

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

JON PESSANO,
NICHOLAS LAWRENCE, and
SID LAJZER,
on behalf of themselves and
all others similarly situated,

Plaintiffs,

v.

CASE NO.:

GOOGLE, INC.,

Class Action

Defendant,

**CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL
(Injunctive Relief and Damages Sought)**

Plaintiffs Jon Pessano, Nick Lawrence and Sid Lajzer, on behalf of themselves and others similarly situated, hereby bring this action against (1) Defendant Google, Inc.; (2) a defendant class of app makers represented by Pandora Media, Inc.; and (3) a second defendant class of electronic tracking/marketing companies represented by Defendants AdMob, Inc. and Traffic Marketplace, Inc., and allege as follows:

INTRODUCTION

1. This action asserts consumers' rights not to have their locations tracked, stored, and communicated to Google. Customers buying the newest gadgets want a product; they are not signing up to volunteer for free as mules for Google's efforts to build its individual location marketing database, which it uses to generate many billions of extra

revenue dollars. "Google Inc. Android smartphones regularly transmit their locations back to Google according to data and documents analyzed by The Wall Street Journal."¹ Although it does not make the actual smartphones, Google engineers the operating systems for many models of smartphones.² Through its operating systems, called Android operating systems, Google creates and stores individual user location data and transmits that data back to its own databases. According to security analysts Samy Kamkar and Ashkan Soltani, "an HTC model phone running the Android operating system collected its location *every few seconds* and transmitted the data to Google at least several times an hour." *Google Collects* (emphasis added). Google also "transmitted a unique phone identifier," even though it "previously has said that the data it collects is anonymous." Id. The unique phone identifier (UDID) can be readily used to identify the name of the phone's users.

2. Along with the UDID and location data, Defendants transmit other user information, including at least "age, gender, income, ethnicity, sexual orientation and political views" in addition to income and parental status.³ Further sources for data "include the phone's camera, memory, contact list, and more than 100 others." *Watching You*. All these data sources are "Sensitive Information" about users.

3. Fifty Google Android apps were tested by the Wall Street Journal to determine whether they transmitted data from six sources: username and password, contacts, age and gender, location, phone ID, and phone number.⁴ Of those tested, thirty-seven apps

¹ *Apple, Google Collect User Data*, by Julia Angwin and Jennifer Valentino-Devries, Wall Street Journal (WSJ), April 22, 2011 (hereafter *Google Collects*).

² To explain by analogy, Google provides the operating system on many smartphones like Microsoft provides the operating system on many computers.

³ *Your Apps are Watching You*, by Scott Thurm and Yukari Iwatani Kane, WSJ, Dec. 17, 2010 (*Watching You*).

⁴ Available at <http://blogs.wsj.com/wtk-mobile/> (last visited 5/9/2011).

transferred information that was not required for the functioning of the application. That is about 75% of the apps that transfer data that users do not expect to be transferred. And that test analyzed only six categories of information ó there are over 100 categories of information to which Google's Android operating system can provide app-makers access. Seven apps transmitted data directly to third parties. App-maker Defendant Pandora, which merely provides music to users, collected user location and phone ID and transferred data directly to third parties.

4. Like a user's location, which is available to anyone with certain commercially available software,⁵ unauthorized third-parties can easily access this additional Sensitive Information about users. According to the Mobile Marketing Association ó an industry trade group of which many Defendants are members ó "In the world of mobile, there is no anonymity." *Watching You*.

5. According to Defendant Traffic Marketplace, "The great thing about mobile is you can't clear a UDID. That's how we track everything." *Watching You* (quoting Meghan O'Holleran of Traffic Marketplace).

6. Google violates user privacy an effort to amass an unlawful database of individual location data unapproved by users, but worth billions of dollars in marketing money to Google and Defendants.

7. Google not only tracks, stores and transmits individual user location data for its own location marketing purposes, it also makes individual location data available to the

⁵ *Apple Inc.'s Response to Request for Information Regarding Its Privacy Policy and Location-Based Services*, letter from Apple's general counsel Bruce Sewell to U.S. Representatives Edward Markey and Joe Barton. July 12, 2010 (hereafter *Apple's Letter*), p. 6-9, 12. Available at <http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf>.

defendant class of third-party app-maker Defendants without providing any oversight whatsoever of those third-party applications.

