CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

NO: 500-06-000551-107

(Class Action)
SUPERIOR COURT

G. ALBILIA

Petitioner

-vs.-

APPLE, INC.

and

APPLE CANADA INC.

and

GOOGLE, INC., legal person duly incorporated, having its head office at 1600 Amphitheatre Parkway, City of Mountain View, State of California, 94043, USA

and

ADMOB, INC., legal person duly incorporated, having its head office at 1600 Amphitheatre Parkway, City of Mountain View, State of California, 94043, USA

and

ADMARVEL, INC., legal person duly incorporated, having its head office at 1875 South Grant St., Suite 750, City of San Mateo, State of California, 94402, USA

and

FLURRY, INC., legal person duly incorporated, having its head office at 282 2nd Street, Suite 202, City of San

Francisco, State of California, 94105, USA

and

MEDIALETS, INC., legal person duly incorporated, having its head office at 450 W. 15th Street, Suite 200, City of New York, State of New York, 10011, USA

(...)

Respondents

MOTION TO AUTHORIZE THE BRINGING OF A CLASS ACTION
&
TO ASCRIBE THE STATUS OF REPRESENTATIVE
(Art. 1002 C.C.P. and following)

TO ONE OF THE HONOURABLE JUSTICES OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, YOUR PETITIONER STATES AS FOLLOWS:

I. GENERAL PRESENTATION

A) THE ACTION

1. Petitioner wishes to institute a class action on behalf of the following group, of which he is a member, namely:

    - all residents in Canada who have downloaded and/or placed an App onto their iPhone or iPad ("iDevices") since approximately December 1st 2008 through to the present, or any other group to be determined by the Court;

    Alternately (or as a subclass)

    - all residents in Quebec who have downloaded and/or placed an App onto their iPhone or iPad ("iDevices") since approximately December 1st 2008 through to the present, or any other group to be determined by the Court;

2. The present action involves Class Member's personal data being collected from their iDevices while using Apple-approved Apps. Such data was identifiable as to each of the Class Members and was transmitted to third parties for purposes wholly unrelated to the use and functionality of their iDevices or the Apps contained thereon;

3. None of the Class Members were made aware of or consented to the taking of this data, and there was no way to opt out of this surreptitious, third-party collection of information. The information collected included but was not limited to: a Class Members' precise home and workplace locations and current whereabouts; unique device identifier (UDID) assigned to Class Members' iDevice; personal name assigned to the device; Class Member's s gender, age, postal code code, and time zone; as well as App-specific activity such as which functions Class Members performed on the App; search terms entered; and selections of movies, songs, restaurants, etc...;

3.1 As a result, each of the Class Members had the resources of their iDevice consumed and diminished without their permission. Such resources were measurable and of actual value, and included iDevice storage, battery life, and bandwidth from each Class Members' wireless services provider. The monetary value of the resources taken from Class Members is quantified herein;

3.2 In addition to Class Members' privacy right being violated, and among other injuries and damages detailed herein, had Class Members known of the above-summarized characteristics of the iDevices during the class period, they would not have purchased iDevices or, certainly, would not have paid what they did for devices that were substantially devalued by the undesirable characteristics inextricably linked to the devices and their operating environment;

B) THE RESPONDENTS

4 Respondent Apple, Inc. ("Apple USA") is an American company. Apple USA developed, manufactured, distributed, and sold the iPhone, as well as, the iPad throughout Canada, including the province of Quebec, either directly or indirectly through its affiliate and/or subsidiary Respondent Apple Canada Inc. ("Apple Canada"), the whole as appears more fully from a copy of the *Registre des enterprises* CIDREQ report, produced herein as **Exhibit R-1**. Given their close ties, both Respondents are being collectively referred to herein as "Apple";

4.1 In addition, Apple is also the developer of iOS, the operating system that runs the iDevices. Apple developed and operates the Apple App Store. Apple reviews and approves each and every App that it offers in the App Store;

5 (...);
6 (...);
7 (...);
8 (...);
9 (...);
10 (...);
11 (...);
12 (...);

Tracking Respondents

13 The Respondents named below, collectively referred to herein as the "Tracking Defendants," collect personal information transmitted from Class Members' iDevices for purposes unrelated to their functionality or the execution of Apps on those devices;

13.1 Respondent Google, Inc. ("Google) is an American company company. Google operates ad networks DoubleClick and AdChoices, and provides analytics services through Google Analytics;

13.2 Respondent AdMob, Inc. ("AdMob") is an American company. AdMob, which was acquired by Google in 2009, purports to be the world's largest mobile advertising marketplace offering both advertisers and publishers the ability to target and personalize advertising to their customers in 150 countries. Admob offers sophisticated targeting options which include demographics, interests and behavioral, device and carrier, keyword and remarketing. In particular, AdMob accesses the GPS location, application package name, and application version information off of iDevices. Additionally for some Apps, it appears that AdMob transmits Class Members' birthday, gender, and postal code information;

