CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

NO: 500-06-000551-107

(Class Action)
SUPERIOR COURT

N. BALMER
and
L. SÉNÉCAL
and
R. SFEIR

Plaintiffs / Class Representatives

-vs.-

APPLE, INC., legal person duly constituted, having its head office at 1 Infinite Loop, City of Cupertino, State of California, 95014, USA

and

APPLE CANADA INC., legal person duly constituted, having its head office at 555, Dr. Frédérik-Phillips, Suite 210, City of Saint-Laurent, Province of Quebec, H4M 2X4

Defendants

AMENDED PARTICULARIZED MOTION TO INSTITUTE PROCEEDINGS
(Art. 141 and following *C.C.P.*)

TO THE HONOURABLE MR. JUSTICE PIERRE NOLLET, JUDGE OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, YOUR PLAINTIFFS/ CLASS REPRESENTATIVES STATE AS FOLLOWS:

I. INTRODUCTION

1. On June 27, 2013, the Superior Court of Quebec authorized (certified) the Plaintiffs / Class Representatives to institute a class action against the Defendants on behalf of the group of:

> "all residents in Quebec who have purchased or otherwise acquired an iPhone or iPad ("iDevice") and who have downloaded free Apps from the App Store onto their iDevices since December 1, 2008 through to the present.
>
> and (the Geolocation Class)
>
> all residents in Quebec who have purchased or otherwise acquired an iPhone and turned Location Services off on their iPhones prior to April 27, 2011 and have unwittingly, and without notice or consent transmitted location data to Defendants' servers";[1]

2. The Defendants are the prominent and prestigious companies that developed, manufactured, licensed, distributed, promoted and/or sold the iPhone and the iPad (collectively the "iDevices"). In addition, they developed "iOS", the closed mobile operating system firmware[2] that runs the iDevices and the "Apple App Store" an Apple-controlled digital distribution platform that makes software available;

3. The present action involves Class Members' personal data being collected from their iDevices while using Apple-approved mobile software applications ("Apps") which were either downloaded from the Apple App Store or which had already been pre-installed on the iDevice upon purchase ("Built-In Apps"). Such data was clearly 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;

4. The Class Members were neither made aware of nor consented to the taking of this data and, there was no way to opt out of this surreptitious, third-party collection of private information. The information collected comprised of the following: a Class Members' precise home and workplace locations and current whereabouts and fine GPS location information, the unique device identifier ("UDID") assigned to Class Members' iDevice, Class Members' full names and contact information (including email address, phone number, physical address, social insurance number, financial information, and credit card information), the personal carrier-assigned user name to the device (e.g., "John's Phone") and password, the name of the iDevice's operating system, the iDevice model, Class Members' address book data, Class Members' detailed personal contact list stored in the Contacts App, (including contact names, phone numbers, physical and e-mail addresses, job titles, birthdays

---

[1] Note: the judgment granting class action status refers to the Defendants as Respondents. Throughout this Motion to Institute Proceedings, the word Respondent(s) has been changed to Defendant(s) for purposes of clarity and consistency.

[2] In electronic systems and computing, firmware is the combination of persistent memory and program code and data stored in it.

and any information stored therein), Class Members' photographs and videos, Class Members' gender, age, postal code, language, and time zone, as well as App-specific activity; i.e. which functions Class Members performed on the App, App ID and password for specific App accounts, the name of the App, the title of a particular App page viewed by the Class Member, and the particular App activity engaged in (e.g., search, view), the search terms entered by the Class Member, the network (e.g., 3G or WiFi), the operating system version, the amount of free storage space on iDevice, Class Members' particular media selections (e.g. movies, songs, videos), the genre of media selected, and the performer in the Class Member's media selection ("Personal and Private Information");

5. As a result, Class Members had the resources of their iDevices consumed and diminished without their knowledge and/or permission. Such resources were measurable and of actual value and included iDevice storage, battery life and bandwidth from each Class Members' wireless services provider;

6. In addition to Class Members' privacy rights 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 had for devices that were substantially devalued by the undesirable characteristics inextricably linked to the devices and their operating environment[3];

7. In the judgment granting class action status on June 27, 2013, the Superior Court of Quebec identified the principle questions or issues of fact and law to be treated collectively as the following:

    a) Did the Defendants cause or facilitate the creation of personally identifiable profiles of Class Members?

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

        Did the Defendants fail to disclose that the Tracking Companies, without authorization, tracked and compiled Class Members' private information?

        Did the Defendants, contrary to their representations, allow the Tracking Companies to create, or cause or facilitate the creation of, personally identifiable consumer profiles of Class Members?

[3] Specifically, these undesirable characteristics refer to the fact that the iDevices allowed Personal and Private Information, identifiable to Class Members, to be collected and transmitted to third-parties.

Are the Defendants continuing to allow the Tracking Companies to retain and/or sell, valuable information assets from and about Class Members?

c) With respect to members of the Geolocation Class:

Did the Defendants collect location data from iPhones even after the user turned "Off" the Location Services function?

Did the Defendants profit, or intend to profit from the collection of geolocation data?

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

e) Were the iDevice Apps used to capture Class Members' UDID, location, username/password, or other such information?

f) What use was made of the Class Members' personally identifiable information?

g) Did the Defendants violate the privacy of Class Members?

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

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

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

II. THE DEFENDANTS

8. Defendant Apple, Inc. ("Apple USA") is an American company with its head office in Cupertino, California. Apple USA developed, manufactured, licensed, distributed, promoted and sold the iDevices throughout Canada, including within the province of Quebec, either directly or indirectly through its affiliate and/or subsidiary Defendant Apple Canada Inc. ("Apple Canada"), the whole as appears more fully from a copy of the *Registraire des enterprises* CIDREQ report, produced herein as **Exhibit P-1**;

9. Apple USA offers a range of mobile communication and media devices, personal computing products and portable digital music players, as well as a

variety of related software, services, peripherals, networking solutions and various third-party hardware and software products. In addition, Apple offers its own software products, including “iOS”, the Company’s proprietary mobile operating system that runs the iDevices; server software; and application software for consumers;

10. Apple also sells Apps (including third-party Apps) that are developed for iDevices in the App Store and it receives a portion of fees for Apps that it sells in the App Store (approximately 30 percent). Apple developed and continues to operate the Apple App Store and it controls the development of, reviews and approves all Apps that are offered in the App Store;

11. At all relevant times, Apple designed, manufactured, promoted, marketed, distributed, and/or sold the iDevices throughout the world, including in Quebec.

12. Given the close ties between Defendants Apple USA and Apple Canada and considering the preceding, both Defendants are solidarily liable for the acts and omissions of the other. Unless the context indicates otherwise, both Defendants will be referred to as “Apple” for the purposes hereof;

- **The Tracking Companies**

13. The Companies named below, collectively referred to herein as the “Tracking Companies”, collect Personal and Private Information transmitted from Class Members’ iDevices for purposes unrelated to their functionality or the execution of Apps on those devices;

14. Google, Inc. (“Google”) is an American company. Google operates ad networks DoubleClick and AdChoices, and provides analytics services through Google Analytics;

15. 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;

16. 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;

17. 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;

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

III. THE SITUATION

A. The iDevices

19. In Canada, the first iPhone model released was the iPhone 3G by Rogers Wireless on July 11, 2008. On June 19, 2009, the iPhone 3GS with the new iPhone 3.0 operating system was released in Canada by Rogers Wireless;

20. Apple designs both the hardware component of the iDevices as well as the operating system (the “iOS”) that runs each iDevice;

21. The iPhone is the most popular of the three (3) iDevices. For example, in 2011 and 2012, Apple sold 72 million and 125 million iPhones respectively. Apple sold approximately 11 million and 8 million iPods touches and 32 million and 58 million iPads in the same time period;

22. ;