8. A Google Android webpage apparently targeting an audience of programmers is titled "Location Services," in which Google explains to app developers:

Android gives your applications access to the location services supported by the device⁶ to determine location and bearing of the underlying device⁶. Your application is able to do three things:

- Query the list of all Location Providers for the last known user location.
- Register/unregister for periodic updates of the user's current location from a location provider (specified either by criteria or name).
- Register/unregister for a given Intent to be fired if the device comes within a given proximity (specified by radius in meters) of a given lat/long.⁶

9. Another Google webpage, titled "Obtaining User Location" explains to programmers that:

you can utilize GPS⁷ and Android's Network Location Provider to acquire the user location. Although GPS is most accurate, it only works outdoors, it quickly consumes battery power and doesn't return the location as quickly⁷. Android's Network Location Provider determines user location using cell tower and Wi-Fi signals, providing location information in a way that works indoors and outdoors⁷. To obtain the user location in your application, you can use both GPS and the Network Location Provider, or just one.⁸

10. Google and the app-maker Defendants both share with the second defendant class of third-party marketing Defendants⁹ led by AdMob and Traffic Marketplace⁹ the individual user location, and other data that they obtain without user consent or knowledge.

⁶ Available at <http://developer.android.com/guide/topics/location/index.html> (last visited 5/6/2011).

⁷ "GPS" is an abbreviation of "global positioning system," which uses satellites to determine location.

⁸ Available at <http://developer.android.com/guide/topics/location/obtaining-user-location.html> (5/6/2011).

Google Collects.

11. Users of Google's Android operating system have no way to prevent Google and the other Defendants from collecting their individual location data because even if users disable Android's global positioning system (GPS) components, Android's tracking system remains fully functional. Further, while an Android device's "location services" are toggled to "off," the device simply stores the user's location information for later transmittal to Google when the location services are toggled back to "on." Location services, which are "on" by default, are required for normal functioning of Android devices. Likewise, the apps collect and transmit data even when they are not in use. "It is nearly impossible to prevent cellphone[s] and apps from transmitting information about a phone and its owner." Thus, Android's location tracking is never "off;" rather, it can merely be postponed temporarily, at best.

PARTIES

12. Plaintiff Jon Pessano is a resident of Hillsborough County, Florida, who at all relevant times has owned a smartphone running Google's Android operating system and the relevant applications from Defendants, and has carried that phone with him everywhere.

13. Plaintiff Nicholas Lawrence is a resident of Texas state, who at all relevant times has owned a smartphone running Google's Android operating system and the relevant applications from Defendants, and has carried that phone with him everywhere.

14. Plaintiff Sid Lajzer is a resident of Texas state, who at all relevant times has owned a smartphone running Google's Android operating system and the relevant

⁹ *What Can You Do? Not Much*, by Jennifer Valentino-Devries, WSJ, Dec. 18, 2011.

applications from Defendants, and has carried that phone with him everywhere.

15. Defendant Google, Inc. is a Delaware corporation with its principal place of business in California.

16. Defendant Pandora Media, Inc. is a Delaware Corporation with its principal place of business in California.

17. Defendant AdMob, Inc. is a Delaware corporation with its principal place of business in California.

18. Defendant Traffic Marketplace, Inc. is a Delaware corporation with its principal place of business in California and is a subsidiary of Epic Media Group.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action under 28 U.S.C. § 1332(d)(2). The amount in controversy between the Class as defined herein and the Defendant exceeds \$5,000,000, exclusive of interest and costs. The Class as defined herein consists of individuals from fifty different states and countries around the globe. Greater than two-thirds of the Class members reside outside of Delaware and California ó the states in which Defendants are citizens.