13.3 Respondent AdMarvel, Inc. ("AdMarvel") is an American company. AdMarvel is a mobile advertising provider that partners with other advertising networks to provide mobile advertising content to mobile devices. AdMarvel schedules, serves and tracks ad units, and enables clients to track and monetize their mobile audience;

13.4 Respondent Flurry, Inc. ("Flurry") is an American company. Flurry is an advertising content and analytics provider for mobile device applications. Specifically, Flurry assists App developers by providing demographic, geographic, and user interest data;

13.5 Respondent Medialets, Inc. (“Medialets”) is an American company. Medialets is a provider of analytics services for mobile devices;

C) THE SITUATION

14 The basis for the present claim rest on the Respondents’ use of an intrusive tracking scheme implemented through the use of mobile device Apps on Class Members’ iPhones and iPads;

14.1 Accordingly, when certain Apps, including but not limited to: Dictionary.com, Paper Toss, Bible App, Urban Spoon, Flixster, The Weather Channel, Textplus 4, Pimple Popper Lite, Pumpkin Maker, and Talking Tom Cat were downloaded and used by Class Members, the personal information was accessed, collected and transmitted to third parties and to the Apps themselves such as includes: fine (GPS) location information, network (*e.g.*, 3G or WiFi), name of the device's operating system, operating system version, the amount of free storage space on iDevice, the carrier-assigned phone name (*e.g.*, "John's phone"), iDevice model (*e.g.*, iPhone 3GS), the phone's unique device identifier (UDID), the Class Members’ age, gender, app ID and password for specific App accounts, the search term entered by the Class Member, time zone, language, postal code, the name of the app, the title of a particular app page viewed by the Class Member, the particular app activity engaged in (e.g., search, view), Class Members’ particular media selection (e.g., song, video), the genre of media selected, and the performer in the Class Member's media selection;

14.2 Reportedly, Apple has limited the availability of some device data in its iOS version 5. Even if so, millions of iDevice purchasers continue to use the prior version;

14.3 Not only were Class Members’ personal information transmitted to the above-named third parties and to the Apps, themselves, but all of Class Members’ information listed above was transmitted “in the clear” (sometimes referred to as “plain text”), that is, without encryption;

15 Apps are computer programs that users can download and install on their mobile computer devices, including iPhones and iPads. Class Members downloaded these Apps from an Apple-sponsored website as part of the use of their mobile devices. Apple claims to review each application before offering it to its users, purports to have implemented app privacy standards, and claims to have created strong privacy protections for its customers. However, Class Members have discovered that some of these Apps have been transmitting their personal, identifying information to advertising networks without obtaining their consent;

16 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;

17 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. 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;

18 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;

19 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. It is estimated that worldwide App sales this year will total $6.7 billion;

20 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;

21 Due 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;

22 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;

23 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;

24 Considering that mobile advertising is such big business, 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;

25 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;

26 Respondents, 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 (*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;

27 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;

28 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;

29 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;

30 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;

31 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;

32 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";

33 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;

34 (...);

35 The general practice engaged in by Respondents 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)", the whole as appears more fully from a copy of said report, produced herein as **Exhibit R-2**;

36 Further, the *Wall Street Journal*, as reported in the article "Your Apps Are Watching You" by Scott Thurm and Yukari Iwatani Kane (December 18, 2010), independently confirmed that many Apps systematically (...) obtain iPhone users' UDID and location data and transmit it to multiple third parties, the whole as appears more fully from a copy of said article, produced herein as **Exhibit R-3**;

37 None of the Respondents adequately informed Class Members of their practices, and none of the Respondents obtained Class Members' consent to do so;

38 Class Members' valuable UDID information, demographic information, location information, as well as their application usage habits is personal and private. Such information was taken from them without their knowledge or consent. Class Members should be compensated for this harm. Class Members are entitled to compensation for this invasion of their privacy;

39 (...);

40 In addition, Apple has also aided and abetted the remaining Respondents in the commission of their legal wrongs against Class Members. Apple knew or should have known the other Respondents' conduct constituted a breach of those Respondents' duties to Class Members, but did not take any meaningful steps to prevent such harm;

The Sale and Use of iDevices

40.1 Apple manufactures, licenses, distributes, and promotes iDevices. However, as explained below, Apple misrepresented the true cost of the iDevices and/or omitted material information from its representations;

40.2 Class Members relied upon Apple's representations with respect to the cost of their iDevices, the availability of "free" Apps, and the ability to opt-out of geolocation tracking, in making their purchasing decisions, and the omission of material facts to the contrary was important to them;

40.3 Apple has represented to Class Members, expressly or by implication, that the App Store does not permit apps that "violate [ ] our developer guidelines" including apps containing pornography, apps that violate a users privacy, and apps that hog bandwidth;

40.4 Apple has represented to Class Members, expressly or by implication, that: "Apple takes precautions — including administrative, technical, and physical measures — to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.";

