IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ALABAMA

SOUTHERN DIVISION

MARCIA BURKE and WILLIAM C. BURKE, III, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, vs. **APPLE, INC.**, a Delaware Corporation; **PANDORA MEDIA, INC.**, a California Corporation; **DOES 1-10**, Defendants.	Case No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

On behalf of themselves and all others similarly situated, Plaintiffs MARCIA BURKE and WILLIAM C. BURKE, JR. bring this action against Defendants, APPLE, INC., PANDORA, INC., and DOES 1-10, inclusive (collectively, "Defendants"), in support thereof allege as follows, all on information and belief except where specifically identified, which allegations are likely to have evidentiary support after further investigation and discovery:

INTRODUCTION

1. This lawsuit involves the intentional interception, by Defendants, of Plaintiffs' personally identifying information ("PII") data by using iPhone and iPad mobile device applications ("Apps") without consumers' knowledge or advance and informed consent. Defendants capture Plaintiffs' devices Unique Device ID ("UDID") – the unique identifying

number that Apple, Inc. ("Apple") assigns to each of these 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.

JURISDICTION

2. This Court has jurisdiction over this action 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.

VENUE

3. Venue is proper pursuant to 28 U.S.C. §1391 because a substantial part of the events or omissions giving rise to the claim occurred in the Northern District of Alabama and because Defendants:

a. are authorized to conduct business in this District and have intentionally availed themselves of the laws and markets within this District through the promotion, marketing, distribution and sale of their products in the Northern District of Alabama;

b. conduct substantial business in the Northern District of Alabama; and

c. are subject to personal jurisdiction in the Northern District of Alabama. The Court has personal jurisdiction over Defendant because they are corporations that have sufficient minimum contacts in Alabama, otherwise intentionally avail themselves of the Alabama market through their marketing and sales of the Products in the State of Alabama, and/or by having such other contacts with Alabama so as to render the exercise of jurisdiction

over them by the Alabama courts consistent with traditional notions of fair play and substantial justice.

PARTIES

4. On personal knowledge, Plaintiff, MARCIA BURKE, is a resident of Tuscaloosa County, Alabama and has owned an iPhone and had the Pandora iPhone App installed on her iPhone during the Class period. None of the Defendants adequately disclosed to Plaintiff either before or after downloading the App that they were transmitting personal data about her to third-party advertising networks as set forth below, and she would not have used this App to the extent she has, if at all, had the true facts been timely disclosed.

5. On personal knowledge Plaintiff, WILLIAM C. BURKE, JR., is a resident of Tuscaloosa County, Alabama, and has owned an iPhone and had the Pandora iPhone App installed on his iPhone during the Class period. None of the Defendants adequately disclosed to Plaintiff either before or after downloading the App that they were transmitting personal data about him to third-party advertising networks as set forth below, and he would not have used this App to the extent he has, if at all, had the true facts been timely disclosed.

6. Defendant, APPLE, INC. ("Apple"), is a California corporation with its principal place of business lat 1 Infinite Loop, Cupertino, California 95014. Apple manufactures and sells the popular mobile phone, the iPhone, as well as the iPad.

7. Defendant PANDORA MEDIA, INC. ("Pandora"), is a Delaware Corporation with its principal place of business at 2101 Webster Street, Suite 1650, Oakland, California 94612. Defendant, Pandora, is the maker of the iPhone App, Pandora.

8. DOES 1-10 are individuals, associations or corporations that are affiliated or related to Defendants, who will be specifically identified and named as discovery progresses and their roles in the wrongdoing at issue is revealed.

9. At all times mentioned in the Causes of Action alleged herein, each and every Defendant was an agent, representative, affiliate, or joint venturer of each and every other Defendant, and in doing the things alleged in the Causes of Action stated herein, each and every

Defendant was acting within the course and scope of such agency, representation, affiliation, or venture and was acting with the consent, permission and authorization of the other Defendants.

10. During the relevant time period, Defendants agreed to misrepresent to the Class members the material facts at issue herein and/or not to notify Class members about the scope and nature of the illegal business practices as detailed herein, thus engaging in a conspiracy that resulted in injury in fact to members of the Class, which conspiracy is still on-going.

11. All actions of each Defendant, as alleged in the Causes of Action stated herein, were ratified and approved by the other Defendants or their respective directors, officers and/or managing agents, as appropriate for the particular time period alleged herein.

