IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

JOAN SMITH and **BYRAN HICKS**, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, vs. **GOOGLE, INC.**, a Delaware Corporation; Defendants.	Case No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs, Joan Smith and Bryan Hicks, on behalf of themselves and all others similarly situated, by and through their attorneys, as and for their complaint, and demanding trial by jury, allege the following upon information and belief, based upon, *inter alia*, investigation conducted by and through their attorneys, and upon their personal knowledge as to all other allegations.

NATURE OF THE ACTION

1. Plaintiffs bring this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of themselves and a class of similarly situated Internet users (each a "class member" of the putative "class") who were victims of privacy violations and unfair business practices wherein their privacy, financial interests, and security rights, were violated by Defendant Google, Inc., (hereinafter referred to as "Google" or "Defendant").

2. The Defendant gained unauthorized access to, and unauthorized use of, Plaintiffs' and class members' mobile devices used for communication over a cellular network which included the Android Operating System (hereinafter referred to collectively as "mobile

devices"). The Android Operating System (hereinafter "AOS") is an operating system for smartphones, netbooks and tablets which allowed Defendant to access, collect, monitor, and remotely store electronic data derived, in whole or in part, from the Mobile Devices traced to Plaintiffs and the class members' Unique Device Identifiers ((hereinafter referred to as "UDIDs"), a feature which could not be turned off even if Plaintiffs and the class members had utilized the so-called "privacy feature" of the system.

3. The nature of this action includes a sequence of events and consequences wherein Application Developers and Application Developers' Affiliates gained, individually and in concert with Defendant Google, unauthorized access to, transmittal of, and/or use of data, which included but was not limited to, Plaintiffs and the class members' UDIDs, obtained from Plaintiffs and the class members' mobile devices.

4. Google acted independently, and in concert with Application Developers and Application Developers' Affiliates, knowingly authorizing, directing, ratifying, acquiescing in, and/or participating in the conduct alleged herein.

5. The Defendant's business plan involved unauthorized access to, and disclosure of, Personal Information ("PI"), Personal Identifying Information ("PII"), Sensitive Identifying Information ("SII"), hereinafter referred collectively to as User's Personal Information ("UPI"), obtained from Plaintiffs and class members' mobile devices using their UDIDs provided by Defendant Google, to aggregate all Plaintiffs' and the class members' data including, but not limited to, users' mobile device activities which Defendant accomplished covertly, without notice and/or the consent of Plaintiffs or class members.

JURISDICTION AND VENUE

6. Venue is proper in this District pursuant to 28 U.S.C. §1391 (b) and (c) against Defendant. A substantial portion of the events and/or conduct giving rise to the violations of law complained of herein occurred in this District and Defendant conducts business with consumers in this District.

7. This court has Federal question jurisdiction as this complaint alleges violation of the following: (1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030; and (2) Electronic Communications Privacy Act 18 U.S.C. § 2510. Subject-matter jurisdiction also exists in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(c).

8. This is the judicial district wherein the basis of the conduct complained of herein involving the Defendant was devised, developed and implemented. The actual collection of information and data was activated from, and transmitted to and from this District.

PARTIES

9. Plaintiff, Joan Smith ("Smith") is a citizen and resident of Shelby County, Alabama (Shelby County, Alabama).

10. Plaintiff, Bryan Hicks ("Hicks") is a citizen and resident of Jackson County, Alabama (Jackson, County, Alabama).

11. Defendant Google, Inc., ("Google") is a Delaware corporation headquartered in California, during the class period, a privately owned corporation, which maintained its headquarters at 1600 Amphitheatre Parkway, Mountain View, Santa Clara County, California. Defendant Google does business throughout the United States.

A. Plaintiffs' Joan Smith and Bryan Hicks Experience

12. At all relevant times herein, Plaintiffs Smith and Hicks owned a mobile device, operated by the AOS, used that mobile device, and on one or more occasions during the class period accessed the Defendant Google's Android Market to download applications, which resulted in Defendant gaining unauthorized access to, and unauthorized use of Ms. Smith's and Mr. Hick's mobile device.

B. Sequence of Events and Consequences – Plaintiff and the class members

13. The sequence of events, and consequences common to Plaintiffs and the class members, made the basis of this action include, but are not limited to the following:

a) Plaintiffs and the class members are individuals in the United States who own and/or use mobile devices, operated by the AOS, and access the Google Android Market;

b) Google Application Developers are Application Developers who entered into a contract referenced as "Android Market Developer Distribution Agreement," with Defendant Google as a "Developer," a licensing agreement with Defendant Google to host a platform for Android user's access to Android applications;

c) Google Application Developer's Affiliates are Ad Networks and/or Web Analytic Vendors that are affiliated with authorized Google Application Developers, and entered into a licensing agreement with one or more of the Google Application Developers;

d) Plaintiffs and the class members accessed Defendant Google's Android Market by entered into a licensing agreement with one or more of the Google Application Developers, installed one or more Android applications associated with one or more of the Google Application Developers, during the class period;

e) Defendant Google then transmitted, and/or allowed access to, without notice and/or authorization, Plaintiffs and the class members' UDIDs, to one or more of the Google Application Developers which transmitted and/or allowed access of the UDIDs to Google Application Developer Affiliates;

f) Google Application Developers and its associated Google Application Developer Affiliates then took the liberty, without notice and/or authorization, with obtaining at will, mobile device data of Plaintiffs and the class members', using the mobile devices' UDIDs to aggregate the mobile device data;

g) Google Application Developers' Affiliates then created, individually and/or in concert with Google Application Developers, a database related to Plaintiffs and the class members' mobile device data, which also revealed web browsing activities, to assist Defendant's tracking scheme. Such tracking could not be detected, managed and/or deleted, and provided, in whole or part, the collective mechanism to track Plaintiffs and the class members, without notice, consent and/or authorization;

h) Defendant Application Developers' Affiliates and Google Application Developers then conducted systematic and continuous surveillance of Plaintiff and the class members' mobile devices activity, which continues to date;

i) Defendant Application Developers' Affiliates and Google Application Developers Affiliates then copied, used, and stored the mobile device UDID data derived from Plaintiffs and the class members' mobile devices, after knowingly accessing, without authorization, Plaintiffs and the class members' mobile devices;

j) Google Application Developers obtained Plaintiffs' and the class members' UPA, derived, in whole and/or part, from its monitoring the mobile application activities of Plaintiffs and the class members. The

personal information Defendant compiled, and misappropriated, includes details about Plaintiffs' and the class members' profiles to identify individual users to track them on an ongoing basis, across numerous applications, and tracking users when the accessed applications from different mobile devices, at home and at work. This sensitive information included but was not limited to such things as users' video application viewing choices to obtain personal characteristics such as gender, age, race, number of children, education level, geographic location, and household income, what the Plaintiffs and class members viewed and their buying propensities, reading habits and materials read, details about their personal finances, sexual preference, and even more specific information like health conditions;