40.5 Class Members were not informed as to the true cost of their iDevices due the lack of disclosures about third party tracking, tracking by Apple when Location Services were set to "Off" and the data transmittal and storage costs that would be imposed, and the iDevice resources that the Respondents would secretly consume;

40.6 Apple induced the purchase of iDevices by Class Members by offering thousands of ostensibly "free" Apps in its App Store. H owever, Apple failed to disclose to Class Members that those "free" apps included third-party spyware that utilized Apple-provided tools to collect Class Members' information, without detection, and send it to third parties, like the Tracking Respondents;

40.7 Class Members would not have purchased their iDevices and/or would not have paid as much for them, if Apple had disclosed the true facts that it and the Tracking Respondents would surreptitiously obtain personal information from their iDevices, track their activity and geolocation [with respect to Apple this occurred even when Location Services were set to "Off"], and consume portions of the "cache" and/or gigabytes of memory on their devices—memory that Class Members paid for the exclusive use of when they purchased their iDevice;

40.8 Because Apple did not disclose the true costs of their iDevices, Class Members were misled into purchasing a product that did not meet their reasonable expectations. Given the undisclosed costs imposed by using the iDevice, it was not as valuable to Class Members as the price they paid for it;

40.9 Apple's competitors manufacture, market, and distribute comparable mobile devices that do not collect personal information and track Class Members without permission, or fail to adequately disclose those material facts. Class Members paid a premium for their iDevice, in part because of Apple's material misrepresentations and omissions about the availability of a large number of "free" Apps that were not actually free as Class Members reasonably believed;

40.10 The Apple App Store was a market differentiator that not only set Apple iPhones apart from its handset competitors, it set the newly released iPhone 3G, with its 2.0 iOS operating system, apart from the prior generations of iPhones. In the post 3G 2.0 iOS era, the success of Apple's iPhones sales is inextricably linked to consumers' access to its App Store;

40.11 Class Members suffered actual damages as a result of Apple's acts and omissions. Specifically, as a proximate result of Apple's conduct, Class Members suffered monetary losses, i.e., the purchase price of the iDevice, or at a minimum, the difference of the inflated price and the price Apple should have charged for a product that fully disclosed all the costs hidden by Apple;

40.12 Every App in the App Store, whether free or paid, must be approved by Apple and digitally signed by Apple. Both Apple and third-party developers create numerous Apps available from the App Store. There are several hundred thousand Apps available at the App Store;

40.13 Apple has complete discretion as to whether it will allow an App to be sold in the App Store. Apple requires that proposed Apps go through a rigorous approval process. Even if an App meets the "Program" requirements (as Apple describes it), Apple may still reject the App for any reason at all;

40.14 iDevice users are only allowed to download software specifically licensed by Apple and available on the iDevice out of the box or through the App Store. If a user installs any software not approved by Apple, the users' warranty is voided. When a user installs Apple's updates to the iDevice operating system, Apple takes the opportunity to erase any non-licensed software on the device. Apple claims this control is necessary to ensure the "tightly integrated," smooth functioning of the iDevice;

40.15 Even after a user downloads an approved app, Apple maintains control by requiring that the end-user license agreement for every App include a clause giving Apple the ability to step into the shoes of the App developer and sue the end-user;

Apple Controls the Development Process for Apps Available for iDevices

40.16 In addition to controlling the characteristics and distribution of Apps, described above, Apple exercises substantial control over their development and functionality;

40.17 A third party who wants to sell an App from the Apple App Store is required to pay to enroll in the iPhone Developer Program. The third party must also agree to the terms of Apple's iPhone Developer Program License Agreement ("iOS Developer Agreement"). The iOS Developer Agreement is, by its terms, confidential, and prohibits the third party from making any public statements about the agreement, its terms and conditions, or the third party's relationship with Apple without Apple's prior written approval;

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

Apple Uses Class Members' Personal Information to Lure Low Cost Apps to its App Store

40.19 Apple's relationship with its App developers is also clearly symbiotic—Apple needs to have a healthy stable of low cost or free Apps available in its App Store to satisfy customer demands for the ability to customize their iDevices;

40.20 Apple takes steps to satisfy App developers' monetary requirements in order to encourage App developers to continue to provide a steady stream of low cost or free Apps for distribution in the App Store. The primary way Apple has done so is by ensuring that App developers have maintained access to a steady supply of valuable information about Class Members;

40.21 The App developers then use that information about Class Members to obtain advertising revenue from the Tracking Respondents;

40.22 One of the most valuable pieces of information that the Tracking Defendants obtain is access to Class Members' Apple-assigned UDID information. Apple knows the Tracking Respondents obtain and use the UDID from Class Members' iDevices, and Apple has failed to end that practice or meaningfully enforce any policy against it;

40.23 Apple understands the significance of identifiers such as its UDID in regards to users' privacy. Indeed, internally, Apple claims that it treats UDID information as "personally identifiable information" because, if combined with other information, such as other information easily available on the iDevice, it can be used to personally identify a user. This is due to the globally unique nature of a UDID—no other device bears the same identifying number;