23. The iPhone combines a mobile phone, an iPod touch and an internet communication device into a single hand-held product. The iPhone is therefore more than simply a cellular phone and Apple’s marketing of the iPhone has not focused on its ability to make/receive phone calls, but instead, on the availability and utility of third-party Apps as is described more fully below. Indeed, since the launch of the App Store, Apple’s Annual Reports to shareholders have continuously cautioned that:

> “The Company’s future performance depends on support from third-party software developers. If third-party software applications and services cease to be developed and maintained for the Company’s products, customers may choose not to buy the Company’s products.
>
> The Company believes decisions by customers to purchase its hardware products…are often based to a certain extent

> on the availability of third-party software applications and services…
>
> With respect to iPhone, iPad and iPod touch, the Company relies on the continued availability and development of compelling and innovative software applications [which are] distributed through a single distribution channel, the App Store",

The whole as appears more fully from a copy of the Defendants' 2010 Annual Report, produced herein as **Exhibit P-2**;

24. The iPad is a multi-purpose mobile device. Like the iPhone, the iPad is based on Apple's multi-touch technology and comes installed with the App Store. The iPhone and the iPad share many of the same Apps;

25. The price of each iDevice depends on the available memory on the device measured in gigabytes (GB) as well as the model. Apple sells a locked iPhone 4s starting at $450.00 for an 8GB phone, the iPhone 5c for $599.00 for a 18GB phone and $719.00 32GB phone, and the iPhone 5s at $719.00 for a 16GB phone, $819.00 for a 32GB phone and $919.00 for a 64GB phone. Thus, Apple sells additional memory at a premium, telling consumers, "[t]he more gigabytes you have, the more content you can store on your iPhone – apps, games, photos, HD videos, music, films and more", the whole as appears more fully from a copy of two (2) extracts from the Defendants' website at www.apple.com/ca, produced herein *en liasse* as **Exhibit P-3**;

26. Similarly, Apple charges a premium for additional space on the iPad: $419 for the 16GB iPad mini, $519.00 for the 32GB iPad mini, $619.00 for the 64GB iPad mini and $719.00 for the 128 GB iPad mini. As for the iPad Air, the pricing is $100.00 more for each amount of memory. As with the iPhone, Apple encourages consumers to purchase an iPad with a larger capacity, the whole as appears more fully from a copy of three (3) extracts from the Defendants' website at www.apple.com/ca, produced herein *en liasse* as **Exhibit P-4**;

27. ;

28. Thus, it appears that, after the first 16GB of memory, every additional 16GB of memory space is worth approximately $100.00. Every App takes up a portion of the available memory on the iDevice depending on the size of the App;

29. 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;

30. Due to the iPhone's tremendous commercial success, iDevices are now used by many consumers in almost all facets of their daily lives, from choosing a restaurant, to making travel arrangements, to contract management, business expense tracking and conducting banking transactions. In fact, most consumers carry their iDevices with them everywhere they go. While this convenience is valuable to consumers, so too is the information that consumers put and/or store into their iDevices;

B. The Apps

31. Apps are computer programs that users can download and install on their iDevices. Class Members downloaded these Apps from Apple's digital distribution platform, the "Apple App Store" or the "App Store", as part of the use of their iDevices. There are over 1,000,000 Apps available for download in the Apple App Store, the most popular app store of any mobile device;

32. In addition, each iDevice comes pre-programmed with certain Built-In Apps created by Apple. These Apps cannot be deleted from the iDevice as they are integrated into its iOS mobile operating system. The App Store is an example of a Built-In App and provides iDevice purchasers with instant access to any App available through the App Store. Similarly, additional Built-In Apps include the "Photos" app (where users can store personal photographs and videos), the "Contacts" app[4], the "Phone" App, the "Camera" App, the "Calendar" App, the "Maps" App, the "Weather" App, the "Clock" App, the "Notes" App, the "Safari" App, the "Tips" App, the "iTunes Store" App, the "Calculator" App, the "Compass" App, the "Passbook" App, the "Voice Memos" App, the "Videos" App, the "Settings" App as well as the "Messages" App that links to the mobile version of Apple's App Store and enables mobile App Store functionality on the owners' iDevices (Exhibit P-4);

33. The Plaintiffs and other members of the Class (as defined above in paragraph 1) downloaded Apps to their iDevices from the App Store as part of the use of their iDevices. As described further below, Apple claims to review each App before offering it to its users, purports to have implemented App privacy standards and claims to have created a strong privacy protection for its customers. However, unbeknownst to consumers such as the Plaintiffs and Class Members, some of these Apps have been accessing and/or uploading Personal and Private Information from other Apps located on the iDevices without user knowledge or consent (See paragraph 4 for a detailed list);

---

[4] In addition to storing Photos, the Photo app also stores information about when and where the photo was taken. The Contacts app allows users to customize contacts information using the following fields: (1) first and last name and phonetic spelling of each, (2) nickname, (3) company, job title and department, (4) address(es), (5) phone number(s), (6) e-mail address(es), (7) instant messenger contact, (8) photo, (9) birthday, (10) related people, (11) homepage, (12) notes, (13) ringtone, and (14) text tone.

34. For example, users who allow Apps to use location data are also unknowingly giving these apps access to the user's private contacts, photo and video files that can be uploaded and saved on the App's servers. Similarly, users who use an App's "find friends" feature unwittingly allowed these Apps to access and download users' entire address book and contacts list;

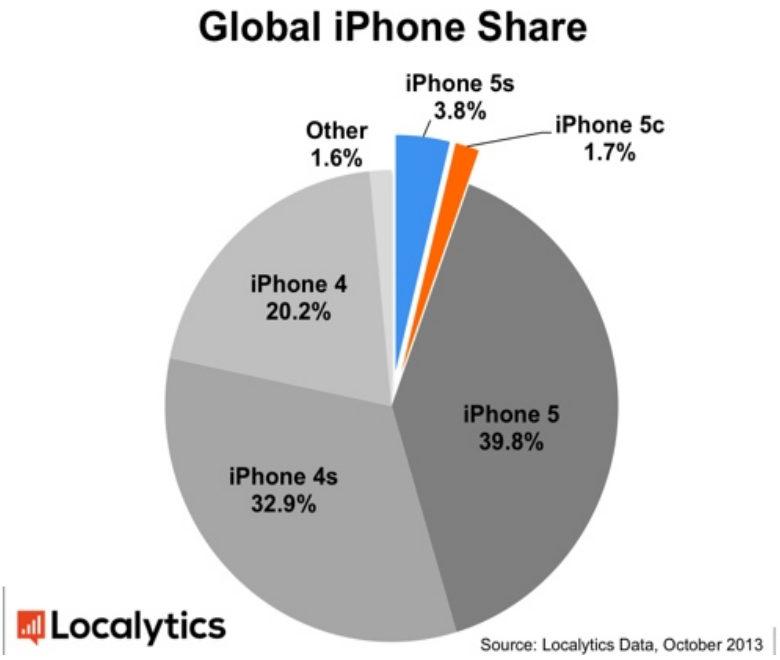
35. Apple failed to properly safeguard iDevices and instead, induced the Plaintiffs and members of the Class to purchase iDevices and to download Apps under the premise that users' private information would remain confidential and would not be shared with third-party developers without express consent. In fact, Apple "has been able to maintain advantage by leveraging its tightly controlled ecosystem—combining compelling hardware and content with the capability to offer consumers a trusted, integrated and simple billing service...", the whole as appears more fully from a copy of the HIS Technology Press Release entitled "Apple Maintains Dominance of Mobile Application Store Market in 2010" dated February 15, 2011, produced herein as **Exhibit P-6**;

36. Apple has repeatedly represented that Apple's products are safe and secure, and that private information could not be accessed by third-party Apps without the user's express consent. Plaintiffs purchased their Apple iDevices with the expectation that Apple had designed the iDevices to protect user privacy and would not have purchased their iDevices and/or would have paid less for the iDevices had they known the truth about the iDevices. Instead, Plaintiffs has learned that third-party Apps are capable of accessing private user data without user consent. Plaintiffs allege that Apple designed the iDevices in such a way as to make these devices vulnerable to unauthorized access by third-parties, despite their misrepresentations that such access was impossible;