k) Google Application Developers used Defendant Application Developer's analytics software to collect, use and disclose device data to third parties, an act that violates Plaintiffs and the class members' mobile device's agreement;

l) Defendant Google then provided assurances to Plaintiffs and the class members that any and all Android authorized applications were safe for downloading;

m) Defendant Google failed to notify and warn Plaintiffs and the class members of its covert activities, and the covert tracking activities of Google Application Developers and Application Developer's Affiliates before, during and after notice, of the unauthorized practices, made the basis of this action, so that Plaintiffs and the class members could take appropriate actions to opt-out of the unauthorized surveillance by Defendant, and/or delete any and all Defendant applications;

n) Defendant Google failed to block access to, and void the licensing agreements of Google Application Developers after it received notice of individual and concerted actions, made the basis of this action;

o) Defendant Google failed to provide any terms of service, or privacy policy, and related to its use of UDIDs for tracking, or provide an updated privacy policy alerting its users of Google Application Developers and Defendant Application activity, made the basis of these actions, thus Plaintiffs and the class members had no notice of such activities, nor the ability to mitigate their harm and damage after the fact;

p) Defendant Google Developers failed to provide any terms of service, or privacy policy, related to its used of UDIDs for tracking, or provide an updated privacy policy alerting its users of Google Application Developers and Defendant Application activity, made the basis of these actions, thus Plaintiffs and the class members had no notice of such activities, nor the ability to mitigate their harm and damage after the fact;

q) Defendant Google Application Developer's Affiliates then failed to provide notice to Plaintiffs and the class members of its tracking activities to obtain authorization, thus Plaintiffs and the class members had no notice of such activities, nor the ability to mitigate their harm and damage after the fact;

r) Defendant Google did not provide Plaintiffs and the class members information within its privacy policies concerning the affiliation of each Android Application Developer, it's Application Developer's Affiliates, and information related to the extent of its tracking, made the basis of this action, nor adequate opt-out information and;

s) Defendant converted Plaintiffs and the class members' electronic data, including but not limited to UDIDs.

14. Plaintiffs and the class members own the right to possess the personal property, including but not limited to, their personal data.

15. Plaintiffs and the class members' electronic data, misappropriated by Defendant, and populated with their actual user data constitute assets with discernable values.

16. Google Application Developer's Terms of Service and Privacy Policy do not reference that Android users' mobile devices' UDIDs shall be obtained for tracking purposes, provided to Application Developer Affiliates, and used to build a profile of data collected of any and all users' mobile device activities. Many application developers do not even provide any Terms of Service and/or Privacy Policies.

PRIVACY DOCUMENTS

17. Defendant Google does business online, using domains which include, but are not limited to: http://www.Google.com and its business includes internet search, cloud computing and advertising technologies including the "Android Market."

18. Defendant Google's document entitled, "Android Market Business and Program Policies," http://www.google.com/mobile/androidmarket-policies.html, fails to provide any reference to a "privacy policy."

19. Defendant Google's document, entitled, "Android Market Terms of Service," fails to reference its association with specific Defendant Application Developer's Affiliates, thus alleviating the possibility of its user opting–out of Defendant Application Developer's Affiliate's tracking.

20. Defendant Google's Terms of Service and Privacy Policy fail to provide notice, nor obtain consent from its users that their Mobile Devices' UDID shall be obtained and used for behavioral tracking.

FACTUAL ALLEGATIONS

A. Background

21. In 2008, Google released the Android Operating System which included unique software visible serial numbers, and permitting Advertising Networks and Web Analytic Vendors access to users mobile devices' Unique Device Identifiers ("UDIDs"), including but not limited to, device identifiers ("SSIDs") MAC address of the wireless access point, ("BSSID"), International Mobile Equipment Identifiers ("IMEI"), International Mobile Subscriber Identifiers ("IMSIs"). On October 22, 2008, Goggle's Android Market was launched as a service for the OS devices, and permitted users to download applications from the Google's Android Market. Recent studies though revealed that Google had transmitted, or allowed access to, user's UDIDs, without authorization, allowing Application Developers, and Application Developers Affiliates to obtain users' UDID for tracking users' mobile device activity.

B. Mobile Tracking

22. Mobile Internet advertising currently consists of streaming graphic files, in real time, into content rendered by a user's mobile device browser. Mobile advertising systems lack reliable browser tracking while traditional online advertising relies on the use of browser cookies, implementations inherent on conventional implementations of mobile ad serving have effectively prevented mobile advertising from being effective.

23. To obtain "uniqueness" in mobile devices, the key was to obtain Unique Device Identifiers or "UDIDs," a special type of identifier used in software applications to provide a unique reference number in mobile devices. Unlike traditional cookies, a user has no choice to disable the UDID. A user can't opt-out and/or delete it, since it is always sent as part of the person's smart phone activities. A user cannot block UDIDs being transmitted (as they would in a browser), since it is hard coded into a user's phone's software.

24. Tracking by use of UDIDs is not exactly comparable to any other type of tracking by advertising networks. It's not anonymous data – it's an exact ID unique to each physical device, and if merged with GPS data, provides unlimited advertising opportunities (i.e., commercial value). When tracking location data on a mobile device, it is calculated to 8 decimal points that can be far more exact and accurate than any sort of geographically-based IP address look-up on the web. Instead of getting a general location, location data on a GPS-enabled mobile can identify your precise latitude and longitude.

25. The advertising and marketing industries have been strongly advancing technical means for synchronizing tracking codes so information about individual consumer behavior in cyberspace can be shared between companies and the UDID used in the majority of mobile devices would be put to this purpose. The records of many different companies are merged without the user's knowledge and/or consent to provide an intrusive profile of activity on the computer. There are no practical limits on what can be collected or used.

26. Application Developer's Affiliates offer "free" software kits (hereinafter referred to as "SDKs"), that application developers download and insert into applications. A software development kit ("SDK") is typically a set a development tools which allow for the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar platform. It may be something as simple as an application programming interface (API) in the form of some files to interface to a particular programming language or include sophisticated hardware to communicate with a certain embedded system. Often SDKs can be downloaded directly via the Internet. Many SDKs are provided for free to encourage Application Developers to use the Application Developer Affiliates system and/or language.

27. SDKs though provided Application Developer Affiliates the access to Application users when Application Developers downloaded the Application Developer Affiliates' SDKs into its application; such provided the ability to obtain Plaintiffs and the class members' UDID and to conduct cross application tracking, activities made the basis of this action.

28. The SDKs also involve tracking libraries whose sole purpose is to collect and compile statistics on application uses and usage, and send the device ID as part of their functionality. These libraries are used to display advertisements so as to provide revenue for the application developer; and the mechanism for the libraries to also provide the mobile device's UDID once the user installed applications.