40.24 That is exactly what happened here – Class Members' UDID information, along with other data like geographic location data, was collected by each Tracking Respondent, such that each Tracking Respondent was able to personally identify each Class Member. Once this was accomplished, every other piece of information collected by the Tracking Respondents was tied to Class Members' respective identities and used to further build a more complete profile of them;

40.25 Because Class Members' UDID is unique to each iDevice, and because each Class Member is the only, or at least the primary, user of their iDevice, the UDID proved to be an invaluable feature for the Tracking Respondents who were looking for a means of reliably identifying and tracking Class Members' online activities;

40.26 It was completely foreseeable to Apple that this would occur and, in fact, was to Apple's direct benefit. Apple knowingly and intentionally allowed the Tracking Respondents to access Class Members' iDevices' UDID and chose to not provide Class Members with any means to disable the iDevice's UDID from being tracked or to restrict access to the UDID;

40.27 Apple's desire to encourage and incentivize App developers is also evidenced by Apple allowing the Tracking Respondents to have access to numerous other pieces of information that Class Members would consider personal. For example: Apple allows App developers to build Apps that—by

design by Apple—will easily access the following personally identifiable information on a consumer's iDevice:

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

b) the numerous items of information collected from Class Members and their iDevices as outlined in paragraph 14.1 above;

40.28 Apple allowed third parties access to that information even as it specifically represented to Class Members that it did not allow Apps that violate their privacy;

40.29 Apple appeared to recognize the conflicted nature of its approach, as, in April of 2010, Apple amended its Developer Agreement, purportedly 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 provided 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.";

40.30 Apple faced a mountain of criticism over this change, so in September 2010, it amended its Developer Agreement again to allow for a significant exception—to allow transmission of data for advertising purposes (but not for data compilation and analytics purposes);

40.31 These changes were not engendered by a concern over consumers' data, however, but only by a concern for protection of Apple's own device data. Neither of Apple's amendments to its Developer Agreements directly addressed use of UDID data;

40.32 After the filing of the USA lawsuit and the present action, however, Apple quietly changed its policy regarding third-party access to UDID information. With the introduction of its iOS 5 operating system, Apple appears to have taken steps to finally stop Apps from sharing UDID information, but not before Class Members were significantly harmed;

40.33 Another example of Apple allowing Apps access to iDevice users' information involves Apple collecting users' location information in an easily accessible database file on the users' iDevice, and any other Apple device used to synchronize or back-up the iDevice;

40.34 In June 2010, with the release of its iOS 4 operating system, Apple began intentionally collecting Class Members' precise geographic location (consisting of accurate longitude and latitude coordinates) and storing that information in a file on the iDevice called "consolidated.db." These files accumulated a log of the longitude and latitude for every place Class Members traveled, along with a timestamp. The geographic location information was pulled either from Wi-fi towers or cell phone towers in Class Members' vicinity, and in some cases from the GPS data on Class Members' own iDevices;

40.35 In essence, this file constitutes a timeline and map of Class Members' every move. This data was also transmitted to Apple, and unknowingly uploaded by Class Members every time they synchronized ("synced") their iDevice to their home computer or another Apple device. The file data was, unbeknownst to Class Members, also available through Apps to third party marketers;

40.36 The data files at issue constitute a significant amount of solid-state memory space on Class Members' iDevices. Although the file size varies among Class Members, the range of sizes for such files for each class member is between 10 and 40 megabytes (which is enough space to store dozens of songs or photographs);

40.37 Based on the premium that Apple charges for its iDevices with extra solid-state memory space (*i.e.,* 32 gigabyte models rather than 16 gigabyte models) the memory space on iDevices has a reasonable market value of $100 per 16 gigabytes. Based on this number, the amount of solid-state memory space consumed by Apple for the undisclosed geolocation file is equal to approximately twenty-three cents ($0.23), for each Class Members' iPhone;

40.38 The storage space on Class Members' iDevices is storage space they paid for, and the twenty-three cents worth of storage that Apple consumes on Class Members' iDevices for Apple's own purposes constitutes a taking of an asset of economic value, paid for by Class Members and to which they have a superior right of possession. Apple's use of this space renders it unavailable for use by the owners of the iDevices;

40.39 The storage space on Class Members' iDevices is storage space they paid for, and the twenty-three cents worth of storage that Apple consumes on Class members' iDevices for Apple's own purposes constitutes a taking of an asset of economic value, paid for Class Members and to which they have a superior right of possession. Apple's use of this space renders it unavailable for use by the owners of the iDevices;

40.40 Apple does not adequately disclose that the geolocation tracking consumes the iDevice resources, and even more so, when Class Members Location Services were set to “Off”. Class Members paid Apple for these solid-state memory e resources, yet Apple essentially took it back from Class Members without their permission, consent or knowledge;

Apple Failed To Protect User Privacy and the Security of User Data as Promised

40.41 Apple’s control of the user experience includes restrictions, such as blocking consumers from modifying devices or installing non-App-store Apps, and blocking developers and researchers from publicly discussing Apple’s standards for App development, and even prohibiting researchers from analyzing and publicly discussing device shortcomings such as privacy flaws;