37. The basis for the present claim rests on the Defendants' clandestine use of an intrusive tracking scheme implemented through the use of mobile device Apps on Class Members' iDevices;

38. Accordingly, when certain Apps, consisting of Dictionary.com, Paper Toss, Bible App, Urban Spoon, Flixster, The Weather Channel, Textplus 4, Pimple Popper Lite, Pumpkin Maker, Talking Tom Cat, Path, Angry Birds, Cut-the-Rope, Twitter, Facebook, LinkedIn, Gowalla, Foodspotting, Instagram, Foursquare, Beluga, Yelp!, Hipster, Kik Messenger, Flickr, Badoo, Yahoo! Messenger, Pinterest, Synthetic, Turntable.fm, Quora, Eye2i, Tapbots, Remixation, Schematic Labs, Massive Health, Trover, District Nerds, SoundCloud, Forkly, Tiny Review, Fashism, Banjo, Localmind, MusicPound, Tweetbot, Showyou, Soundtracking, Recollect, Ness Computing, Socialcam, Piictu, Stamped, Glancee, Momento, and dishPal, were downloaded and used by Class Members, their Personal and Private Information was harvested, uploaded, stolen and transmitted to third parties and to the Apps themselves;

39. Apple has supposedly limited the availability of some device data in its iOS version 5. Even if this is in fact accurate, millions of iDevice purchasers continue to use the prior version as is depicted below:



40. Not only was Class Members' Personal and Private Information transmitted to third-parties and to the Apps themselves, but a large degree of Class Members' Personal and Private Information was transmitted "in the clear" (sometimes referred to as "plain text"), that is, without any encryption;

C. The App Store – An Apple-Controlled Market Differentiator

41. In 2008, Apple launched the App Store where customers could shop for and download Apps offered by Apple and by third-party developers. Apple heavily promoted the App Store with its "There's an App for That" ad campaign to encourage iDevice purchasers to download Apps from the App Store. For example, Apple's "Dilemmas" commercial encouraged users to download the App UrbanSpoon – which allows users to search for nearby restaurants – with a tagline "the iPhone. Solving life's dilemmas one app at a time." In promoting Apps in July 2008, Apple's website provided:

> *Applications unlike anything you've seen on a phone before.*
> Applications designed for iPhone are nothing short of amazing. That's because they leverage the groundbreaking technology in iPhone — like the Multi-Touch interface, the accelerometer, GPS, real-time 3D graphics, and 3D

> positional audio. Just tap into the App Store and choose from over 500 applications ready to download now.[5]

42. Apple's strong promotion of the App Store proved successful. In the first week of the App Store's launch, Apple reported that users already downloaded more than 10 million Apps from the App Store:

> "The App Store is a grand slam, with a staggering 10 million applications downloaded in just three days,' said Steve Jobs, Apple's CEO. 'Developers have created some extraordinary applications, and the App Store can wirelessly deliver them to every iPhone and iPod touch user instantly."

The whole as appears more fully from a copy of the Apple Press Release entitled "iPhone App Store Downloads Top 10 Million in First Weekend" dated July 14, 2008, produced herein as **Exhibit P-7**;

43. Today, Apple boasts that the App Store has over 1,000,000 Apps for the iPhone and 500,000 Apps for the iPad. Apple heavily encourages purchasers to download Apps. For example, since the inception of the App Store, Apple has told consumers "[t]he more apps you download, the more you'll realize your iPhone can do just about anything you can imagine" and has made similar representations regarding the iPad, the whole as appears more fully from copies of two (2) extracts from the Defendants' website at www.apple.com/ca, produced herein *en liasse* as **Exhibit P-8**;

44. The vast availability of Apps has been credited with propelling the popularity of the iDevices (Exhibit P-2). Apps are not only an integral part of the iDevices themselves, but are the key feature that has differentiated iDevices from similar products;

45. Apple has designed the iDevices to accept Apps only from the App Store, making the App Store the exclusive source from which consumers may obtain Apps for their iDevices. Moreover, the App Store is under Apple's exclusive domain and it has ultimate control of what Apps are available for purchase or download by consumers. In other words, Apple's App store is the exclusive source for Apple and third-party developed Apps designed to run on Apple's iDevices;

46. Since July 2008, over 50 billion Apps have been downloaded by customers using iDevices. In 2011 alone, Apple sold 72.3 million iPhone handsets and 32.4 million iPads. By 2012, Apple's iPhone sales increased to 125 million units and iPad sales rose to 58 million units, the whole as appears more fully from a copy of the Apple Press Release entitled "Apple's App Store Marks

[5] *Cultural Adaptation*, Albert Moran and Michael Keane, Eds., 2010 at page 131.

Historic 50 Billionth Download, from a copy of the Apple Press Release entitled "Apple Reports Fourth Quarter Results" dated October 18, 2011 and from a copy of Apple's Q4 2011 Unaudited Summary Data, produced herein *en liasse* as **Exhibit P-9**;

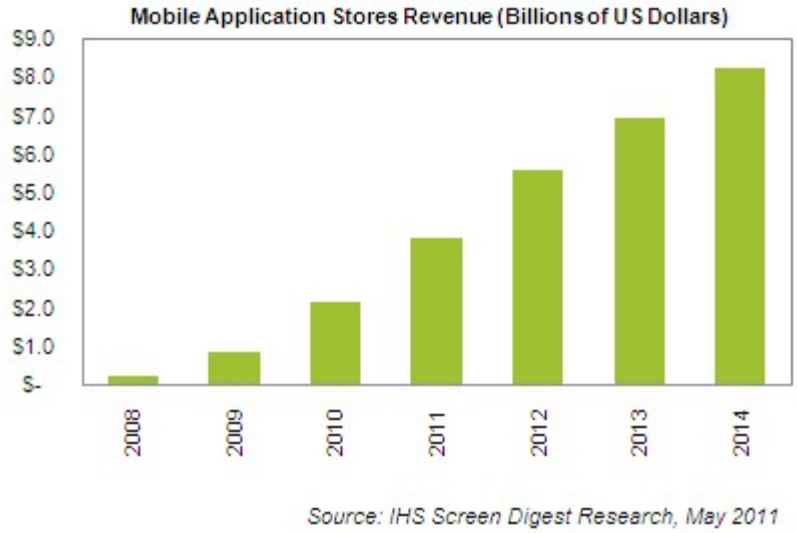
47. As is depicted below, in 2010, the App Store had $1.8 billion in revenues (representing an 82.7 percent market share) and, in 2009, it had $768.7 million in revenues (representing a 92.8 percent market share). Apple was on track to generate over $9 billion for calendar year 2012 (Exhibit P-9);

IHS Screen Digest Table: Global Mobile Applications Store Ranking in 2010 and 2009
(Ranking by Revenue in Millions of U.S. Dollars)

2010 Rank	Store	2009 Revenue	2009 Share	2010 Revenue	2010 Share	Year-Over-Year Growth
1	Apple App Store	$769	92.8%	$1,782	82.7%	131.9%
2	BlackBerry App World	$36	4.3%	$165	7.7%	360.3%
3	Nokia Ovi Store	$13	1.5%	$105	4.9%	719.4%
4	Google Android Market	$11	1.3%	$102	4.7%	861.5%
	Total	**$828**	**100.0%**	**$2,155**	**100.0%**	**160.2%**