29. Application Developers Analytics reports are now available for mobile websites by simply pasting server-side code snippets (available for PHP, JSP, ASP, NET, and PERL) on each page they wish to track. Web Analytics vendors then create a profile for their mobile website where they can view the same kind of information that's in standard analytics reports including visitor information and traffic sources, including tracking users visiting their mobile websites from both high-end "smartphones" and WAP devices.

C. Android Market

30. The Android Market is an online software store developed by Google for Android devices. An application program ("app") called "Market" is preinstalled on most Android devices and allows users to browse and download apps developed by third-party developers, hosted on Android market. Users can also search for and read detailed information about apps from the Android market website.

31. Android devices can run applications written by third party developers and distributed through the Android Market or one of several applications available immediately, without a lengthy approval process. When an application is installed, the Android Market displays all required permissions. The user can then decide whether to install the application based on those permissions. The user may decide whether to install the application based on those permissions. The user may decide not to install an application whose permission requirements seem excessive or unnecessary. Possible app permissions include functionality such as:

- Accessing the internet
- Making phone calls

- Sending SMS messages
- Reading and writing to the installed memory card
- Accessing a user's address book data

32. The Android's Software Developer Kit provides the Defendant the ability to import the tracking code into Android apps to track Plaintiffs and the class members' activity on their mobile devices. The Android Software Development Kit License Agreement, Terms and Conditions provides assurances to Plaintiffs and the class members of Google's contractual obligation to protect the privacy and security of Android User:

- "You agree that if you use the SDK to develop applications for general public users, you will protect the privacy and legal rights of those users. If the users provide you with user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your application, and you must provide legally adequate privacy notice and protection for those users. If your application stores personal or sensitive information provided by users, it must do so securely. If the user provides your application with Google Account information, your application may only use that information to access the user's Google Account when, and for the limited purposes for which, the user has given you permission to do so."

33. The Android Operating System's "sandboxing mechanism", a technique to create a configured execution environment, attempts to limit access to other application's data, by preventing third party applications from seeing other or accessing specific locations; however, when Defendant combines the UDIDs and mobile device data derived from the sandboxing mechanism, such prevention serves no purpose.

34. Ad Networks and Web Analytics Vendors are associated with a multitude of Android applications and are thus able to cross-track user's mobile devices, accessing the ICCID (SIM card serial number) and the IMSI (International Mobile Subscriber Identity), making it possible to track users even when they change their device.

35. When Google requires Android apps to notify users before they download the app, of the data sources the app intends to access, Google does not require apps to ask permission to access some forms of the device ID, or to send it to outsiders. Possible sources

include the phone's camera, memory, contact list, and the like. When Smartphone users let an app see her location, apps generally fail to disclose if they will pass the location to ad companies, thus avoiding the Android manifest file.

36. Plaintiffs and the class members were provided assurances by Google that the Android Operating System's root directing shall protect them from exploits.

37. The Android Operating System thus is used to obfuscate the privacy and security settings of the user's mobile device, such as the application developer's ability to write code to get the MAC address of the phone. Multiple applications from that same developer can also send the same UDID to servers the developer runs, and Google's Android operating system doesn't provide controls to adequately protect users' sensitive data.

D. Google Controls All Facets of Android's Operating System

1. Android Operating System

38. The responsibility for complete user experience begins with a consumer's purchase of a mobile device which includes an Android Operating System, designed and manufactured by Google that works the way Google wants it to work. All device manufactures that are involved with the Android Market, all run Google's proprietary Android operating system software.

39. Since Defendant Google, Inc. launched its mobile device business, it has maintained control of how mobile devices that have its Android Operating System work, how consumers use them, and what happens when consumers use them – including functions that Google controls, hidden from consumers' sight, although Google claimed Android would be transparent and inclusive.

40. Google controls the process for the development software as well – such as by influencing developers to use Google's software development kit ("SDK"), and providing highly detailed guidelines for app development.

41. Google uses the mobile devices with Android operating systems, the Android Market, and the software development process to completely control the user experience by constructing the user's entire mobile computing environment.

42. Behind Google's wall of control, it designs the Android Operating System to be readily accessible to ad networks and we analytic vendors' consumers and access her personal information. These companies not only provide an important revenue source for app developers who provide "free" apps through the Android Market, they also furnish the analytic data that demonstrates Google's market leadership which it so often heralds in its quarterly investor conference calls. These companies, by helping finance third-party apps, gain access to consumers' mobile devices to collect personal information they use to track and profile consumers, such as consumers' cell phone numbers, address books, unique device identifiers, and geo-location histories – highly personal details about who they are, who they know, and where they are.

43. Since Google launched its mobile device business, it has sought to completely control the user experience by controlling all facets of the mobile environment and had differentiated itself in the marketplace by advertising that it provides its customers a tightly integrated user experience. With this control comes responsibility.

2. Google Controls Distribution of Apps for Android Devices

44. The mobile device enables a user to download apps that utilize an Android Operating System. Apps may only be obtained from Google's Android Market application and website. Google owns, controls, and operates the Android Market, which is launched on October 22, 2008.

45. Numerous apps available from the Android Market are created by third-party developers. There are several hundred thousand third-party apps available at the Android Market. Some of these are ostensibly free and some are sold for a fee. Google distributes approved free apps through the Android Market without charging the developer a fee. Google also distributes approved apps for which the consumer is charged a price set by the developer;

Google collects payment through its revenue collection mechanism and retains 30 percent of the payment as its fee.

46. Google claims it has no control of the Application Developers by not "vetting" the Android software applications for the devices, but then controls the only marketplace for Android apps – the Google Android Market. No third party app developer is also permitted to sell an app in the Android Market without entering into Google's form AOS Developer Agreement, but then Google fails to control the developers by failing to implement a system to obligate the developers to abide by the terms of this agreement.

47. Google represents to every user of the Android Market, pursuant to a click-through agreement required to create a user Android Market account, that users' are provided assurances that the Android Market will not permit apps that violate their prices: "Android Market Terms of Service", online: http://www.google.com/mobile/android/market-tos.html.

48. Google has also sought to exercised "indirect" control over what apps may be offered by the Android market. No developer is permitted to sell an app in the Android Market without entering into Google's forms AOS Developer Agreement. Google trades on its control of the Android Market, by implementing illusory contractual obligations in lieu of "vetting" the applications claiming to offer only apps that agree to its AOS Developer Agreement; however users rely on Google to allow only those found safe and appropriate.

49. Mobile Device users are only allowed to download software specifically licensed by Google and available through the Android Market. If a user installs any software which affects the "routing" of the Android Operating System, the users' warranty is voided.

