IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

LYMARIS M. RIVERA DIAZ, Individually, and on behalf of all others similarly situated, Plaintiff(s) v. APPLE, INC.; PANDORA MEDIA, INC.; THE WEATHER CHANNEL, INC., and DOES 1-10 Defendants	CIVIL NO. 11-1433 PLAINTIFF(S) DEMAND TRIAL BY JURY

CLASS ACTION COMPLAINT

On behalf of themselves and all others similarly situated, Plaintiff(s) bring this action against Defendants, APPLE, INC., PANDORA, INC., THE WEATHER CHANNEL, 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:

I. INTRODUCTION

1. This lawsuit involves the intentional interception, by Defendants, of Plaintiff(s)' personally identifying information ("PII") data by using iPhone and iPad mobile device application(s) ("App(s)") without consumers' knowledge or advance and informed consent. Defendants capture Plaintiff(s)' 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 Plaintiff(s)' PII. All of this is done without Plaintiff(s)' consent and in violation of their legal

rights. Plaintiff(s) bring this lawsuit to rectify this wrong being systematically perpetrated upon them.

II. JURISDICTION AND VENUE

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.

3. Venue is proper pursuant to *28 U.S.C. §1391* because, members of the proposed class are residents of this District, Defendants have committed torts within this District, a substantial part of the events or omissions giving rise to the claim occurred in the District of Puerto Rico 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 District of Puerto Rico;

B. Conduct substantial business in the District of Puerto Rico; and

C. Are subject to personal jurisdiction in the District of Puerto Rico.

4. The Court has personal jurisdiction over the Defendants because they are corporations that have sufficient minimum contacts in Puerto Rico, otherwise intentionally avail themselves of the Puerto Rico market through their marketing and sales of the Products in Puerto Rico, and/or by having such other contacts with Puerto Rico so as to render the exercise of jurisdiction over them by the Puerto Rico courts consistent with traditional notions of fair play and substantial justice.

III. PARTIES

5. Plaintiff LYMARIS M. RIVERA DIAZ is a resident of the Commonwealth of Puerto Rico. At all times relevant to this action, Plaintiff has owned an iPhone and had the following iPhone Applications installed on her iPhone: Pandora and the Weather Channel.

6. None of the Defendants adequately disclosed to Plaintiff either before or after downloading the Apps that they were transmitting personal data about her to third-party advertising networks as set forth below, and she would not have used these Apps to the extent she has, if at all, had the true facts been timely disclosed.

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

8. 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.

9. 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.

10. 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.

11. At all times mentioned in the Causes of Action alleged herein, each and every Defendant was an agent, representative, affiliate, or joint venture 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.

12. 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.

13. 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.

14. 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.

15. 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.

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

IV. STATEMENT OF FACTS

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

18. The basis for Plaintiff(s)' claims rest on Defendants' collective use of an intrusive tracking scheme implemented through the use of mobile device Apps on Plaintiff(s)' iPhones and iPads.

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

20. 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.

21. 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.

22. The iPhone allows users to install after-market programs, called Apps, onto their mobile device. This allows users, such as Plaintiff(s), to customize their iPhones to perform functions other than those that the phones could perform when they were initially sold to the consumers.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. Because Apps are software that users, such as Plaintiff(s), 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. Plaintiff(s) in this action consider the information on their phone to be personal and private information.

31. 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.

32. 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.

33. A piece of software known as "browser cookies" is 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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."

41. 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.

42. Each of the non-Apple Defendants, through the use Apps placed on Plaintiff(s)' mobile devices, either accessed Plaintiff(s)' 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.

43. 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.)

44. 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.

45. None of the Defendants adequately informed Plaintiff(s) or Class members of their practices or obtained Plaintiff(s)' consent to do so.

46. 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.

47. 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.

48. There are no location based services involved in these Apps that would justify access to Plaintiff(s)' location data. When this information is combined with Plaintiff(s)' UDID

information, it becomes PII. None of these Defendants adequately disclosed to Plaintiff(s) or Class members that they are transmitting such information to third-party advertising networks.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. Plaintiff(s) 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. Plaintiff(s) 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.