12. Whenever this Complaint refers to any act or acts of Defendants, the reference also is to mean that the directors, officers, employees, affiliates, or agents of the responsible defendant authorized such act while actively engaged in the management, direction or control of the affairs of Defendants and/or by persons who are the alter egos of Defendants,

13. To the extent this Complaint refers to the actions of individuals, the reference also is to mean that such acts were taken while such persons were acting within the scope of their agency, affiliation, or employment.

14. Whenever this Complaint refers to any act of Defendants, the reference shall be deemed to be the act of each defendant, jointly and severally.

STATEMENT OF FACTS

15. This is a consumer class action lawsuit pursuant to Federal Rules of Civil Procedure 23(a) and (b)(2)/(b)(3).

16. The basis for Plaintiffs' claims rest on Defendants' collective use of an intrusive tracking scheme implemented through the use of mobile device Apps on Plaintiffs' iPhones and iPads.

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

18. 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.

19. 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. These electronic high speed data processing devices are capable of performing logical, arithmetic, or storage functions and as a data storage or communications facility, and are intended to be used in interstate or foreign commerce or communications.

20. 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.

21. Apple, as well as each of the Defendants, is aware of what type of personal consumer information is required and gathered by an App installed on an iPhone or iPad, because 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.

22. 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.

23. Apple also retains a significant amount of control over the types of Apps it allows. 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 Apps.

24. 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.

25. 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 seven (7) billion total downloads. Market researcher, Gartner Inc., estimates that world-wide App sales this year will total $6.7 billion.

26. Approximately fifty-nine (50) 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.

27. Thanks in part to the iPhone's tremendous commercial success, mobile devices (including iPhones and iPads) are now used by many consumers in numerous facets of their daily lives, from making travel arrangements to conducting banking transactions. While this convenience is valuable and material to consumers who purchase these products and is a substantial factor in them doing so, the information that consumers put into their mobile devices is equally important and not intended to be publicly shared.

28. Because Apps are software that users, such as Plaintiffs, download and install on their iPhone, 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.

29. 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, 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.

30. Just as with the advent of widespread use of the internet back in the late 1990s, considering that mobile advertising is projected to be a $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.

31. A piece of software known as "browser cookies" are the traditional method used by advertisers to track web users' activities. Browser cookies have a large hurdle when it comes to an advertiser's ability to track a viewer – users can delete them because they do not want advertising companies to have information about them.

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

33. 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." This description aptly summarizes the desirability of access to the UDID from an advertising perspective.

34. These types of software can potentially be more intrusive than traditional cookies. 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.

35. 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.

36. Apple 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.

37. 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.

38. 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."

39. This change prompted a number of third-party advertising networks who have (undisclosed to users) 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.

40. Each of the non-Apple Defendants, through the use Apps placed on Plaintiffs' mobile devices, either accessed Plaintiffs' UDID and location information and transmitted that information to numerous third-party ad networks or conspired with the other Defendants to keep that information hidden from the general public.

41. The general practice engaged in by Defendants as described above was brought to light 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 (UDIDs)" (online: http://www.pskl.us/wp/wp-content/uploads/ 2010/09/iPhone-Applications-Privacy-Issues.pdf.)

42. 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.

43. None of the Defendants adequately informed Plaintiffs or Class members of their practices or obtained Plaintiffs' consent to do so.

44. Apple's 15-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.

45. 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.

46. There are 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 PII. None of these Defendants adequately disclosed to Plaintiffs or Class members that they are transmitting such information to third-party advertising networks.

47. What makes such unauthorized access all the more alarming is that these devices record consumers' actual geographic locations. According to an April 21, 2011 article in the *International Business Times* entitled "How Apple's iPhone and iPad Secretly Store A Users' Location Data" (http://www.ibtimes.com/articles/136838/20110421), researchers Pete Warden and Alasdair Allan reported in *TechTree* that they have discovered that iPhones and 3G iPads that use the iOS4 operating system regularly record users' position into a hidden database file called consolidated.db, stored in a folder Users// Library/ApplicationinsideSupport/MobileSync/Backups/. The Manifest.mbdb and Manifest.mbdx files contain a listing of the real names of the files represented by random strings in that folder. These folders store a long list of latitude-longitude coordinates and timestamps by the second. The coordinates are not always exact, but there are typically tens of thousands of data points. The location is likely being determined by cell-tower triangulation, either triggered by traveling between cells or activity on the device itself. Furthermore, all this data is being stored across backups, and even device migrations.