50. Even after a user downloads an app, Google maintains control by requiring that the end-user license agreement for every third-party app include a clause giving Google the ability to step into the shoes of the app developer control's the user's use of apps. Specifically, the Android Developer distribution agreement, "Section 7.2, Google takedown Android Market Terms of Service" (last accessed April 26, 2011), online: http://www.google.com/mobile/android/market-tos.html.

3. Google Controls The Development Process for Apps Available on Android Devices

51. In addition to controlling the characteristics and distribution of apps, described above, Google exercises substantial control over its development and functionality.

52. The third party must also agree to the terms of Google's Developer Program License Agreement ("AOS Developer Agreement"). An App developed using Google's SDK will only function on Android Devices and can only interact with the Android Device operating system and features in the ways permitted by the Android Developer Agreement and SDK.

53. Google's control of the user experience includes restrictions, such as blocking consumers from modifying devices or installing non-Android Market Apps. As a direct consequence of the control exercised by Google, Plaintiffs and the class cannot reasonably review the privacy effects of apps and must rely on Google to fulfill its duty to do so. Google represents that it undertakes such a duty, representing that all apps available in its Android Market have agreed to Google's mobile policies, and that it retains broad discretion to remove an App from the Android Market.

54. A third party cannot upload an App for sale in the Android Market until Google enters into a licensing agreement with the App developer thereby giving its approval for sale of the App through the Android Market. Google represents that an app may not access information from, or about, the user stored on the user's Android Device unless the information is necessary for the advertising functioning of the App. Google represents that it does not allow an app to transmit data from a user's Android Device to other parties without the user's consent. Google though does not review its app source code, i.e. it does not review the code written by the developer in a programming language to inspect in order to determine if apps acquire users' personal information without the users' knowledge. Thus, Google's policy of not reviewing app's executable files permits apps that subject consumers to privacy exploits and security vulnerabilities to be offered in the Android Market. Contrary to Google's representations to

consumers, Google does not analyze the traffic generated by apps to detect apps that violate the privacy terms of the AOS Developer Agreement and Google's commitments to users.

55. Google provides additional assurances to users that their privacy and security interests are provided since it possesses an app "kill switch", maintaining the ability to "enter" a user's mobile device to remove apps, thus according to the Android Market's terms of service"

> "Google may discover a product that violates the developer distribution agreement . . . in such an instance; Google retains the right to remotely remove those applications from your device at its sole discretion."

56. Google recommends users should install only applications they trust and provides assurances to users that their privacy and security shall be protected since suspicious apps can be uninstalled at any time, but Google fails to address how users can make informed decisions about which apps are trustworthy and which are not; however knowing what an app is capable of is different than knowing what it actually does. There's no way of knowing what liberties apps on competing platforms take with users' personal information, since Google failed to adequately inform users that her mobile device's UDIDs would be provided to any party.

57. Google provides assurances when its terms of service and privacy policy state that Plaintiff and the class members are not at risk for privacy and security violations when using Android Devices, but fails to provide notice that the origin of mobile tracking by third parties originates with the third party's access to the user's UDIDs, which is provided by Google.

58. Plaintiffs in this action consider the information from and about themselves on their Mobile Devices to be personal and private information.

59. Because Defendant imposed an undisclosed cost on consumers, by taking more information than they were entitled to take, Defendant's practices imposed economic costs on consumers.

60. The scarcity of consumer information increases its value. The Defendant devalued consumers' information by taking and propagating it.

61. The undisclosed privacy and information transfer consequences of Defendant's practices imposed costs on consumers in the form of the loss of the opportunity to have entered into value-for-value exchanges with other app providers whose business practices better conformed to consumers' expectations. Likewise, Defendant's lack of disclosure coupled with his taking of information imposed costs on consumers who would otherwise have exercised her rights to utilize the economic value of her information by declining to exchange it with Defendant or any other app provider.

E. <u>"Bandwidth Hogs" - Economic Harm</u>

62. The Defendant's activities, made the basis of this action includes, but is not limited to, economic harm due to the unauthorized use of Plaintiffs' and class member's Bandwidth.

63. Bandwidth is the amount of data that can be transmitted across a channel in a set amount of time. Any transmission of information on the internet includes bandwidth. Similar to utility companies, such as power or water, the "pipeline" is a substantial capital expenditure, and bandwidth usage controls the pricing model. Hosting providers charge users for bandwidth because his upstream provider charges them and so forth until it reaches the "back bone providers". Retail providers purchase it from wholesalers to sell its consumers.

64. Network provider's data plans charge consumers based upon items such as usage and "caps", i.e. $30.00 per month for an unlimited plan is standard, but limited plans have caps, such as: 256 GB per month. Some national providers charge $1.00 per GB of bandwidth exceeding a certain cap. Whether the data plan is marketed as "unlimited" or "limited", the costs for the plans are allocated based upon the bandwidth usage, thus as the standard use of bandwidth increases, so too does the plan costs increase. Since plans are based upon user's average use, as consumer's usage increases collectively, costs increase for all users, while individual bandwidth overages can be costly.

65. Ads consume vast amounts of bandwidth, slowing a user's internet connection by using his bandwidth, in addition to diminishing the mobile device's "Battery Life", in order to retrieve advertisements. Web Analytics use up more bandwidth than ads, accessing bandwidth to download and run ad script, thus Plaintiffs and class members that did not access ads on an application still had the Defendant's Application Developer and Defendant Application Affiliate use his bandwidth.

66. Advertisers are now using the internet as their primary ad-delivery pipe, continually upcoming and downloading data from its networks causing substantial bandwidth use. Ads that were hidden in content, or bundled used substantial bandwidth, as did Application updates. Web analytics activities delayed movement on a site, users on a site, using his bandwidth, to complete its activities.

67. The Defendant's use of the Plaintiffs and class member's bandwidth for its data mining activities is similar in nature to a practice called "hot linking"; wherein one (1) server uses another server in its bandwidth to send data. While it slows down the server, it also allows bandwidth costs to be transferred to another server. Any redirect of a user's browsing capabilities to access or download Defendant's and/or data mining activities produces similar unauthorized bandwidth use. While only the tech Excluding the amount that the Plaintiffs and the class members use by her own activities, the Defendant's unauthorized data mining activities caused substantial bandwidth use to the Plaintiffs and the class members resulting in actual out of pocket expenditures, for Defendant's activities which include, but are not limited to the following:

a. Transmittal of and access to Plaintiffs and the class members UDIDs;
b. Loading of Ads first before content, building ads, and ads with excessive bandwidth;
c. Use of SDKs, and its functions within Plaintiffs and class member's mobile device;
d. "Harvesting" of Plaintiffs and class member's mobile device data;
e. "Background" Activities including "data mining".