Source: IHS Screen Digest February 2011

48. As is depicted below, total mobile app revenues have been growing at an astounding rate. News reports estimate that by 2016, total mobile app revenues will reach a staggering $46 billion. Apple profits from the Apps directly through sales (although it shares App revenue with developers) and, more importantly, through the increased popularity of its iDevices. For example, Apple reported third-party App sales were one of the primary contributors to the $13.8 billion increase in Apple's net sales for its America segment in 2011 along with the higher sales of the iPhone, the whole as appears more fully from a copy of the ABI Research News Report entitled "In-App Purchases to Outpace Pay-Per-Download Revenues in 2012" dated February 16, 2012 and from a copy of the CNET article entitled "Mobile app revenue set to soar to $46 billion in 2016" dated February 16, 2012, produced herein *en liasse* as **Exhibit P-10**;



49. The App Store has been described by many as a game changer both for Apple and for smart phones in general. According to one Morgan Stanley analyst, "Apple changed the view of what you can do with that small phone in your back pocket….Applications make the smartphone trend a revolutionary trend — one we haven't seen in consumer technology for many year", the whole as appears more fully from a copy of The New York Times article entitled "Apple's Game Changer, Downloading Now" dated December 5, 2009 and from a copy of the Mac Observer article entitled "NY Times Takes a Long Look at iPhone, App Store" dated December 7, 2009, produced herein *en liasse* as **Exhibit P-11**;

50. In sum, Apps are an integral part of the iDevices and have propelled Apple and iDevices' popularity. (Exhibit P-11):

> One need not look further than the lobby of Apple's headquarters in Cupertino, Calif., to see that the iPhone and applications that run on it are centerpieces of the company's mobile strategy. Planted squarely in the lobby of the main office, at 1 Infinite Loop, is an impressive, 24-foot-wide array built out of 20 LED screens populated with 20,000 tiny, brightly colored icons.
>
> As Philip W. Schiller, head of worldwide product marketing at Apple, describes how the wall works — each time an application is purchased, the corresponding icon on the electronic billboard jiggles, causing its neighbors to ripple in unison — he, too, becomes animated.
>
> Normally reserved and on message, Mr. Schiller waves his hands back and forth and allows his voice to ascend into giddy registers as he speaks about the potential unleashed by the App Store.

> "I absolutely think this is the future of great software development and distribution," Mr. Schiller says. "The idea that anyone, all the way from an individual to a large company, can create software that is innovative and be carried around in a customer's pocket is just exploding. It's a breakthrough, and that is the future, and every software developer sees it."

51. Apple is heavily reliance on Apps to drive the sale of iDevices and as recognized by Apple itself, it's success, both past and future depends on the availability of Apps (Exhibit P-2);

52. Thus, Apple has a keen interest in continuing to promote the iDevices without disclosing that the Apps are capable of and are actually collecting private data without user consent. As Apple has recognized in its Annual Report (Exhibit P-2), the Company faces significant competition in the mobile communication and media device industry and attracting third-party App manufacturers and consumers are a key to the Company's future:

> The Company currently markets certain mobile communication and media devices, and third-party digital content and applications. The Company faces substantial competition from companies that have significant technical, marketing, distribution and other resources, as well as established hardware, software and digital content supplier relationships. Additionally, the Company faces significant price competition as competitors reduce their selling prices and attempt to imitate the Company's product features and applications within their own products or, alternatively, collaborate with each other to offer solutions that are more competitive than those they currently offer.

53. Apple claims to review each third-party App prior to offering it to its users in the App Store, purports to have implemented App privacy and security measures and claims to have created strong privacy protections for its customers. However, some of these Apps have been transmitting their personal, identifiable information to advertising networks without obtaining their consent;

54. Because of the manner in which Apple developed the iDevices and constructed the App Store, consumers are only able to use their iDevices in the confines of an environment that is controlled by Apple;

55. 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 iDevices. For instance, iDevice users are only allowed to download software specifically licensed by Apple;

56. If a user installs any software that is 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;

57. 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. To the extent Apple is a third-party beneficiary of that contract, consumers are intended third-party beneficiaries of any contract between the App developer and Apple that requires the protection of, and restricts access to, personal consumer information contained on the iDevice. Specifically, the iOS Developer Agreement states:

> 9. Third Party Beneficiary: You and the end-user must acknowledge and agree that Apple, and Apple's subsidiaries, are third party beneficiaries of the EULA, and that, upon the end-user's acceptance of the terms and conditions of the EULA, Apple will have the right (and will be deemed to have accepted the right) to enforce the EULA against the end-user as a third party beneficiary thereof,

The whole as appears more fully from a copy of the iPhone Developer Program License Agreement, produced herein as **Exhibit P-12**;

58. Because Apps are software that users download and install on their iDevices, Apps have access to a huge amount of information about the iDevice user, namely their Personal and Private Information (as described in paragraph 4 herein);

59. All of this information is of great interest to many advertising networks because it is 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 iDevice, supposedly in order to serve ads that are catered to the App user and more likely to be of interest to them;

60. Considering that mobile advertising is such big business, advertisers, website publishers and ad networks are seeking ways to better track their web users

and to learn 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;

61. Apple induced customers to purchase iDevices, at least in part, by offering thousands of so-called "free" Apps in its App Store. However, during the relevant time period, Apple failed to disclose to the Class Members that, *inter alia*, those "free" Apps collected their Personal and Private Information and sent it to third-party mobile advertising and analytics companies, i.e. the Tracking Companies, with neither user consent, nor detection;

62. During the relevant time period, Class Members had no means to otherwise avoid the data collection and tracking by Apple and the third-party Tracking Companies. As noted above and detailed further below, Apple controls the environment in which its iPhones operate and Apple controls what data Apps can and cannot transmit to third-parties. Most importantly, Apple controls the fact that its customers are kept in the dark regarding the level of data collection that is actually built into this environment;

63. Apple obtains revenue by marketing the ostensibly "free" Apps, and the availability of "free" Apps is tied to the availability of free data from iDevice purchasers, who have no idea what they are allowing access to, in terms of personal data, when they purchase an iDevice;

64. Class Members were not fully informed by Apple that, to use "free" Apps or geolocation features on their iDevices, they would unknowingly provide data that would allow the third-parties to personally identify them and thereafter give the third-parties full access to any user data on their iDevices as detailed below;

D. Apple Controls the Development Process for Apps Available for iDevices

65. In addition to controlling the characteristics and distribution of Apps, described above, Apple exercises substantial control over their development and functionality. Apple is notorious for complete control over its products. Apple's former Chief Executive Officer ("CEO"), Steve Jobs has publicly stated, "…our job is to take responsibility for the complete user experience. And if it's not up to par, it's our fault, plain and simply", the whole as appears more fully from a copy of an extract from the CNN Money article entitled "Steve Jobs speaks out", dated March 7, 2008, produced herein as **Exhibit P-13**;

66. To that end, Apple has designed iDevices to accept Apps only from the App Store, thereby making the App Store the exclusive source from which consumers may obtain apps for their iDevices whether or not the Apps are sold or available for free. The only exception to this restriction, are devices that are

modified by users to circumvent the iOS operating system's restrictions on downloading apps from sources other than the App Store, a process known as "iOS jailbreaking" or simply, "jailbreaking". While jailbreaking iDevices is legal, Apple has sought to discourage jailbreaking by announcing that the practice voids the iDevices' warranty, the whole as appears more fully from a copy of an article from the Defendants' website at www.apple.com entitled "Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues" dated February 9, 2014, produced herein as **Exhibit P-14**;

67. In order to offer an application for download in the App Store, a third-party developer must be registered as an "Apple Developer" and agree to the iOS Developer Agreement (the "IDA"), the Program License Agreement (the "PLA") with Apple as well as pay the $99.00 yearly registration fee. 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;

68. Apple provides third-party developers with Review Guidelines and conducts a review of all applications submitted for inclusion in the App Store for compliance with the above documents;

69. To get applications into the App Store, Apple requires developers to submit their App and to wait for approval or rejection by Apple[6]. Apple has the sole discretion over the App approval process and may reject a proposed App for any reason. Apple may further unilaterally choose to cease distributing any App at any time and for any reason. Apple has explicitly reserved the right to cease distributing any App that, among other things, (i) breaches the terms and conditions of the licensing agreements, (ii) provide Apple with inaccurate documents or information, or (iii) Apple has been notified or has reasons to believe that the App violates, misappropriates, or infringes the rights of a third party;

70. In addition to having exclusive control of the Apps offered for sale or download at the App Store, Apple controls the App development process. For example, App developers must buy and use Apple's Software Development Kit ("SDK"), which provides highly detailed guidelines for App development. The SDK can only be installed on an Apple computer and all Apps developed using Apple's SDK will only function on iDevices. These Apps can only interact with the iDevice operating system and features in the ways permitted by the iOS Developer Agreement and SDK;

---

[6] Rejected apps are given feedback on the reason they were rejected so they can be modified and resubmitted.