40.42 As a direct consequence of the control exercised by Apple, Class Members could not and cannot reasonably review the privacy effects of Apps and must rely on Apple to fulfill its duty to do so;

40.43 Apple undertook a duty to Class Members to protect their privacy, representing that it reviews all Apps available in its App Store for suitability, and that it retains broad discretion to remove an App from the App Store;

40.44 A third party cannot upload an App for sale in the App Store until Apple digitally signs the App, thereby signifying Apple’s review and approval of the App for sale in the App store;

40.45 Apple represents that:

a) an App may not access information from or about the user stored on the user’s iDevice unless the information is necessary for the advertised functioning of the App;

b) it does not allow one App to access data stored by another App;

c) it does not allow an App to transmit data from a user’s iDevice to other parties without the user’s consent;

40.46 Despite its representations and the duties to Class Members Apple undertook to protect their personal information from being accessed and exploited by third parties like the Tracking Respondents, Apple knowingly permits Apps that subject consumers to privacy exploits and security vulnerabilities to be offered in the App Store;

40.47 Contrary to Apple’s representations to Class Members, Apple does not screen App Store candidates to determine their use of proper standards in

transmitting personal information or analyze the traffic generated by Apps to detect Apps that violate the privacy terms of the iOS Developer Agreement and Apple's commitments to users;

40.48 Apple has a duty of reasonable care that arises independent of its promises and its undertaken duties. Apple shares the duty everyone shares to use ordinary care to prevent others from being injured as the result of its conduct. This duty arises independently of any contractual provision;

40.49 Apple also has a duty of reasonable care to act in a reasonable manner in designing its product so as to prevent Class Members from being harmed; to warn Class Members of any harm of which it is aware might foreseeably occur; or take reasonable steps to prevent others from causing Class Members harm when that harm is reasonably foreseeable by Apple;

40.50 Apple also has a duty as the proprietor of its App Store, which is the functional equivalent any other traditional business establishment, to protect its patrons from, or at least warn of, harm from third parties that Apple reasonably foresees—particularly where the harm is not evident to Class Members;

40.51 Apple breached each of these duties to Class Members as outlined in the preceding sections. Apple's breach of its duties caused foreseeable harm to Class Members and was a proximate cause thereof;

40.52 Apple breached its duty by designing iDevices so that the Tracking Respondents could acquire personal information without Class Members' knowledge or permission, by failing to review and remove privacy-violating apps from the App Store, and by constructing and controlling consumers' user experience and mobile environment so that consumers could not reasonably avoid such privacy-affecting actions;

Apple Misled Class Members about Opting-Out of Its Tracking Program

40.53 Apple's Terms and Conditions ("TAC") expressly stated that customers could opt-out of Apple's tracking program and prevent geolocation information from being collected and sent from their iPhones:

> "Location Data: Apple ... may provide certain services through your iPhone that rely upon location information. To provide these services, where available, Apple ... may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone ... By using any location-based services on your iPhone, you agree and consent to Apple's ... transmission, collection, maintenance, processing and use of your location data to provide such products and services. *You*

may withdraw consent at any time by ... turning off the Location Services setting on your iPhone[.]"

40.54 Unfortunately, despite the fact that many iPhone users affirmatively withdrew their consent to be tracked by turning off their iPhones' Location Services, Apple still continued to collect and transmit geolocation information;

40.55 On April 27th 2011, Apple admitted that its iPhones were collecting and transmitting its users' geolocation information to its servers, even when users affirmatively opted out by turning their Location Service settings "Off". Rather than owning up to its misconduct and taking responsibility for it as it advertised, Apple chalked up its misconduct to "a bug, which [it] plan[s] to fix shortly.", the whole as appears more fully from a copy of said Press Release, produced herein as **Exhibit R-5**. This admission plainly contradicts Apple's representations to its customers regarding the ability to opt-out of its geolocation tracking program;

40.56 Apple's failure to fulfill its commitments included Apple's practice of capturing frequent and detailed information about iDevice users' locations for up to one year, including the locations of iDevice users who had utilized Apple's prescribed method for disabling Global Positioning System services, and

a) maintaining records of such location histories on users' iDevices,

b) transferring such location history files to users' replacement iDevices, and to other computers with which users synchronized their iDevices,

c) storing such location history files in accessible, unencrypted form,

d) without providing notice to users or obtaining users' consent,

e) where consumers had no reasonable means to become aware of such practice or to manage it, and

f) where such practice placed users at unreasonable risk of capture and misuse of such highly detailed and personal information;

The Tracking Defendants Exploit Access to Consumer Data

40.57 Notwithstanding Apple's control of the user experience, it designs its mobile devices to be very open when it comes to disclosing information about consumers to the Tracking Respondents, companies that incentivize App developers to provide the App Store with free Apps for iDevices and provide Apple the metrics to support its claims of market leadership;