F. Defendant's Harmful Business Practices

68. Defendant's business practice unfairly wrests control Defendant used and consumed the resources of Plaintiffs and the class members' mobile devices by gathering user information, adding such information to their mobile database, and transferring such to Defendant. Defendant caused harm and damages to Plaintiffs' and the class members' mobile devices finite resources, depleted and exhausted its memory, thus causing an actual inability to use it for its intended purposes, and significant unwanted CPU activity, usage, and network traffic, resulting in instability issues.

69. A milli-second was the time allotted for the Plaintiffs and the class members downloading a Defendant Google Android Market application, before Google Application Developers and Google Application Developer Affiliates intentionally, and without user's authorization and consent, had Defendant Google transmit, and/or allowed access to, data related to whole or part, from the Plaintiffs' and the class members' UDID. Such occurred without the benefit of being advised of the association between Defendant Application Developer and its Application Developer Affiliate, provided adequate time to access, read, and comprehend the Terms of Service/Use and Privacy Policy for Defendant. While only the most technical savvy mobile device users were familiar with UDIDs, a finite amount of individuals even knew about "UDID," let alone could possibly comprehend the technical aspects inherent within the Defendant's privacy documents.

70. Traditional online advertising does not obtain an UDID of user's mobile devices. The Defendant's objective was to obtain a mobile device's "Fingerprint," a practice of obtaining mobile device information to perpetually identify the mobile device as identification, which can then be linked to additional data elements to identify "personable identifiable information" ("PII"), personal information and/or sensitive information.

71. The collection, use and disclosure of tracking data, such as obtaining a users' UDIDs by Defendant to provide its services, implicates Plaintiffs' and the class members' privacy and physical safety. Such information is afforded special attention due to the

consequences for both privacy and physical safety that may flow from its disclosure. The heightened privacy and physical safety concerns generated by the collection, use and disclosure of location information are apparent in U.S. law that creates restrictive content standards for its use and disclosure in the private sector in the context of telecommunications services.

Allegations as to Class Certification

72. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a class action, on behalf of themselves and all others similarly situated as members of the following classes (collectively, the "class"):

> All persons residing in the United States who possessed a mobile device, operated by the Android Operating System, and downloaded an application from October 22, 2008 to the date of the filing of this complaint.

73. The class action period, (the "class period"), pertains to the dates, October 22, 2008 to the date of class certification.

74. On behalf of the U.S. Resident Class, Plaintiffs seek equitable relief, damages and injunctive relief pursuant to:

a. Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

b. Electronic Communications Privacy Act, 18 U.S.C. § 2510;

c. Breach of Contract;

d. Breach of Implied Covenant of Good Faith and Fair Dealing;

e. Conversion;

f. Negligence;

g. Trespass to Personal Property/Chattels; and

h. Unjust Enrichment.

75. **Persons Excluded From Classes:** Specifically excluded from the proposed class are Defendant, his officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint ventures, or entities controlled by Defendant, and his heirs, successors, assigns, or other persons or entities related to or affiliated

with Defendant and/or his officers and/or directors, or any of them; the Judge assigned to this action, and any member of the Judge's immediate family.

76. **Numerosity:** The members of the class are so numerous that their individual joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that the proposed class contains tens of thousands of members. The precise number of class members is unknown to Plaintiffs. The true number of class members is known by Defendant.

77. **Class Commonality:** Pursuant to Federal Rules of Civil Procedure, Rule 23(a)(2) and Rule 23(b)(3), are satisfied because there are questions of law and fact common to Plaintiffs and the class, which common questions predominate over any individual questions affecting only individual members, the common questions of law and factual questions include, but are not limited to:

a. What was the extent of Defendant's business practice of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs")?
b. What information did Defendant collect from its business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs"), and what did it do with that information?
c. Whether users, by virtue of them downloading the application, had pre-consented to the operation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs");
d. Was there adequate notice, or *any* notice, of the operation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") provided to Plaintiffs and the class members?
e. Was there reasonable opportunity to decline the operation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") provided to Plaintiffs and the class members?
f. Did Defendant's business practices of obtaining, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") disclose, intercept, and transmit personally identifying information, or sensitive identifying information, or personal information?
g. Whether Defendant devised and deployed a scheme or artifice to defraud or conceal from Plaintiffs and the class members Defendant's ability to, and practice of, intercepting, accessing, and manipulating, for its own

benefit, personal information, and tracking data from Plaintiffs' and the class members' personal mobile device via the ability to track their mobile device by tracking its UDID on their mobile device;

h. Whether Defendant engaged in deceptive acts and practices in connection with its undisclosed and systematic practice of transmitting, accessing and/or disclosing unique identifiers, tracking data, and personal information on Plaintiffs' and the class members' personal mobile device and using that data to track and profile Plaintiffs' and the class members' Internet activities and personal habits, proclivities, tendencies, and preferences for Defendant's use and benefit;

i. Did the implementation of Defendant's business practices of transmitting accessing, collecting, monitoring, and remotely storing users Unique Device Identifiers ("UDIDs") violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030?

j. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 2510?

k. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") involve a Breach of Contract?

l. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") involve a Breach of Implied Covenant of Good Faith and Fair Dealing?

m. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") involve a Conversion?

n. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") involve Negligence?

o. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") involve a Trespass to Personal Property/Chattels?

p. Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, and remotely storing users' Unique Device Identifiers ("UDIDs") result in Unjust Enrichment?

q. Is the Defendant liable under a theory of aiding and abetting others for violations of the statutes listed herein?

r. Is the Defendant liable under a theory of civil conspiracy for violations of the statutes listed herein?

s. Is the Defendant liable under a theory of unjust enrichment for violations of the statutes listed herein?

t. Whether Defendant participated in and/or committed or is responsible for violation of law(s) complained of herein?

u. Are class members entitled to damages as a result of the implementation of Defendant's marketing scheme, and, if so, what is the measure of those damages?

v. Whether Plaintiffs and members of the class have sustained damages as a result of Defendant's conduct, and, if so, what is the appropriate measure of damages?

w. Whether Plaintiffs and members of the class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

x. Whether Plaintiffs and members of the class are entitled to punitive damages, and, if so, in what amount?

78. **Typicality:** Plaintiffs' claims are typical of the claims of all the other members of the class, because their claims are based on the same legal and remedial theories as the claims of the class and arise from the same course of conduct by Defendant.

79. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of the members of the class. Plaintiffs have retained counsel experienced in complex consumer class action litigation. Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the class.

80. **Superiority:** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual class members is relatively small compared to the burden and expense that would be entailed by individual litigation of her claims against the Defendant. It would thus be virtually impossible for the class, on an individual basis, to obtain effective redress for the wrongs done to them.

81. In the alternative, the class may also be certified because:

a. the prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudication with respect to individual class members that would establish incompatible standards of conduct for the Defendant and/or;

b. the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other class members not

parties to the adjudications, or substantially impair or impede their ability to protect their interests.

82. Defendant has acted or refused to act on grounds generally applicable to the class thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the class as a whole.