71. Apple strictly regulates the Apps that are available in the App Store. Moreover, the Apps can only collect information and data from iPhones as allowed by Apple, and they can only be distributed in Apple's App Store upon Apple's approval and digital signature;

72. Thus, Apple retains complete control over the types of Apps it allows into its marketplace and acts as a gatekeeper to the App Store. Indeed, when Apple first launched the App Store, Steve Jobs stated, "[t]here are going to be some apps that we're not going to distribute. Porn, malicious apps, apps that invade your privacy", the whole as appears more fully from a copy of the Engadget article entitled "Engadget Cares: save us from Apple's groundbreaking, developer-shackling App Store" dated September 25, 2008, produced herein as **Exhibit P-15**;

73. Mr. Jobs further made this clear at an iOS SDK (or Software Developer Kit) Press Conference[7] on March 6, 2008 showing the limitations on the type of Apps that would be allowed on the iPhone:

74. In October 2007, Mr. Jobs similarly stated:

> Let me just say it: We want native third party applications on the iPhone, and we plan to have an SDK in developers' hands in February. We are excited about creating a vibrant third party developer community around the iPhone and enabling hundreds of new applications for our users. It will take until February to release an SDK because we're trying to do two diametrically opposed things at once — provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. As our phones become more powerful, these malicious programs will become more dangerous, and since the iPhone

[7] Formerly, iPhone SDK.

> is the most advanced phone ever, it will be a highly visible target. We think a few months of patience now will be rewarded by many years of great third party applications running on safe and reliable iPhones.

The whole as appears more fully from a copy of the Apple Insider article entitled “Steve Jobs confirms native iPhone SDK by February” dated October 17, 2007, produced herein as **Exhibit P-16**;

75. Apple has echoed this sentiment on several occasions. For example, in 2010, it cracked down on Apps that contained “overtly sexual” content and removed several such apps from the App Store:

> Philip W. Schiller, head of worldwide product marketing at Apple, said in an interview that over the last few weeks a small number of developers had been submitting “an increasing number of apps containing very objectionable content.”
>
> “It came to the point where we were getting customer complaints from women who found the content getting too degrading and objectionable, as well as parents who were upset with what their kids were able to see,” Mr. Schiller said.

The whole as appears more fully from a copy of the New York Times article entitled “Apple Bans Some Apps for Sex-Tinged Content” dated February 22, 2010, produced herein as **Exhibit P-17**;

76. In essence, right from the beginning in 2008, Apple has taken and has maintained the role of gatekeeper of the Apps available in the App Store:

> “Apple wants to be seen as reaffirming control over the App Store and reaffirming control over the entire ecosystem so that everybody knows that Apple’s in charge…
>
> Apple has been very clear since day one that it owns the playground and it will define the rules by which all games within that playground are played.”

The whole as appears more fully from a copy of the National Post article entitled “No sex, please, we're Apple” dated February 27, 2010, produced herein as **Exhibit P-18**;

77. Likewise, Mr. Jobs, who often responded to user emails, wrote in a much publicized e-mail responding to a reporter’s question:

> "Yep, freedom from programs that steal your private data. Freedom from programs that trash your battery. Freedom from porn. Yep, freedom. The times they are a changing', and some traditional PC folks feel like their world is slipping away. It is…We believe we have a moral responsibility to keep porn off the iPhone. Folks who want porn can buy an Android."

The whole as appears more fully from a copy of Tech Crunch article entitled "Steve Jobs Spars With Gawker Blogger Over Revolutions, Freedom, and Porn" dated May 15, 2010, produced herein as **Exhibit P-19**;

78. Apple has also famously refused to integrate Adobe Flash technology despite users' requests, with Mr. Jobs explaining that Apple will not integrate Adobe's flash technology because of reliability, security and performance concerns. These "concerns" have been criticized as being merely a "smokescreen" as over 100 Apps that used Adobe's software have been accepted in the App Store. According to the CEO of Adobe, "[w]hen you resort to licensing language" to restrict this sort of development, it has "nothing to do with technology", the whole as appears more fully from a copy of an extract from the Defendants' website at www.apple.com/ca and entitled "Thoughts on Flash" dated April, 2010 and from a copy of the Wall Street Journal article entitled "Highlights: The Journal's Exclusive Interview With Adobe CEO" dated April 29, 2010, produced herein *en liasse* as **Exhibit P-20**;

79. On April 20, 2011, Apple's current CEO, Timothy Cook noted that users appreciate Apple's gatekeeper function, stating "I think the user appreciates that Apple can take full responsibility for their experience..." the whole as appears more fully from a copy of the Business Insider article entitled "Here's Apple's Weak Non-Answer To Why Android Won't Torch The iPhone Like Windows Did To The Mac" dated April 20, 2011, produced herein as **Exhibit P-21**;

80. In sum, Apple has attempted to cultivate a perception that its products are safe and that Apple strives to protect users;

81. Apple completely controls users' experience from development of the iDevice, development and selection of the Apps available at the App Store, as well as restriction of how the iDevice can be modified by users (e.g., such as blocking users from modifying their devices or installing unapproved software on their iDevices). Apple further restricts information concerning the development process and prohibits developers from publicly discussing Apple's standards for App development through the PLA;

82. The App Store Review Guidelines set forth the technical, design, and content guidelines Apple will use when reviewing an app for inclusion in Apple's App Store. These guidelines state that apps "cannot transmit data about a user

without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." The guidelines further provide that "Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected." This includes the transmission of personally identifiable information. In addition, the requirements of the PLA empower users to control access to user or device data, and require user consent before user or device data can be collected, the whole as appears more fully from a copy of the App Store Review Guidelines and from a copy of Into Mobile article entitled "Apple confirms apps will soon require user permission to access contact data" dated February 15, 2012, produced herein *en liasse* as **Exhibit P-22**;

83. According to Apple, its operating system, iOS, "is highly secure from the moment you turn on your iPhone." For example, in September 2011, Apple's website provided:

Safe and secure by design.

iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information. Optional parental controls let you manage iTunes purchases, Internet browsing, and access to explicit material. To guard your privacy, apps requesting location information must get your permission first. You can set a passcode lock to prevent unauthorized access to your phone and configure iPhone to delete all your data after too many unsuccessful passcode attempts. And in the event your iPhone is lost or stolen, Find My iPhone allows you to locate it on a map, lock its screen, and remotely delete all your data. If you get it back, you can restore everything from your last backup.

84. Apple makes similar claims with respect to the iPad;

85. With respect to location-based services, the Apple privacy policy provides only that the company may obtain anonymous location data that does not personally identify the user:

> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.