40.58 The personal and private information is of extreme interest to many advertising networks and web analytics companies, including the Tracking Respondents. For this reason, the Tracking Respondents pay to support App development, so that many Apps are provided to consumers ostensibly "free" or at a lower cost;

40.59 When users download and install the Apps on their iDevices, the Tracking Respondents' software accesses personal information on those devices without users' awareness or permission and transmits the information to the Tracking Respondents, supplying them with details such as consumers' cellphone numbers, address books, UDIDs, and geolocation histories—highly personal details about who the consumers are, who they know, what they do, and where they are;

40.60 Some Tracking Respondents pay App developers to include code that causes ads to be displayed when users run the apps. Those ads are then populated with content from the Tracking Respondents and provide the communications channel for the Tracking Respondents to acquire and upload users' personal information;

40.61 In the wake of Apple's prohibition against sending user information to third parties, described above, protests erupted from a number of third-party advertising networks and metrics/analytics companies (who have been receiving a steady flow of user data from iDevice Apps). One prominent critic was the CEO of Google-owned AdMob. Following this criticism, Apple has taken no steps to actually implement its changed Developer Agreement or enforce it in any meaningful way;

40.62 As a result, the Tracking Respondents, through the Apps with whom they had entered into relationships and to whom they had provided code, have continued to acquire details about consumers and to track consumers on an ongoing basis, across numerous applications, and tracking consumers when they accessed Apps from different mobile devices;

40.63 With the personal information acquired, the Tracking Respondents used the information to compile—in addition to the types of information described in paragraph 14.1 above —personal, private, and sensitive information that included consumers' video application viewing choices, web browsing activities, and their personal characteristics such as gender, age, race, family status, education level, geographic location, and household income, even though the Tracking Respondents require none of this information to provide the user services for which the Apps were marketed;

40.64 The Tracking Respondents acquired personal information and compiled profiles that were unnecessary to the Apps' stated functions but were useful

to the Tracking Respodents in their commercial compilation, use, and sale of consumers' personal information;

40.65 Because of Apple's and the Tracking Respondents' control and coding, Class Members are unable to detect, manage, or avoid this collection and transmittal of information;

40.66 Apple is aware that Apps are providing a conduit for the Tracking Respondents to acquire consumers' personal information without consumers' knowledge or consent;

40.67 However, because consumers are unaware of the Tracking Respondents, they cannot complain to Apple about particular Apps and request that Apple remove the apps from the App Store;

40.68 Apple has continued to allow App developers to run their apps on its iOS platform and failed to void the licensing agreements with App developers, even after it received notice of Tracking Respondents' practices;

No Consent

40.69 Class Members would consider the information from and about themselves on their iDevices to be personal and private information. Consumers using iDevices that download Apps from the App Store would reasonably consider information from and about themselves stored on their iDevices to be personal and private information that they would not expect to be collected and used by third parties without the consumers' express consent;

40.70 Class Members did not expect, receive notice of, or consent to the Tracking Respondents tracking their App use. Class Members did not expect, receive notice of, or consent to the Tracking Respondents' acquisition of their personally identifiable information;

40.71 The Tracking Respondents' activities were in conflict with Apple's representations about what information third parties were permitted to access;

40.72 The Tracking Respondents' actions exceeded the scope of any authorization that could have been granted by Class Members at the time of downloading and using Apps;

40.73 The Tracking Respondents sell users' personal information to, or purchase and merge user's personal information with, other personal information about the same users that is available in the commercial, secondary information market, which the traffickers take substantial efforts to shield from the public eye;

40.74 The Tracking Respondents and other parties to the information market use the merger of personal information to effectively or actually de-anonymize consumers;

40.75 The Tracking Respondents used Class Members' personal information for their own economic benefit;

40.76 Class Members did not consent to being personally identified to the Tracking Respondents or for their personally identifiable information to be shared with and used on behalf of the Tracking Respondents;

40.77 The Tracking Respondents actions were knowing, surreptitious, and without notice and so were conducted without authorization and exceeding authorization. The Tracking Respondents misappropriated Class Members' personal information;

Tracking Defendants' Harmful Use of Class Members' Resources

40.78 In addition to the harms alleged above, the Tracking Respondents' unauthorized, surreptitious collection of Class Members' information, as outlined in paragraph 14.1 above, subjected Class Members to harms because the Tracking Respondents actions consumed resources to which Class Members had the right of controls and use;

40.79 For example, some Tracking Respondents caused compressed .zip files of varying megabytes in size to be downloaded to each of Class Members' iDevices and for purposes unrelated to the App. In doing so, the Tracking Respondents unexpectedly utilized such Class Members' bandwidth resources for which Class Members paid charges to their carriers, and consuming storage space on their iDevices, which Class Members had purchased without expectation of such unauthorized resource use by Apps from the App Store;

40.80 In addition, as to all Tracking Respondents, their actions in collecting information from Class Members utilized power resources on Class Members' iDevices, without disclosure or authorization;