First Cause of Action
Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030 *et seq.*

83. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

84. Plaintiffs assert this claim against each and every Defendant named herein in this Complaint on behalf of themselves and the class.

85. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA" regulates fraud and relates activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

86. Defendant violated 18 U.S.C. § 1030 by intentionally accessing Plaintiffs' and the class members' mobile computing device, without authorization by exceeding access, thereby obtaining information from such a protected device, causing the transmission to users' Android Devices, either by native installation or AOS upgrade of code that caused users' Android Devices to maintain, synchronize, and retain detailed, unencrypted location history files.

87. At all relevant times, Defendant engaged in business practices of transmitting code from within Plaintiffs' and the class members' downloaded Android Applications so as to access their mobile devices to obtain a UDID and mobile device data. Such acts were conducted without authorization and consent of the Plaintiffs and the class members.

88. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), provides a civil cause of action to "any person who suffers damage or loss by reason of a violation" of CFAA.

89. The Computer Fraud and Abuse Act, 18 U.S.C. § 103(a)(5)(A)(i), makes it unlawful to "knowingly cause[s] the transmission of a program, information, code or command and as a result of such conduct, intentionally cause[s] damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

90. Plaintiffs' and the class members' computers are a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

91. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing a Plaintiff's and the class members' mobile computer device, without authorization or by exceeding access, thereby obtaining information from such a protected mobile computing device.

92. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command embedded within his webpages, downloaded to Plaintiffs' and the class members' mobile computing device, which are protected mobile computing devices as defined in 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs' and the class members' viewing habits, Defendant intentionally caused damage without authorization to those Plaintiffs' and the class members' mobile computing devices by impairing the integrity of the computer.

93. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs' and the class members' protected mobile computing devices without authorization, and as a result of such conduct, recklessly caused damage to Plaintiffs' and the class members' mobile computing devices by impairing the integrity of data and/or system and/or information.

94. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing Plaintiffs' and the class members' protected mobile computing devices without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and the class members.

95. Plaintiffs and the class members have suffered damage by reason of these violations, as defined in 18 U.S.C. § 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

96. Plaintiffs and the class members have suffered loss by reason of these violations, as defined in 18 U.S.C. § 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its conditional prior to the offense, and any revenue lost, cost incurred or other consequential damages incurred because of interruption of service."

97. Plaintiffs and the class members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, disclosure of personal identifying information, sensitive identifying information, and personal information, interception, and transactional information that otherwise is private, confidential, and not of public record.

98. Defendant Google is jointly and severally liable for the violations of the Computer Fraud and Abuse Act alleged herein.

99. As a result of these takings, Defendant's conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

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

101. Defendant's unlawful access to Plaintiffs' and the class members' computers and electronic communications has caused Plaintiffs and the class members irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' and the class members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs and the class members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

Second Cause of Action
Violations of the Electronic Communications Privacy Act
18 U.S.C. § 2510
Against All Defendant

102. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

103. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the class.

104. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as "ECPA," regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

105. Defendant violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiffs' and the class members' electronic communications, without knowledge, consent or authorization.

106. At all relevant times, Defendant engaged in business practices of intercepting Plaintiffs and the class members' electronic communications which included endeavoring to intercept the transmission of a UDID from within her mobile device. Once the Defendant obtained the UDID they used such to aggregate mobile device data of the Plaintiffs and the class members as they used their mobile device, browsed the Internet, and activated downloaded Android applications.

107. The contents of data transmissions from and to Plaintiffs' and the class members' personal computers constitute "electronic communications" within the meaning of 18 U.S.C. § 2510.

108. Plaintiffs and the class member are "person[s] whose . . . electronic communication is intercepted . . . or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

109. Defendant violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiffs' and the class members' electronic communications.

110. Defendant violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing, or endeavoring to disclose, to any other person the contents of Plaintiffs' and the class members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and the class members' electronic communications.

111. Defendant violated 18 U.S.C. § 211(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiffs' and the class members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and the class members' electronic communications.

112. Defendant's intentional interception of these electronic communications without Plaintiffs' or class members' knowledge, consent, or authorization was undertaken without a facially valid order or certification.

113. Defendant intentionally used such electronic communications, with knowledge, or having reason to know, that the electronic communications were obtained through interception, for an unlawful purpose.

114. Defendant unlawfully accessed and used, and voluntarily disclosed the contents of the intercepted communications to enhance his profitability and revenue through advertising. This disclosure was not necessary for the operation of Defendant's system or to protect Defendant's rights or property.

115. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2520(a) provides a civil cause of action to "any person whose wire, oral, or oral electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

116. Defendant is liable directly and/or vicariously for this cause of action. Plaintiffs therefore seek remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of

that section to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fee and other litigation costs reasonably incurred.

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

118. Plaintiffs and the class, pursuant to 18 U.S.C. § 2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendant's profits obtained from the above-described violations. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' and the class members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs and the class members to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

Third Cause of Action
Breach of Contract
Against All Defendant

119. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

120. Plaintiffs and the class members entered into a contract with Defendant Google in order to use the Google Store apps. This contract had rights, obligations, and duties between Plaintiffs and the class members and Defendant Google, including but not limited to, protecting the privacy of its users.

121. Plaintiffs' and the class members' activities involved in their use of the Google App Store included, but was not limited to, providing personal identifying information to Defendant Google; furthermore Defendant Google designed Plaintiffs and the class members' mobile device data, including but not limited to, their mobile devices' UDID with third parties, including Google Application Developers and Defendant Application Developers Affiliates, on violation of its own contract with Plaintiffs and the class members.

122. Plaintiffs and the class members did not have notice, nor consent to, Defendant Google sharing his mobile devices UDID with Google Application Developers or Defendant Application Developers' Affiliates.

123. Plaintiffs and the class members have performed their obligation pursuant to Defendant Google's contract.

124. Defendant Google has materially breached its contractual obligations through its conduct.

125. Plaintiffs and the class members have been damaged as a direct and proximate result of Defendant Google's breach of its contract with Plaintiffs and the class members.

Fourth Cause of Action
Breach of Implied Covenant of Good Faith and Fair Dealing
Against All Defendant

126. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs in this complaint.

127. As set forth above, Plaintiffs and the class members submit personal information to Google and such information is stored on Plaintiffs' and the class members' Android Operating System, and Google promises in its Privacy Policy that it will not share this information with third-party advertisers or application developers without Plaintiffs' consent, and the consent of each class Member, respectively, and promises in its Android Market click-through agreement to protect users' privacy.

128. A covenant of good faith and fair dealing, which imposes upon each party to a contract a duty of good faith and fair dealing in its performance, is implied in every contract, including his agreement in the transactions for acquisitions of Android Operating System and apps that embodies the relationship between Goggle and its users.