The whole as appears more fully from a copy of the Defendants' Privacy Policy, produced herein as **Exhibit P-23**;

86. In February 2012, an Apple spokesperson further reaffirmed that "apps that collect or transmit a user's contact data without their prior permission are in violation of our guidelines" (Exhibit P-22);

E. Despite Apple's Promises to Safeguard Users' Privacy, Apps Have Been Surreptitiously Collecting User Data

87. In contrast to Apple's public statements, Apple-approved Apps have accessed, downloaded and/or copied users' Class Members' Personal and Private Information (See Paragraph 4 for a detailed list) without the users' knowledge or consent when a user agrees to allow an App to access the user's then current locations;

88. For example, when an App such as Angry Birds asks purchasers to use their current location, in addition to using the purchaser's location, the App is able to gain access to other apps such as the Photos App. This is in direct contravention to Apple's representation, as depicted above in paragraph 89, that its iOS is safe and secure and that "All apps run in a safe environment, so a website or app can't access data from other apps";

89. Similarly, several App manufacturers acknowledged that they had surreptitiously accessed and uploaded information from users Contacts App without disclosing to users that the feature would leave their private information vulnerable to unauthorized download by the third-party app manufacturer, the whole as appears more fully from a copy of the BBC News article entitled "iPhone apps Path and Hipster offer address-book apology" dated February 9, 2012, from a copy of the Into Mobile article entitled "Congress jumps into the Path address book fray" dated February 15, 2012 and from a copy of the TNW article entitled "What iOS apps are grabbing your data, why they do it and what should be done" dated February 15, 2012, produced herein *en liasse* as **Exhibit P-24**;

90. These uses go well beyond what a reasonable iDevice user understands himself or herself to be consenting to when he or she allows an App to access data on the iDevice for the App's functionality;

91. In early February 2012, it was uncovered that the App "Path" was uploading data stored on users' iDevices (including address book and calendar) to its servers, causing the App developers' CEO to issue an apology to Path users for accessing and using their Personal and Private Information, the whole as appears more fully from a copy of the Apology dated February 8, 2012, produced herein an **Exhibit P-25**;

92. Likewise, other popular apps consisting of: Dictionary.com, Paper Toss, Bible App, Urban Spoon, Flixster, The Weather Channel, Textplus 4, Pimple Popper Lite, Pumpkin Maker, Talking Tom Cat, Angry Birds, Cut-the-Rope, Twitter, Facebook, LinkedIn, Gowalla, Foodspotting, Instagram, Foursquare, Beluga, Yelp!, Hipster, Kik Messenger, Pinterest, Synthetic, Turntable.fm, Quora, Eye2i, Tapbots, Remixation, Schematic Labs, Massive Health, Trover, District Nerds, SoundCloud, Forkly, Tiny Review, Fashism, Banjo, Localmind, MusicPound, Tweetbot, Showyou, Soundtracking, Recollect, Ness Computing, Socialcam, Piictu, Stamped, Glancee, Momento, and dishPal may have also downloaded users' data without their explicit consent in contrast to Apple's stated Privacy Policy (Exhibits P-23 and P-31);

93. Following revelations that Path secretly uploaded user data, it was discovered that another App, Hipster, also uploads users' address books to its servers:

> The Hipster app allows you to deselect the 'Contacts' button when looking for new friends, but it is enabled by default. Therefore, there is no way to avoid sending address book emails to Hipster, as far as I can tell.

The whole as appears more fully from a copy of the Info Security article entitled "Clueful – an app to describe app behavior" dated May 24, 2012, produced herein as **Exhibit P-26**;

94. In response to the above, Hipster's CEO, Doug Ludlow, posted an apology to Hipster's users for failing to protect users' privacy, the whole as appears more fully from a copy of the Apology, dated February 8, 2012, produced herein as **Exhibit P-27**;

95. Indeed, copying address book data, photos, videos and more without a user's consent is against Apple's rules. Nevertheless, Apple failed to properly screen Apps and allowed such Apps to be sold in the App Store without disclosing to iDevice purchasers that their iDevices may be vulnerable to unauthorized access;

96. This significant data breach as well as claims that the practice of collecting consumers' address book contacts without their permission is common and accepted among iOS app developers has led two (2) members of Congress to write to Apple's CEO to inquire about Apple's privacy problems and whether Apple's iOS app developer policies and practices adequately protect consumer privacy, the whole as appears more fully from a copy of the Letter dated February 15, 2012, produced herein as **Exhibit P-28**;

97. Apple's response to this letter was quite unsatisfactory simply referring the members of Congress to its webpage for answers, the whole as appears more

fully from a copy of the Letter dated March 2, 2012, produced herein as **Exhibit P-29**;

98. On March 14, 2012, the two (2) members of Congress sent a follow-up letter to the CEO of Apple re-requesting that their questions be addressed and that Apple address new concerns that Apps are accessing photos on the iDevice as well as online tracking concerns, the whole as appears more fully from a copy of the Letter dated March 14, 2012, produced herein as **Exhibit P-30**;

99. On March 22, 2012, Representatives Waxman and Butterfield also sent letters to thirty-four (34) sellers of Apps inquiring about their information collection and use practices. These sellers included Foodspotting; Inc.; Synthetic, LLC (Disposable); Turntable.fm, Inc.; Twitter, Inc.; Foursquare Labs, Inc.; Quora, Inc.; Eye2i, Inc.(MusicPound); Tapbots, LLC (Tweetbot); Remixation (Showyou); Schematic Labs (Soundtracking); Massive Health, Inc.; Trover LLC; District Nerds, LLC; SoundCloud Ltd.; Hipster, Inc.; Forkley, Inc.; Tiny Review; Fashism, LLC; Path, Inc.; Banjo, Inc.; Redaranj, LLC (Recollect); Socialcam, Inc.; Brew Labs, Inc. (Pinterest); Piictu, Inc.; Stamped, Inc.; Burbn, Inc. (Instagram); Apple Inc., Glancee, Inc.; d3i Ltd. (Momento); LinkedIn Corporation; SK Plante, Co., Ltd. (dishPal); and Facebook, the whole as appears more fully from a copy of the Business Insider article entitled "These 34 App Makers Got Letters From Congress Questioning Their Privacy Practices" dated March 22, 2012, produced herein as **Exhibit P-31**;

100. Similar concerns were raised by Senator Charles E. Schumer who called for a Federal Trade Commission investigation into the "disturbing and potentially unfair practices in the smartphone application market", the whole as appears more fully from a copy of the Press Release entitled "Schumer call for FTC Investigation of Apple and Android Phone Platforms that allow Apps to Steal Private Photos and Address Books and Post them Online – Without Consumer's Consent" dated March 5, 2012, produced herein as **Exhibit P-32**;

101. The fact remains simple, Apple led iDevice users to believe that their private data stored on their iDevices would be protected and not be accessible to third-parties. However, as the investigations into privacy continued, it became apparent that a myriad of user information was being sent to third-parties, the whole as appears more fully from a copy of The New York Times article entitled "Apple Loophole Gives Developers Access to Photos" dated February 28, 2012, produced herein as **Exhibit P-33**;

F. <u>The Unique Device ID – The Ultimate Tracker</u>

102. Browser cookies are the traditional method used by advertisers to track web users' activities. But browser cookies have a significant disadvantage 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;

103. The Defendants; however, have found their solution— the Unique Device ID ("UDID") that Apple assigns to every iDevice. 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;

104. Because the UDID is unique to each iDevice, 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 from the iDevice, 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;

105. Apple's UDID causes concern for several reasons. First, unlike with desktop computers, the iDevices travel almost everywhere with the user. In addition, iDevices tend to be unique to an individual. While someone might borrow someone else's iDevice briefly, it is unusual for individuals to frequently trade iDevices;

106. Furthermore, unlike a desktop computer, the iDevices come equipped with the tools necessary to determine their geographic location as is detailed further below. Thus, being able to identify a unique device and combining that information with the device's geographic location, gives the advertiser a huge amount of information about the user of an iDevice, namely their Personal and Private Information (as described in paragraph 4 herein). From the perspective of advertisers engaged in surreptitious tracking, this is a perfect means of tracking iDevice users' interests and likes on the Internet;