55. Plaintiff(s)' 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. Plaintiff(s) also consider this information to be personal and private data. Such

information was taken from them without their knowledge or consent. Plaintiff(s) should be compensated for this harm and are entitled to compensation for this invasion of their privacy.

56. Each of the non-Apple Defendants is liable to Plaintiff(s) 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 Plaintiff(s) 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.

57. Plaintiff(s) 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.

58. Plaintiff(s) 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.

A. Defendant Apple Aided and Abetted the Other Defendants

59. Defendant Apple knew or should have known the other Defendants' conduct constituted a breach of those Defendants' duties to Plaintiff(s) and the Class.

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

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

B. **Defendant Apple is in a Joint Venture with the Other Defendants**

62. 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.

63. 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.

64. 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.

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

V. CLASS ACTION ALLEGATIONS

66. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3) Plaintiff(s) 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 the filing of this lawsuit (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 Plaintiff(s) to represent the named Plaintiff(s) 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.

67. 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.

68. 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 Plaintiff(s)' UDID, location and/or Username/password information to third parties; and

e. whether Plaintiff(s)' PII data were used to track their activity.

69. Plaintiff(s) 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, Plaintiff(s) will necessarily establish the liability of the Defendants to all Class members;

b. Without the representation provided by Plaintiff(s), it is unlikely that any Class members would receive legal representation to obtain the remedies specified by relevant statutes and the common law;

c. Plaintiff(s) have retained competent attorneys who are experienced in the conduct of class actions. Plaintiff(s) and their counsel have the necessary resources to adequately and vigorously litigate this class action, and Plaintiff(s) 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.

70. 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.

VI. CAUSES OF ACTION

COUNT I

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

(By Plaintiff(s) Against All Defendants)

71. Plaintiff(s) incorporate by reference each proceeding and succeeding paragraph as through set forth fully at length herein.

72. By accessing and transmitting Plaintiff(s)' UDID and location data on the devices of Plaintiff(s) and members of the Class, Defendants have accessed Plaintiff(s)' devices, in the

course of interstate commerce and/or communication, in excess of the authorization provided by Plaintiff(s) as described in 18 U.S.C. §1030(a)(2)(C).

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

74. Plaintiff(s)' 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.

75. 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.

76. Defendants' actions were knowing and/or reckless and, as outlined above, caused harm to Plaintiff(s) and members of the proposed class.

77. Plaintiff(s) seek recovery for this loss, as well as injunctive relief, to prevent future harm.

COUNT II

TRESPASS TO PERSONAL PROPERTY

(By Plaintiff(s) Against All Defendants)

78. Plaintiff(s) incorporate by reference each proceeding and succeeding paragraph as though set forth fully at length herein.

79. By obtaining UDID and location data from Plaintiff(s)' and members of the Class' devices without or beyond the scope of their consent or knowledge, Defendants have

improperly exercised dominion and control over Plaintiff(s)' and members of the Class's personal property.

80. Defendants' actions were done knowingly and intentionally.

81. Defendants' actions caused harm to Plaintiff(s) and members of the Class, as described above.

82. Plaintiff(s) and the proposed class seek damages for this harm as well as injunctive relief to remedy this harm.

COUNT III

COMMON LAW CONVERSION

(By Plaintiff(s) Against All Defendants)

83. Plaintiff(s) incorporate the above allegations by reference as if set forth herein at length.

84. Defendants have taken Plaintiff(s)' property in the form of PII data about them that is private and personal.

85. Plaintiff(s) have been harmed by this exercise of dominion and control over their information.

86. Plaintiff(s) bring this case seeking recovery for their damages and appropriate injunctive relief.

COUNT IV

COMMON COUNTS, ASSUMPSIT, AND UNJUST ENRICHMENT/RESTITUTION

(By Plaintiff(s) Against All Defendants)

87. Plaintiff(s) incorporate the above allegations by reference as if set forth herein at length.

88. Defendants entered into a series of implied at law contracts with Plaintiff(s) and the Class that resulted in money being had and received by Defendants at the expense of Plaintiff(s) 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. Plaintiff(s)' detriment and Defendants' enrichment were related to and flowed from the conduct challenged in this Complaint.

89. 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 Plaintiff(s) and Class members and converting it into revenues and profits.

90. 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.