129. Good faith and fair dealing is an element imposed by common law or statute as an element of every contract under the laws of every state. Under the covenant of good faith and fair dealing, both parties to a contract impliedly promise not to violate the spirit of the bargain

and not to intentionally do anything to injure the other party's right to receive the benefits of the contract.

130. Plaintiffs and the class members reasonably relied upon Google to act in good faith with regard to the contract and in the methods and manner in which it carries out the contract terms. Bad faith can violate the spirit of his agreements and may be overt or may consist of inaction. Google's inaction in failing to adequately notify Plaintiffs and the class members of the release of his personal information to the Google Application Developers, and by Defendant Application Developers Affiliates, depriving Plaintiffs and the class members of the means to discover their information was "leaked", thus evidencing bad faith and ill motive.

131. The contract is a form contract, the terms of which Plaintiffs are deemed to have accepted once Plaintiffs and the class members signed up with Google. The contract purports to give discretion to Google relating to Google's protection of users' privacy. Google is subject to an obligation to exercise that discretion in good faith. The covenant of good faith and fair dealing is breached when a party to a contract users discretion conferred by the contract to act dishonestly or to act outside of accepted commercial practices. Google breached its implied covenant of good faith and fair dealing by exercising bad faith in using its discretionary rights to deliberately, routinely, and systematically make Plaintiffs' and the class members' personal information available to third parties.

132. Plaintiffs and the class members' have performed all, or substantially all, of the obligations imposed on them under contract, whereas Google has acted in a manner as to evade the spirit of the contract, in particular by deliberately, routinely, and systematically without notifying Plaintiffs and the class members of its disclosure of Plaintiffs' and the class members' personal information to Defendant Affiliates, and by Defendant Developers. Such actions represent a fundamental wrong that is clearly beyond the reasonable expectation of the parties. Google's causing the disclosure of such information to the Defendant Affiliates, and by Defendant Developers is not in accordance with the reasonable expectations of the parties and evidences a dishonest motive.

133. Google's ill motive is further evidence by its failure to obtain Plaintiffs' and the class members' consent in data mining efforts while at the same time consciously and deliberately facilitating data mining efforts while at the same time consciously and deliberately facilitating data mining to automatically and without notice provide user information the Defendant Affiliates, and by Defendant Developers. Google profits from advertising revenues derived from its mining efforts from Plaintiff and the class.

134. The obligation imposed by the implied covenant of good faith and fair dealing is an obligation to refrain from opportunistic behavior. Google has breached the implied covenant of good faith and fair dealing in his agreement through its policies and practices as alleged herein. Plaintiffs and the class have sustained damages and seek a determination that the policies and procedures of Google are not consonant with Google's implied duties of good faith and fair dealing.

135. Google's capture, retention, and transfer through synchronization of uses' detailed location histories, even when such users had disabled GPS services on his Android Operating System, and storing such location histories in unencrypted form, was a breach of the implied covenant of good faith and fair dealing.

Fifth Cause of Action
Conversion
Against All Defendant

136. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

137. Plaintiffs and the class members' mobile device data, including but not limited to his mobile devices' UDID is being used by Defendant to obtain sensitive and personal identifying information derived from Plaintiffs' and the class members' mobile browsing activities. Such property, owned by the Plaintiffs and the class members, as valuable to the Plaintiffs and the class members.

138. Plaintiffs and the class members' mobile devices use bandwidth. Defendant's activities, made the basis of this action, used without notice or authorization, such bandwidth for purposes not contemplated, not agreed to, by Plaintiffs and the class members when they downloaded Defendant Application Developer's applications. Such property, owned by the Plaintiffs and the class members, is valuable to the Plaintiffs and the class members.

139. Defendant unlawfully exercised dominion over said property and thereby converted Plaintiffs' and the class members' property, by providing sensitive and personal identifying information to third parties and by using Plaintiffs and the class members' bandwidth for data mining, in violation of the collective allegations, made the basis of this action.

140. Plaintiffs and the class members were damaged thereby.

Sixth Cause of Action
Negligence
As to Defendant Google

141. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

142. As set forth above, Google owed a duty to Plaintiffs and the class members.

143. Google breached its duty by designing Android Operating System so that the Defendant Affiliates, and by Defendant Developers could acquire personal information without consumers' knowledge or permission, and by constructing and controlling consumers' user experience and mobile environment so that consumers could not reasonably avoid such privacy-affecting actions.

144. Google failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiffs' and the class members' personal information, privacy rights, and security.

145. Google's failure to fulfill its commitments included Google's practice of capturing frequent and detailed information about Android Operating System users' locations for up to one year, including the locations of Android Operating System users who had utilized Google's

prescribed functioning for disabling Global Positioning System services, maintaining records of such location histories on users' Android Operating System, transferring such location history files to users' replacement android Operating System, transferring such location history files to other computers with which users synchronized her Android Operating System, and storing such location history files in accessible, unencrypted form, without providing notice to users or obtaining users' consent, and where such practice placed users at unreasonable risk of capture and misuse of such highly detailed and personal information, and where a reasonable consumer would consider such a practice unexpected, objectionable, and shocking to the conscience of a reasonable person.

146. Google's unencrypted storage on Android Operating System and computers with which they were synchronized the information described above was negligent.

147. Plaintiffs and the class members were harmed as a result of Google's breaches of its duty, and Google proximately caused such harms.

Seventh Cause of Action
Trespass to Personal Property/Chattels
Against All Defendant

148. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

149. The common law prohibits the intentional intermeddling with personal property, including a mobile device, in possession of another which results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

150. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiffs and the class members, Defendant dispossessed Plaintiffs and the class members from use and/or access to her mobile devices, or parts of them. Further, these acts impaired the use, value, and qualify of Plaintiffs' and the class members' mobile device. Defendant's acts constituted an intentional interference with the use and enjoyment of their

mobile devices. By the acts described above, Defendant has repeatedly and persistently engaged in trespass to personal property in violation of the common law.

151. Without Plaintiffs and the class members' consent, or in excess of any consent given, Defendant knowingly and intentionally accessed Plaintiffs' and the class members' property, thereby intermeddling with Plaintiffs' and the class members' right to possession of the property and causing injury to Plaintiffs and the members of the class.

152. Defendant engaged in deception and concealment in order to gain access to Plaintiffs' and the class members' mobile devices.

153. Defendant undertook the following actions with respect to Plaintiffs' and the class members' mobile devices:

a) Defendant accessed and obtained control over the users' mobile device;
b) Defendant caused the installation of code on the hard devices of the mobile devices;
c) Defendant programmed the operation of its code to circumvent the mobile device owners privacy and security controls, to remain beyond his control, and to continue function and operate without notice to them or consent from Plaintiff and the class members;
d) Defendant obtained users' UDID from a tracking code on the users' mobile device; and
e) Defendant used the users' UDID to obtain without notice of consent, mobile browsing activities of the mobile device, and outside of the control of the owner of the mobile device.