107. Apple certainly understands the significance of its UDID and users' privacy and has recently opted to no longer accept new apps or app updates that access UDIDs, the whole as appears more fully from a copy of the Ad Exchanger article entitled "Apple Sets Cut-Off For UDID Apps" dated March 22, 2013 and from a copy of the Macstories article entitled "New iPhone Dev Agreement Bans the Use of 3rd Party Services and Analytics" dated April 11, 2010, produced herein *en liasse* as **Exhibit P-34**;

108. 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", the whole as appears more fully from a copy of the 148 Apps article entitled "Is Apple Trying to Create a Mobile Ad Monopoly on the iPhone?" dated April 12, 2010, produced herein as **Exhibit P-35**;

109. This change prompted a number of third-party advertising networks and metrics/analytics companies (who have been receiving a steady flow of user data from iDevice Apps) to protest. One prominent critic was the CEO of Google-owned AdMob, the whole as appears more fully from a copy of the Style Loft article entitled "AdMob protests as Apple changes developer rules" dated June 10, 2010, produced herein as **Exhibit P-36**;

110. Apple faced a mountain of criticism over this change and accordingly, 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);

111. These changes were not engendered by a genuine concern over consumers' data, but only by a concern for protection of Apple's own iDevice data. Furthermore, neither of Apple's amendments to its Developer Agreement directly addressed use of UDID data;

112. The general practice engaged in by the Defendants was recently confirmed by Eric Smith, Assistant Director of Information Security and Networking at Bucknell University in Lewisburg, Pennsylvania. His research is contained in a report entitled, "iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)", the whole as appears more fully from a copy of said report, produced herein as **Exhibit P-37**;

113. 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 P-38**;

114. Class Members' valuable UDID information, demographic information, location information, address book, as well as their application usage habits is personal and private. Such information was taken from them without their knowledge or consent. Class Members are entitled to compensation for this unlawful and intentional invasion of their privacy;

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

G. Apple's Collection of Geolocation Data Apple Misled Class Members about the ability to Opt-Out of Its Tracking Program

116. Apple is developing an expansive database containing information about the geographic location of cellular towers and wireless networks throughout Canada. This information forms the underlying data necessary for a digital marketing grid that Apple can use to accurately deploy targeted advertisements to mobile phone users in the future. A digital marketing grid of this scope is highly lucrative to Apple, as the mobile phone advertising industry is projected to become a $2.5 billion-dollar market by 2015;

117. In order to collect the information needed to create the digital marketing grid described above, Apple previously designed iOS to send geolocation data from customers' iPhones to Apple's servers, including, inter alia, information revealing the unique identifiers of nearby cellular towers and wireless networks;

118. 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*[.]"

The whole as appears more fully from a copy of Apple's Terms and Conditions, produced herein as **Exhibit P-39**;

119. 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 to transmit geolocation information;

120. Furthermore, it now appears that the information collected and sent from users' iPhones to Apple can be inputted into a publicly searchable database, which in turn can potentially reveal an estimate of each users' exact location;

121. As a result, Apple— or anyone with access to this geolocation data— is able to approximate the location of thousands, if not millions of users, even after these users believed that they had actually denied Apple access to their geolocation information;

122. On April 27, 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". This admission plainly contradicts Apple's representations to its customers regarding the ability to opt-out of its geolocation tracking program. 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 P-40**;

123. Apple's failure to fulfill its commitments, namely, Apple's practice of capturing frequent and detailed information about iDevice users' locations for up to one year, even when the iDevice users 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 and Private Information;

124. As a result of the above, Geolocation Class members who had their respective "Location Services" turned to "off" could not prevent Apple from collecting data about their real-time locations;

125. In June 2010, with the release of its iOS 4, 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;

126. 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 iDevice. The file data was, unbeknownst to Class Members, also available through Apps to third-party marketers;

127. 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);

128. The storage space on Class Members' iDevices is storage space they paid for, and the cost 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;

129. 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 resources when they purchased their iDevices, yet Apple essentially took it back from Class Members without their permission, consent or knowledge;

H. <u>The True Cost of the iDevices</u>

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

131. 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;

132. 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", the data transmission and storage costs that would be imposed and the iDevice resources that the Defendants would secretly consume;

133. Apple induced the purchase of iDevices by Class Members by offering thousands of ostensibly "free" Apps in its App Store. However, 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, i.e. the Tracking Companies;

134. 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 iDevice used to synchronize or back-up the iDevice;

135. 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 Companies would surreptitiously obtain Personal and Private 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;

136. 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;

137. Apple's competitors manufacture, market, and distribute comparable mobile devices that do not collect Personal and Private 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;

138. 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 had it fully disclosed all its data-sharing activities;

I. Apple Uses Class Members' Personal and Private Information to Lure Low Cost Apps to its App Store

139. 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 (Exhibit P-2);

140. Apple takes steps to keep App developers satisfied in order to encourage them 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;

141. The App developers then use that information about Class Members to obtain advertising revenue from the Tracking Companies;

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

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

144. 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 Companies 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;

145. 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' privacy was compromised, the whole as appears more fully from a copy of the Tech Crunch article entitled "Apple Sneaks A Big Change Into iOS 5: Phasing Out Developer Access To The UDID" dated August 19, 2011, produced herein as **Exhibit P-41**;

J. Apple Failed to Protect User Privacy and the Security of User Data as Promised

146. As described above, 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;

147. 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;

148. 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;

149. Apple positively 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; and

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

150. Despite Apple's representations to Class Members and its duty to protect their data from third-parties such as the Tracking Companies, Apple knowingly offered Apps in the App Store that allowed consumers' privacy to be violated and their security to be compromised;

151. 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 and Private 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;

K. The Tracking Companies Exploit Access to Consumer Data

152. Notwithstanding Apple's control of the user experience, it designs its iDevices to be very open when it comes to disclosing information about consumers to the Tracking Companies, 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;

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

154. When users download and install the Apps on their iDevices, the Tracking Companies' software accesses Personal and (…) Private Information on those devices without users' awareness or permission and transmits the information to the Tracking Companies, 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;

155. Some Tracking Companies 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 Companies and provide the communications channel for the Tracking Companies to acquire and upload users' Personal and Private Information;

156. The Tracking Companies, 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;

157. With the Personal and Private Information acquired, the Tracking Companies used the information to compile 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 Companies require none of this information to provide the user services for which the Apps were marketed;

158. The Tracking Companies acquired Personal and Private Information and compiled profiles that were unnecessary to the Apps' stated functions but were useful to the Tracking Companies in their commercial compilation, use, and sale of consumers' Personal and Private Information;

159. Because of Apple's and the Tracking Companies' control and coding, Class Members are unable to detect, manage, or avoid this collection and transmission of information;

160. Apple is aware that Apps are providing a conduit for the Tracking Companies to acquire consumers' Personal and Private Information without consumers' knowledge or consent;

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

162. 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 Companies' practices;

L. <u>Lack of Consent</u>

163. 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;

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

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

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

167. The Tracking Companies sell to and/or purchase and merge users' Personal and Private Information with other Personal and Private 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;

168. The Tracking Companies and other parties to the information market use the merger of Personal and Private Information to effectively or actually de-anonymize consumers;

169. The Tracking Companies used Class Members' Personal and Private Information for their own economic benefit;

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

171. The Tracking Companies' actions were knowing, surreptitious, and without notice and so were conducted without authorization and exceeding authorization. The Tracking Companies misappropriated Class Members' Personal and Private Information;

172. Class Members were not informed as to the true cost of their iDevices due to the lack of disclosures about third party tracking, tracking by Apple (even when Location Services were set to "Off"), the data transmission and storage costs that would be imposed, and the iDevice resources that Apple and the Tracking Companies would secretly consume;

173. The 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 Companies would surreptitiously obtain Personal and Private Information from their iDevices, track their activity and geolocation, and consume portions of the "cache" and/or gigabytes of memory on their devices— memory that consumers paid for the exclusive use of when they purchased their iDevice;

174. Because Apple did not disclose the true costs of their iDevices, the Plaintiffs/Class Representatives and the Class Members were misled into purchasing a product that did not meet their reasonable expectations;