48. To make matters worse, the file on the devices with said data is unencrypted and unprotected, and is on any machine synced with such devices. According to Warden and Allan, the key problem is: "That this data is stored in an easily-readable form on your machine. *Any other program you run or user with access to your machine can look through it*. [Emphasis added.]" While cellular telephone companies have always collected such data, it is kept behind company firewalls and takes a court order to access it. Now this information is sitting in plain view on these devices, unprotected from the world. It is not clear why Apple is gathering these data points, although the way it is implemented shows that it is intentional. While the researchers reported that from what they could tell the data are not being siphoned from the

device to another source, it would be quite easy if they are not already doing so for Defendants, having previously accessed the devices using unauthorized means, to locate such data. Indeed, there is evidence that in fact this occurs, since devices operating outside the United States that run various Apps deliver foreign language or foreign country advertisements, which would be possible if present location based data were being transmitted to third party advertisers.

49. 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, this information was sent to eight third parties.

50. As discussed above, Apple considers users' UDID information to be PII data. 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.

51. Plaintiffs and members of the Class were injured in fact and lost control of their personal property by Defendants' actions in that their personal, private PII data were obtained by third parties they were not dealing with without or beyond their knowledge or consent -- similar to confidentially providing an individual with their unlisted cellular telephone number and then having them publicly announce it. Plaintiffs and members of the Class were further harmed in that their personal property in terms of their iPhone or their iPad was hijacked and turned into a device capable of spying on their every online move.

52. Plaintiffs' valuable UDID information, demographic information, location information, as well as their application usage habits is a valuable commodity that has a property value to research firms. Indeed, the non-Apple Defendants are paid money by third party advertisers in exchange for having access to such information, demonstrating a market value for such data. Plaintiffs also consider this information to be personal and private data. Such information was taken from them without their knowledge or consent. Plaintiffs should be compensated for this harm and are entitled to compensation for this invasion of their privacy.

53. Each of the non-Apple Defendants is liable to Plaintiffs and the Class 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 in that they are all equally aware of, but did not disclose, the extent of their information gathering capabilities. Defendant Apple has also aided and abetted the remaining Defendants in the commission of their legal wrongs against Plaintiffs and the Class. Based on the above, Apple and the other Defendants have acted sufficiently in concert with each other to impose liability as to all Class members.

54. Plaintiffs and members of the 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 without first obtaining their advance authorization and consent.

55. Plaintiffs seek monetary relief 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

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

57. 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.

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

Defendant Apple is in a Joint Venture with the Other Defendants

59. 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.

60. 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.

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

62. All members of a joint venture are jointly and severally liable for injuries resulting from the tortuous conduct alleged in each of the Counts.

CLASS ACTION ALLEGATIONS

63. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3) 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 the Defendants' iPhone Apps or iPad Apps on their iPhone or iPad in the four years preceding December 18, 2010 (the "Class").
>
> Excluded from the Class are Defendants as well as all employees of the judges assigned to this action in this Court, their spouses and any minor children living in their households and other persons within a third degree 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.

64. 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 of persons.

65. 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 members' PII data without their knowledge and without first adequately containing their consent, or beyond the scope of any consent adequately obtained;

b. whether Defendants failed to disclose material terms regarding the collection and dissemination of the Class members' PII data;

c. what use was made of the Class members' PII data, 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' PII data were used to track their activity.

66. Plaintiffs can and will fairly and adequately represent and protect the interests of the Class as defined and have no interests that materially 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.

67. Defendants' actions have affected numerous consumers in a similar way. This class action is superior to any other method for remedying Defendants' 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.

CAUSES OF ACTION

COUNT I

COMPUTER FRAUD AND ABUSE ACT ("CFAA"), 18 U.S.C. § 1030

(By Plaintiffs Against All Defendants)

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

69. By accessing and transmitting Plaintiffs' UDID and location data on the devices of Plaintiffs and members of the Class, Defendants have accessed Plaintiffs' devices, 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).

70. Defendants violated 18 U.S.C. §1030(a)(2)(C) by intentionally accessing Plaintiffs' and members of the Class's devices without having first received informed authorization and consent and/or by exceeding the scope of that authorization.