40.81 The rate at which battery charge was diminished on the iDevices as a result of the Tracking Respondents' actions was material to Class Members, particularly given the power resource constraints on the iDevice: the Tracking Respondents' repeated actions during App executions utilized approximately two to three seconds of battery capacity with each action due to the power requirements of CPU processing, file input and output actions, and Internet connectivity;

40.82 Not only did Tracking Respondents' actions cause Class Members' iDevice batteries to discharge more quickly, rendering the iDevices less useful given power constraints, but the Tracking Respondents repeated actions also resulted in lasting impairment because, by repeatedly utilizing power and causing Class Members to have to re-charge their iDevices batteries sooner, the Tracking Respondents shortened the actual utility and life of the iDevice batteries, for which charging capabilities are diminished over repeated re-chargings;

D) THE FOREIGN PROCEDURES

41 Several class action actions have been instituted in the United States based on the Respondents' conduct, which have all been consolidated as In Re iPhone Application Litigation in the Northern District Court of California, the whole as appears more fully from a copy of said Complaints and Amended Complaints, produced herein *en liasse* as **Exhibit R-4**;

II. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PETITIONER

42 Petitioner purchased an iPhone on or about the end of 2009 from Rogers;

43 Since that time, he has downloaded numerous Apps including, but not limited to: Pandora, Dictionary.com, Paper Toss, The Weather Channel, Textplus 4, Pimple Popper Lite, Pumpkin Maker, and Talking Tom Cat;

44 Petitioner has learned of the institution of two (2) class actions filed in the United States regarding the facts as alleged in the present proceedings;

45 Petitioner believes that as a consequence of his installation of the various Apps onto his iPhone and considering the allegations as set forth in the American actions, that his privacy rights have been violated by the Respondents' actions;

46 Petitioner's damages are a direct and proximate result of the Respondents' conduct;

47 In consequence of the foregoing, Petitioner is justified in claiming damages;

III. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE MEMBERS OF THE GROUP

48 Every member of the class has downloaded Apps onto either their iPhone or iPad;

49 Each member of the class has had their privacy rights violated due to the Respondents' unlawful actions;

50 All of the damages to the class members are a direct and proximate result of the Respondents' conduct;

51 In consequence of the foregoing, members of the class are justified in claiming damages;

IV. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

A) The composition of the class renders the application of articles 59 or 67 C.C.P. difficult or impractical

52 The sale of iPhones and iPads, as well as the downloading of Apps for said devices, are widespread in Quebec and Canada;

53 Petitioner is unaware of the specific number of persons who downloaded these Apps, however, given their tremendous popularity, it is safe to estimate that it is in the tens of thousands (if not hundreds of thousands);

54 Class members are numerous and are scattered across the entire province and country;

55 In addition, given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the Respondents. Even if the class members themselves could afford such individual litigation, the court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues raised by the conduct of Respondents would increase delay and expense to all parties and to the court system;

56 Also, a multitude of actions instituted in different jurisdictions, both territorial (different provinces) and judicial districts (same province), risks having contradictory judgements on questions of fact and law that are similar or related to all members of the class;

57 These facts demonstrate that it would be impractical, if not impossible, to contact each and every member of the class to obtain mandates and to join them in one action;

58 In these circumstances, a class action is the only appropriate procedure for all of the members of the class to effectively pursue their respective rights and have access to justice;

B) The questions of fact and law which are identical, similar, or related with respect to each of the class members with regard to the Respondents and that which the Petitioner wishes to have adjudicated upon by this class action

59 Individual questions, if any, pale by comparison to the numerous common questions that predominate;

60 The damages sustained by the class members flow, in each instance, from a common nucleus of operative facts, namely, Respondents' misconduct;

61 The recourses of the members raise identical, similar or related questions of fact or law, namely:

a) Did the Respondents create, cause, or facilitate the creation of personally identifiable profiles of Class Members?

b) Did the Respondents obtain, retain and/or sell Class Members' personally identifiable information without their knowledge and consent, or beyond the scope of their consent?

c) Did the Respondents fail to disclose material terms regarding the collection and dissemination of the Class Members' personally identifiable information?

d) Did the Respondents use iPhone Apps or iPad Apps to capture Class Members' UDID, location, username/password, or other such information (...)?

e) What use was made of the Class Members' personally identifiable information (...)?

f) Did the Respondents violate the privacy of Class Members?

g) Were Class Members prejudiced by the Respondents' conduct, and, if so, what is the appropriate measure of these damages?

h) Are Class Members entitled to, among other remedies, injunctive relief, and, if so, what is the nature and extent of such injunctive relief?

i) Are the Respondents liable to pay compensatory, moral, punitive and/or exemplary damages to Class Members, and, if so, in what amount?

j) Were the Respondents unjustly enriched?