M. Tracking Companies' Harmful Use of Class Members' Resources

175. In addition to the harms alleged above, the Tracking Companies' unauthorized, surreptitious collection of Class Members' information, subjected Class Members to harm because the Tracking Companies' actions consumed resources to which Class Members had the right of control and use;

176. For example, some Tracking Companies 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 Companies 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;

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

178. The rate at which battery charge was diminished on the iDevices as a result of the Tracking Companies' actions was material to Class Members, particularly given the power resource constraints on the iDevice: the Tracking Companies' 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;

179. Not only did the Tracking Companies' actions cause Class Members' iDevice batteries to discharge more quickly, rendering the iDevices less useful given power constraints, but the Tracking Companies' 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 Companies shortened the actual utility and life of the iDevice batteries, for which charging capabilities are diminished over repeated re-chargings;

180. Class Members purchased the iDevices believing the purchase included the advertised features provided by the plethora of "free" Apps available, unaware of the undisclosed costs imposed by Apple, including the appropriation of their iDevice resources and bandwidth, as well the exploitation of their Personal and Private Information;

181. Apple played an active role in facilitating and fostering an environment that encouraged routine violations of Class Members' reasonable expectations and ironically, with Apple's own assurances;

182. Class Members had a reasonable expectation that their privacy rights would be protected and the Defendants' various unlawful and intentional interference with their privacy has caused offence, distress, humiliation and/or anguish;

183. 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 an important factor in their purchasing decisions;

184. 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 Companies would surreptitiously obtain Personal and Private Information from their iDevices, track their activity and geolocation, deplete battery resources, and consume portions of the "cache" and/or gigabytes of memory on their devices – memory that Plaintiffs paid for the exclusive use of when they purchased their iDevice;

N. The Fault

185. Apple has represented to Plaintiffs and other Class Members, expressly or by implication, that the App Store does not permit apps that "violate[] [Apple's] developer guideline' including apps that violate user privacy";

186. Apple has represented to the Plaintiffs and other purchasers, 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" (Exhibit P-22);

187. Apple has represented to Plaintiffs and Class Members, expressly or by implication, that iDevices are "Safe and secure" and that "iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information…To guard your privacy, apps requesting location information must get your permission first." However, third-party apps such as Hipster and Path have admittedly accessed and uploaded users' full contacts information without user consent. Likewise, the iDevices are vulnerable to third-party apps uploading photos and videos when requesting access to user's location, despite Apple's promise that the iOS is secure and that apps cannot access data from other Apps;

188. Apple failed in its duties, including, but not limited to the following:

a) It failed to exercise reasonable care to protect Class Members' privacy,

b) It failed to design the iDevices so as to prevent Class Members from being harmed,

c) It failed to review and/or to remove privacy-violating apps from the App Store,

d) It failed to warn Class Members of any harm of which it is aware might foreseeably occur and instead actively misrepresented to Class Members that the iDevices were safe and secure,

e) It constructed and controlled consumers' user experience and mobile environment so that consumers could not reasonably avoid such privacy-affecting actions,

f) It failed to take reasonable steps to prevent others from causing Class Members harm when that harm is reasonably foreseeable by Apple, and

g) It failed, as the proprietor of its App Store, to protect its patrons from, or at least warn of, harm from third parties;

IV. THE EXAMPLE OF THE PLAINTIFFS/ CLASS REPRESENTATIVES

A. NUMA BALMER

189. Plaintiff/ Class Representative Numa Balmer purchased an iPhone 3G in the summer of 2008 from Fido Solutions in the province of Quebec;

189.1 Plaintiff/ Class Representative Balmer purchased an iPhone 4 in the Summer of 2010 from Fido Solutions in the province of Quebec;

190. Plaintiff/ Class Representative Balmer has downloaded numerous Apps onto his iPhone 3G and/or 4 including, but not limited to: Dictionary.com, Urban Spoon, The Weather Channel, Talking Tom Cat, Cut-the-Rope, Angry Birds, Twitter, Facebook, LinkedIn, Instagram, SoundCloud;

191. As a consequence of his installation of the various Apps onto his iPhones, Plaintiff / Class Representative Balmer has had his privacy rights violated by the Defendants' unlawful and intentional actions;

B. LISE SÉNÉCAL

191.1 Plaintiff/ Class Representative Lise Sénécal purchased an iPhone 3 from Fido Solutions in late 2008 in the province of Quebec;

191.2 Plaintiff/ Class Representative Sénécal purchased an iPhone 4S from Fido Solutions in the spring of 2011 in the province of Quebec;

191.3 She had downloaded numerous Apps onto her iPhone 3 and/or iPhone 4S including, but not limited to: Dictionnary.com, Paper Toss, Urban Spoon, Flixster, Weather Channel, Textplus 4, Talking-Tom-Cat, Angry Birds, Twitter, Facebook, LinkedIn, Foodspotting, Instagram, Foursquare, Yelp!, Hipster, Badoo, Pinterest, SoundCloud, and Soundtracking;

191.4 As a consequence of her installation of the various Apps onto her iPhones, Plaintiff / Class Representative Sénécal has had her privacy rights violated by the Defendants' unlawful and intentional actions;

C. RAMZI SFEIR

191.5 Plaintiff/ Class Representative Ramzi Sfeir purchased an iPhone 3 from *Société française du radiotéléphone* (SFR) in late 2009 in France;

191.6 Plaintiff/ Class Representative Sfeir purchased an iPhone 4 from Fido Solutions in late 2011 in the province of Quebec, the whole as appears

more fully from a copy of Plaintiff/ Class Representative Sfeir's introductory email communication from Fido, dated October 17, 2011, produced herein as **Exhibit P-42**;

191.7 He had downloaded numerous Apps onto his iPhone 3 and/or iPhone 4 including, but not limited to: Dictionnary.com, Urban Spoon, Flixster, Weather Channel, Talking-Tom-Cat, Angry Birds, Twitter, Facebook, LinkedIn, Instagram, Foursquare, Kik Messenger Pinterest, Soundcloud

191.8 As a consequence of his installation of the various Apps onto his iPhones, Plaintiff/ Class Representative Sfeir has had his privacy rights violated by the Defendants' unlawful and intentional actions;

192. The Plaintiffs'/ Class Representatives' damages are a direct and proximate result of the Defendants' conduct;

193. In consequence of the foregoing, Plaintiffs / Class Representatives are justified in claiming damages;

V. THE DAMAGES

194. Every member of the Class has downloaded Apps onto either their iPhone or iPad;

195. Each member of the Class has had their privacy rights violated due to the Defendants' unlawful and intentional actions and/or invasions;

196. All of the damages to the Class Members are a direct and proximate result of the Defendants' conduct;

197. In consequence of the foregoing, members of the class are justified in claiming as damages an estimated, *sauf à parfaire* when further information is available so as to better evaluate the number of Class Members in Quebec:

FOR THESE REASONS, MAY IT PLEASE THIS HONOURABLE COURT TO:

GRANT the Class Action of the Plaintiffs/ Class Representatives and each of the members of the Classes;

DECLARE the Defendants solidarily liable for the damages suffered by the Plaintiffs / Class Representatives and each of the members of the Classes;

ORDER the Defendants to permanently cease the collection and dissemination of Class Members' personally-identifiable information without their consent;

CONDEMN the Defendants to pay to each member of the Classes 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 Classes, 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 December 30, 2010, 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 Classes;

Montreal, December 29, 2016

(s) Jeff Orenstein

_____
CONSUMER LAW GROUP INC.
Per: Me Jeff Orenstein
Attorneys for the Plaintiffs/ Class Representatives

CONSUMER LAW GROUP INC.
1030 rue Berri, Suite 102
Montréal, Québec, H2L 4C3
Telephone: (514) 266-7863
Telecopier: (514) 868-9690
Email: jorenstein@clg.org