71. Plaintiffs' devices, and those of the Class, satisfy the definition of "protected computers" pursuant to 18 U.S.C. §1030(e)(2), as the devices in question are an electronic or other high speed data processing device that perform logical, arithmetic, or storage functions, including as a data storage facility or communications facility directly related to or operating in conjunction with such devices and is used in or affecting interstate or foreign commerce or communications.

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

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

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

COUNT II

TRESPASS TO PERSONAL PROPERTY

(By Plaintiffs Against All Defendants)

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

76. By obtaining UDID and location data from Plaintiffs' and members of the Class' devices without or beyond the scope of their consent or knowledge, Defendants have improperly exercised dominion and control over Plaintiffs' and members of the Class's personal property.

77. Defendants' actions were done knowingly and intentionally.

78. Defendants' actions caused harm to Plaintiffs and members of the Class, as described above.

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

COUNT III

COMMON LAW CONVERSION

(By Plaintiffs Against All Defendants)

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

81. Defendants have taken Plaintiffs' property in the form of PII data about them that is private and personal.

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

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

COUNT IV

COMMON COUNTS, ASSUMPSIT, AND UNJUST ENRICHMENT/RESTITUTION

(By Plaintiffs Against All Defendants)

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

85. Defendants entered into a series of implied at law contracts with Plaintiffs and the Class that resulted in money being had and received by Defendants at the expense of Plaintiffs and members of the Class under agreements in assumpsit. Defendants have been unjustly enriched by the resulting profits enjoyed by Defendants as a result of such agreements. Plaintiffs' detriment and Defendants' enrichment were related to and flowed from the conduct challenged in this Complaint.

86. Under common law principles recognized in claims of common counts, unjust enrichment, restitution and/or assumpsit, Defendants should not be permitted to retain the benefits conferred upon them based on the taking of PII data from Plaintiffs and Class members and converting it into revenues and profits.

87. Under the principles of equity and good conscience, Defendants should not be permitted to retain the benefits they have acquired through the unlawful conduct described above.

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

89. Plaintiffs and members of the Class seek restitutionary disgorgement of all profits of such amounts and the establishment of a constructive trust from which Plaintiffs and Class members may seek restitution, as all funds, revenues and benefits that Defendants have unjustly received as a result of their actions rightfully belong to Plaintiffs and the Class. Plaintiffs also seek declaratory relief as to the rights and responsibilities of all parties to such implied at law agreements.

WHEREFORE, Plaintiffs demand judgment on their behalf and on behalf of the other members of the Class to the following effect, as appropriate and applicable for the particular cause of action:

1. Declaring that this action may be maintained as a class action;

2. Granting judgment in favor of Plaintiffs and the other members of the Class against Defendants;

3. Exemplary damages should the Court find that the Defendants acted in willful or reckless disregard of the law;

4. Declarations that Defendants' acts and practices alleged herein are wrongful;

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

6. Statutory or compensatory damages in an amount to be proved at trial;

7. Pre- and post-judgment interest to the maximum extent permissible;

8. An award to Plaintiffs and the Class of their costs and expenses incurred in this action, including reasonable attorneys' fees, to the extent permissible;

9. Injunctive relief preventing Defendant from further collecting and disseminating the Class' PII data and/or requiring more detailed disclosure and informed consent from the Class regarding this activity; and

10. Such other relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

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

DATED: April 22, 2011

Respectfully Submitted,

/s/ E. Kirk Wood
E. Kirk Wood (ASB-2397-W55E)
Attorney for Plaintiffs

OF COUNSEL:
E. Kirk Wood
Wood Law Firm, LLC
P.O. Box 382434
Birmingham, Alabama 35238-2434
Telephone: (205) 612-0243
Facsimile: (866) 747-3905
ekirkwood1@bellsouth.net

REQUESTS FOR SERVICE BY CERTIFIED MAIL

Pursuant to MRCP 4.1 and 4.2, Plaintiffs request service of the foregoing Complaint by certified mail.

By: /s/ E. Kirk Wood
E. Kirk Wood
Attorney for Plaintiffs

SERVE DEFENDANTS BY CERTIFIED MAIL AS FOLLOWS:

Apple, Inc.
1 Infinite Loop
Cupertino, California 95014-2084

Pandora Media, Inc.
2101 Webster Street, Suite 1650
Oakland, California 94612