154. All these acts described above were acts in excess of any authority any user granted when he or she visited the Defendant Google's Android Market and downloaded one (1) or more of the Defendant applications and none of these acts was in furtherance of users viewing the Defendant applications. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and the class members may have granted to Defendant Google and/or Google Application Developers was visited.

155. Defendant's installation and operation of its program used, interfered and/or intermeddled with Plaintiffs' and the class members' mobile devices. Such use, interference and/or intermeddling was without Plaintiffs' and the class members' consent or, in the alternative, in excess of Plaintiffs' and the class members' consent.

156. Defendant's installation and operation of its program constitutes trespass, nuisance, and an interference with Plaintiffs' and the class members' chattels, to wit, their mobile devices.

157. Defendant's installation and operation of its program impaired the condition and value of Plaintiffs' and the class members' mobile devices.

158. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and the class members.

159. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiffs' and the class members' property, Defendant has injured and impaired in the condition and value of class members' mobile devices, as follows:

a) By consuming the resources of and/or degrading the performance of Plaintiffs' and the class members' mobile devices (including space, memory, processing cycles, Internet connectivity, and unauthorized use of their bandwidth);
b) By diminishing the use of value, speed, capacity, and/or capabilities of Plaintiffs' and the class members' mobile devices;
c) By devaluing, interfering with, and/or diminishing Plaintiffs' and the class members' possessory interest in their mobile devices;
d) By altering and controlling the functioning of Plaintiffs' and the class members' mobile devices;
e) By infringing on Plaintiffs' and the class members' right to exclude other from their mobile devices;
f) By infringing on Plaintiffs' and the class members' right to determine, as owners of their mobile devices, which programs should be installed and operating on their mobile devices;
g) By compromising the integrity, security, and ownership of class members'

mobile devices; and

h) By forcing Plaintiffs and the class members to expend money, time, and resources in order to remove the program installed on their mobile devices without notice of consent.

Eighth Cause of Action
Unjust Enrichment
Against All Defendant

160. Plaintiffs hereby incorporate by reference the allegations contained in all of the paragraphs of this complaint.

161. By engaging in the conduct described in this Complaint, Defendant has knowingly obtained benefits from the Plaintiffs under circumstances that make it inequitable and unjust for Defendant to retain them.

162. Plaintiffs and the class have conferred a benefit upon the Defendant which have, directly or indirectly, received and retained personal information of Plaintiffs and the class members, as set forth herein. Defendant has received and retained information that is otherwise private, confidential, and not of public record, and/or have received revenue from the provision, use, and/or trafficking in the sale of such information.

163. Defendant appreciates and/or has knowledge of said benefit.

164. Under principles of equity and good conscience, the Defendant should not be permitted to retain the information and/or revenue that they acquired by virtue of his unlawful conduct. All funds, revenue, and benefits received by them rightfully belong to Plaintiffs and the class, which the Defendant has unjustly received as a result of his actions.

165. Plaintiffs and the class members have no adequate remedy at law.

166. Defendant has received a benefit from Plaintiffs and Defendant has received and retains money from advertisers and other third-parties as a result of sharing the personal

information of Defendant's users' with those advertisers without Plaintiffs' knowledge or consent as alleged in this Complaint.

167. Plaintiffs and the class members did not expect that Defendant would seek to gain commercial advantage from third-parties by using their personal information without their consent.

168. Defendant knowingly used Plaintiffs' and the class members' personal information without their knowledge or consent to gain commercial advantage from third-parties and had full knowledge of the benefits they have received from Plaintiffs and class members. If Plaintiffs and the class members had known Defendant was not keeping their personal information from third-parties, they would not have consented and Defendant would not have gained commercial advantage from third-parties.

169. Defendant will be unjustly enriched if Defendant is permitted to retain the money paid to them by third-parties, or resulting from the commercial advantage they gained, in exchange for Plaintiffs' and the class members' personal information.

170. Defendant should be required to provide restitution of all money obtained from his unlawful conduct.

171. Plaintiffs and the class members are entitled to an award of compensatory and punitive damages in an amount to be determined at trial or to be imposition of a constructive trust upon the wrongful revenues and/or profits obtained by and benefits conferred upon Defendant as a result of the wrongful actions as alleged in this complaint.

172. Plaintiffs and the class have no remedy at law to prevent Defendant from continued unjust retention of the money Defendant received from third-party advertisers.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendant as follows:

A. Certify this case as a class action on behalf of the classes defined above, appoint Plaintiffs as class representatives, and appoint their counsel as;

B. Declare that the actions of Defendant, as set out above, violate the claims;

C. Awarding injunctive and equitable relief including, *inter alia:* (i) prohibiting Defendant from engaging in the acts alleged above; (ii) requiring defendant to disgorge all of its ill-gotten gains to Plaintiffs and the other class members, or to whomever the Court deems appropriate; (iii) requiring Defendant to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Defendant to provide Plaintiffs and the other class members a means to easily and permanently decline any participation in any data collection activities; (v) awarding Plaintiffs and the class members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendant;

D. Award damages, including statutory damages where applicable, to Plaintiffs and the class members in an amount to be determined at trial;

E. Award restitution against Defendant for all money to which Plaintiffs and the classes are entitled in equity;

F. Restrain Defendant, his officers, agents, servants, employees, and attorneys, and those in active concert or participation with them from continued access, collection, and transmission of Plaintiffs' and the class members' personal information via preliminary and permanent injunction;

G. Award Plaintiffs and the classes:

a) Compensatory damages sustained by Plaintiffs and all others similarly situated as a result of Defendant's unlawful acts and conduct;
b) Restitution, disgorgement and/or other equitable relief as the Court deems proper;
c) Their reasonable litigation expenses and attorneys' fees;
d) Pre- and post-judgment interest, to the extent allowable;
e) Statutory damages, including punitive damages; and
f) Permanent injunction prohibiting Defendant from engaging in the conduct and practices complained of herein.

H. For such other and further relief s this Court may deem just and property.

JURY TRIAL DEMAND

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

DATED: August 6th, 2011

Respectfully Submitted,

/s/ E. Kirk Wood
E. Kirk Wood
Counsel for Plaintiffs

OF COUNSEL:

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

Joe R. Whatley, Jr.
Whatley, Drake & Kallas
2001 Park Place North, Suite 1000
Birmingham, Alabama 35203
(205) 328-9576
(205) 328-9669 facsimile
Email: jwhatley@wdklaw.com

REQUESTS FOR SERVICE BY CERTIFIED MAIL

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

By: /s/ Joe R. Whatley, Jr.
Joe R. Whatley, Jr.
Attorney for Plaintiffs

SERVE DEFENDANTS BY CERTIFIED MAIL AS FOLLOWS:

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043