62 The interests of justice favour that this motion be granted in accordance with its conclusions;

V. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

63 The action that the Petitioner wishes to institute on behalf of the members of the class is an action in damages and for injunctive relief;

64 The conclusions that the Petitioner wishes to introduce by way of a motion to institute proceedings are:

GRANT the class action of the Petitioner and each of the members of the class;

DECLARE the Defendants solidarily liable for the damages suffered by the Petitioner and each of the members of the class;

ORDER the Defendants to permanently cease from continuing to collect and disseminate Class Members' personally identifiable information;

CONDEMN the Defendants to pay to each member of the class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the motion to authorize a class action;

ORDER the Defendants to deposit in the office of this court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual class members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable court shall determine and that is in the interest of the members of the class;

A) The Petitioner requests that he be attributed the status of representative of the Class

65 Petitioner is a member of the class;

66 Petitioner is ready and available to manage and direct the present action in the interest of the members of the class that they wish to represent and is determined to lead the present dossier until a final resolution of the matter, the whole for the benefit of the class, as well as, to dedicate the time necessary for the present action before the Courts of Quebec and the *Fonds d'aide aux recours collectif*s, as the case may be, and to collaborate with his attorneys;

67 Petitioner has the capacity and interest to fairly and adequately protect and represent the interest of the members of the class;

68 Petitioner has given the mandate to his attorneys to obtain all relevant information with respect to the present action and intends to keep informed of all developments;

69 Petitioner, with the assistance of his attorneys, are ready and available to dedicate the time necessary for this action and to collaborate with other members of the class and to keep them informed;

70 Petitioner is in good faith and has instituted this action for the sole goal of having his rights, as well as the rights of other class members, recognized and protecting so that they may be compensated for the damages that they have suffered as a consequence of the Respondents' conduct;

71 Petitioner understands the nature of the action;

72 Petitioner's interests are not antagonistic to those of other members of the class;

B) The Petitioner suggests that this class action be exercised before the Superior Court of justice in the district of Montreal

73 A great number of the members of the class reside in the judicial district of Montreal and in the appeal district of Montreal;

74 The Petitioner's attorneys practice their profession in the judicial district of Montreal;

75 The present motion is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present motion;

AUTHORIZE the bringing of a class action in the form of a motion to institute proceedings in damages and for injunctive relief;

ASCRIBE the Petitioner the status of representative of the persons included in the class herein described as:

- all residents in Canada who have downloaded and/or placed an App onto their iPhone or iPad ("iDevices") since approximately December 1st 2008 through to the present, or any other group to be determined by the Court;

Alternately (or as a subclass)

- all residents in Quebec who have downloaded and/or placed an App onto their iPhone or iPad ("iDevices") since approximately December 1st 2008 through to the present, or any other group to be determined by the Court;

IDENTIFY the principle questions of fact and law to be treated collectively as the following:

a) Did the Respondents create, cause, or facilitate the creation of personally identifiable profiles of Class Members?

b) Did the Respondents obtain, retain and/or sell Class Members' personally identifiable information without their knowledge and consent, or beyond the scope of their consent?

c) Did the Respondents fail to disclose material terms regarding the collection and dissemination of the Class Members' personally identifiable information?

d) Did the Respondents use iPhone Apps or iPad Apps to capture Class Members' UDID, location, username/password, or other such information (...)?

e) What use was made of the Class Members' personally identifiable information (...)?

f) Did the Respondents violate the privacy of Class Members?

g) Were Class Members prejudiced by the Respondents' conduct, and, if so, what is the appropriate measure of these damages?

h) Are Class Members entitled to, among other remedies, injunctive relief, and, if so, what is the nature and extent of such injunctive relief?

i) Are the Respondents liable to pay compensatory, moral, punitive and/or exemplary damages to Class Members, and, if so, in what amount?

j) Were the Respondents unjustly enriched?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

GRANT the class action of the Petitioner and each of the members of the class;

DECLARE the Defendants solidarily liable for the damages suffered by the Petitioner and each of the members of the class;

ORDER the Defendants to permanently cease from continuing to collect and disseminate Class Members' personally identifiable information;

CONDEMN the Defendants to pay to each member of the class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the motion to authorize a class action;

ORDER the Defendants to deposit in the office of this court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual class members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable court shall determine and that is in the interest of the members of the class;

DECLARE that all members of the class that have not requested their exclusion, be bound by any judgement to be rendered on the class action to be instituted in the manner provided for by the law;

FIX the delay of exclusion at thirty (30) days from the date of the publication of the notice to the members, date upon which the members of the class that have not exercised their means of exclusion will be bound by any judgement to be rendered herein;

ORDER the publication of a notice to the members of the class in accordance with article 1006 C.C.P. within sixty (60) days from the judgement to be rendered herein in LA PRESSE and the NATIONAL POST;

ORDER that said notice be available on the various Respondents' websites with a link stating "Notice to iPhone and iPad App users";

RENDER any other order that this Honourable court shall determine and that is in the interest of the members of the class;

THE WHOLE with costs including publications fees.

Montreal, January 17, 2012

(s) Jeff Orenstein

_____

CONSUMER LAW GROUP INC.
Per: Me Jeff Orenstein
Attorneys for the Petitioner