, Section 1798.80.

106. In addition, Defendants' modus operandi constitutes a sharp practice in that Defendants knew, or should have known, that consumers care about the

status of personal information but were unlikely to be aware of the manner in which Defendants failed to fulfill their commitments to respect consumers' privacy. Defendants are therefore in violation of the "unfair" prong of the UCL.

107. Defendants' acts and practices were fraudulent within the meaning of the UCL because they are likely to mislead the members of the public to whom they were directed.

COUNT V – TRESPASS TO PERSONAL PROPERTY

(By Plaintiffs Against All Defendants)

108. Plaintiffs incorporate by reference each proceeding and succeeding paragraph as though set forth fully at length herein.

109. By obtaining UDID and location data from Plaintiffs' and members of the Class' computers without their consent or knowledge, Defendants have improperly exercised dominion and control over Plaintiffs' and members of the Class's personal property – their computer.

110. Defendants' actions were done knowingly and intentionally.

111. Defendants' actions caused harm to Plaintiffs and members of the proposed class, as described above.

112. Plaintiffs and the proposed class seek damages for this harm as well as injunctive relief to remedy this harm.

COUNT VI – COMMON LAW CONVERSION

(By Plaintiffs Against All Defendants)

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

114. Defendants have taken Plaintiffs property in the form of information about them that is private and personal.

115. Plaintiffs have been harmed by this exercise of dominion and control over their information.

116. Plaintiffs bring this case seeking recovery for their damages and appropriate injunctive relief.

COUNT VII-UNJUST ENRICHMENT/

RESTITUTION

(By Plaintiffs Against All Defendants)

117. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

118. Defendants have improperly and illegally profited from the obtainment and/or sale of Plaintiffs' and members of the class' personal, private data. Defendants' actions have been done knowingly and secretively with the intent that Plaintiffs not realize what was being done.

119. These actions constitute violations of both statutory as well as common law obligations as outlined above.

120. Under the principles of equity and good conscience, Defendants should not be permitted to retain the benefits they have acquired through this unlawful conduct. All funds, revenues and benefits that Defendants have unjustly received as a result of their actions rightfully belong to Plaintiffs and the Class.

WHEREFORE, Plaintiffs demand judgment on their behalf and on behalf of the other members of the Class to the following effect:

a. declaring that this action may be maintained as a class action;

b. granting judgment in favor of Plaintiffs and the other members of the Class against the Defendants;

c. treble and/or punitive damages should the Court find that the Defendants acted in willful or reckless disregard of the law;

d. declarations that Defendants' acts and practices alleged herein are wrongful;

e. an order directing restitution or disgorgement in an allowable amount to be proven at trial;

f. compensatory damages in an amount to be proved at trial;

g. pre and post judgment interest to the maxim extent permissible;

h. an award to Plaintiffs and the class of their costs and expenses incurred in this action, including reasonable attorneys' fees, to the extent permissible;

i. injunctive relief preventing Defendant from further collecting and disseminating the Class' personally identifiable information and/or requiring more detailed disclosure and informed consent from the Class regarding this activity; and

j. such other relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all issues so triable.

Respectfully submitted,

Dated: December 23, 2010

PARISI AND HAVENS LLP

By: _____

David C. Parisi (SBN 162248)
15233 Valleyheart Drive
Sherman Oaks, CA 91403-1545
Telephone: 818-990-1299
Facsimile: 818-501-7852
Email: dcparisi@parisihavens.com

FEARS | NACHAWATI LAW FIRM

Majed Nachawati
State Bar No. 24038319
mn@fnlawfirm.com
Bryan Fears
State Bar No. 24040886

4925 Greenville Ave, Suite 715
Dallas, Texas 75206
Telephone: (214) 890-0711
Facsimile: (214) 890-0712

WILSON TROSCLAIR & LOVINS, P.L.L.C.

Jeremy R. Wilson
State Bar No. 24037722
Kenneth P. Trosclair
State Bar No. 24033548
302 N. Market St., Suite 510
Dallas, Texas 75202
Telephone: (214) 484-1930
Facsimile: (214) 276-1475

ATTORNEYS FOR PLAINTIFFS
(pro hac vice application pending)

DECLARATION OF DAVID C. PARISI

I, David C. Parisi, hereby declare on oath as follows:

1. I am an attorney licensed to practice law in the state of California. I am over the age of 18 years and I have personal knowledge of the matters attested to herein. If called upon to testify, I would and could competently do so.

2. I make this declaration pursuant to California Civil Code section 1780(c) on behalf of my clients, Plaintiffs DUSTIN FREEMAN, JARED PARSLEY, COLE PARR and PRECIOUS ARRINGTON, on behalf of themselves and all others similarly situated.

3. Defendant, Apple, Inc. is a California Corporation with its principal place of business at 1 Infinite Loop, Cupertino, California 95014.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Dated this 23rd day of December at Sherman Oaks, California.