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

92. Plaintiff(s) and members of the Class seek restitutionary disgorgement of all profits of such amounts and the establishment of a constructive trust from which Plaintiff(s) 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 Plaintiff(s) and the Class. Plaintiff(s) also seek declaratory relief as to the rights and responsibilities of all parties to such implied at law agreements.

COUNT V

PUERTO RICO COMPUTER CRIME LAW
PUERTO RICO PENAL CODE §§ 183, 184, 185, 186 AND 187 AND LAW 311 DATED OCTOBER 5, 1999

(By Plaintiffs Against All Defendants)

93. Plaintiff(s) incorporate the above allegations by reference as if set forth herein at length.

94. The Puerto Rico Computer Crime Laws, regulate "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."

95. Defendants violated Puerto Rico Computer Crime Law by Knowingly accessing, copying, using, made use of, interfering, and/or altering, data belonging to Plaintiffs and Class members: (1) in and from the Commonwealth of Puerto Rico; (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.

96. Pursuant to Puerto Rico Computer Crime Law – 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.

97. Pursuant to Puerto Rico Computer Crime Law, 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.

98. Defendants have violated Puerto Rico Computer Crime Law 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 member into surrendering private electronic communications and activities for Defendants' financial gain, and to wrongfully obtain valuable private data from Plaintiffs.

99. Defendants have violated Puerto Rico Computer Crime Law by knowingly accessing and without permission, taking, or making use of data from Plaintiffs' computers.

100. Defendants have violated Puerto Rico Computer Crime Law by knowingly and without permission, using and causing to be used Plaintiffs' computer services.

101. Defendants have violated Puerto Rico Computer Crime Law by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs computer, computer system, and/or computer network.

102. Defendants have violated Puerto Rico Computer Crime Law by knowingly and without permission accessing, or causing to be accessed, Plaintiffs computer, computer system, and/or computer network.

103. Puerto Rico Computer Crime Law 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.

104. 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.

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

106. As a direct and proximate result of Defendants' unlawful conduct within the meaning of P.R. Computer Crime Law 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 P.R. Civil Code.

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

COUNT VI

UNFAIR TRADE PRACTICES ACT
32 LAWS OF PUERTO RICO SEC. 3341

(By Plaintiffs Against All Defendants)

108. Plaintiff(s) incorporate the above allegations by reference as if set forth herein at length.

109. In violation of Puerto Rico Unfair Trade Practices Act, 32 L.P.R.A. sec.3341 (the "PRUTPA"), Defendants' conduct in this regard is ongoing and includes, but is not limited to, unfair, unlawful and fraudulent conduct.

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

111. Defendants' business acts and practices are unlawful, in part, because they violate PRUTPA, 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.

112. 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 Puerto Rico tethered to the state constitutional right of privacy, and Puerto Rico statutes recognizing the need for consumers to obtain material information that enables them to safeguard their own privacy interests, including Puerto Rico Civil Code, Article 1802.

113. 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 PRUTPA.

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

WHEREFORE, Plaintiff(s) 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:

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

B. Granting judgment in favor of Plaintiff(s) and the other members of the Class against Defendants;

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

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

H. An award to Plaintiff(s) 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' PII data 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

Plaintiff(s) demand a trial by jury of all issues and cause of action so triable.

RESPECTFULLY SUBMITTED, in San Juan, Puerto Rico, this 10 th day of May, 2011.

/s/ Eric Quetglas Jordan

ERIC QUETGLAS-JORDAN
USDC-PR No. 202514
Email: Quetglaslaw@gmail.com;
Eric@Quetglaslaw.com

JOSE QUETGLAS JORDAN
USDC-PR No. 203411
Email: JFQuetglas@gmail.com

QUETGLAS LAW OFFICES
PO Box 16606
San Juan PR 00908-6606
Tel: (787) 722-0635/(787) 722-7745
Fax: (787) 725-3970

REQUESTS FOR SERVICE BY CERTIFIED MAIL

Pursuant to MRCP 4.1 and 4.2, Plaintiff(s) request service of the foregoing Complaint by certified mail.

By: /s/ Eric Quetglas Jordan

ERIC QUETGLAS-JORDAN
Attorney for Plaintiff(s)

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

The Weather Channel, Inc.
300 Interstate North Parkway SE
Atlanta, Georgia 30339-2403