20. Additionally, this Court has federal question jurisdiction under 28 U.S.C. § 1331 based on the federal civil causes of action provided in: 18 U.S.C. § 1030(g); 18 U.S.C. § 2520; 47 U.S.C. § 605(e)(3)(A); 18 U.S.C. § 2707; and 47 U.S.C. § 207.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 in that Plaintiff Jon Pessano is a resident of this district, many of the acts and transactions giving rise to this action occurred in this district, and because Defendants:

- a. are authorized to conduct business in this district and have availed themselves of the laws and markets within this district through the promotion, marketing, distribution and sale of their products in this district;
- b. do substantial business in this district; and
- c. are subject to personal jurisdiction in this district.

DEFENDANTS' PRIVACY VIOLATIONS

22. Android devices log, record and store users' locations based on latitude and longitude alongside a timestamp. Google, Pandora, AdMob, and Traffic Marketplace do this both domestically in the United States and internationally. The devices store this information in a file and transfer it to Google, the other Defendants and third parties of the Defendants' choosing. Defendants intentionally began recording this sensitive user information in 2008, when they began to accrue a marketing database worth billions of dollars.

23. Google uses a cell-tower triangulation to obtain user location. Alternatively, Google may use wireless hotspots or GPS data to obtain user location. Google and the other Defendants access and transmit the data created by Google.

24. Android devices download the user location data to the user's computer when the mobile device synchronizes (or syncs) or shares data with the computer.

25. Users of Android devices, including Plaintiffs, were unaware of Google's and Defendants' logging, recording and storing the latitude and longitude of their locations, alongside a timestamp, and did not consent to such tracking. Plaintiffs and users were also

unaware of Google's and Defendants accessing, collecting and transferring of other Sensitive user Information.

26. Google's Android "Privacy Policy"¹⁰ does not disclose its comprehensive tracking of users: "Google offers location-enabled services, such as Google Maps and Latitude. If you use those services, Google may receive information about your actual location." It does not explain the extent of Sensitive personal Information that Google and Defendants access. Further, it omits the fact that even if users do not utilize Google's location-based services, "such as Google Maps and Latitude," their location and other Sensitive Information will still be collected and shared with third-parties. Plaintiffs and other users did not provide any sort of informed consent to the tracking and information sharing at issue in this case. As Google uses it, the term "Privacy Policy" is an oxymoron.

27. The privacy policies of the other Defendants similarly fail to inform users of the Defendants' intentions to access, create and transmit user location data or other Sensitive Information.

28. Google and Defendants collect user location information and other user data covertly, surreptitiously and in violations of law.

29. Google tracks users' locations on its own, separate, apart and in addition to the information it collects in conjunction with other businesses that develop applications for Android devices. This action is specifically in objection to (1) Google's own collection of user location data and other Sensitive user Information, and the collection of the same data and information by (2) app-maker Defendants, and (3) marketing Defendants.

¹⁰ Available at <http://www.android.com/privacy.html>.

30. Android devices are carried with users to essentially every location they travel to, making the information collected by Defendants highly personal. Google's creation and collection, and enabling of third party collection of such data violates people's rights ó which they do not relinquish to Defendants through the ordinary purchase of a phone, or use of an app.

31. In addition to directly violating users' rights, the accessibility of the information collected by Google and Defendants places users at serious risk of privacy invasions and crimes. Even encrypted data is easily decipherable, making it important to collect no sensitive user information.

32. The individual location data is, or can be, readily combined by Defendant with each device's "unique device identification" (UDID), or equivalent, to identify particular users either by name or otherwise.

33. Defendants have a strong incentive to violate users' privacy. Databases such as the one Google began assembling in 2007 "could help them tap the \$2.9 billion market for location-based services ó expected to rise to \$8.3 billion in 2014, according to research firm Gartner Inc." ¹¹ Thus, Google and Defendants have billions of reasons annually not to allow users to disable the "location services," or other stop Defendants from collecting location data and Sensitive Information.

34. Plaintiffs and proposed Class members were harmed by Defendants' accrual of personal location, movement, travel histories and other Sensitive data because their personal devices were used in ways they did not approve, and because they were personally

¹¹ *Apple, Google Collect User Data*, by Julia Angwin and Jennifer Valentino-Devries, WSJ, April 22, 2011.

tracked just as if by a tracking device for which, in the U.S., a court-ordered warrant and probable cause would ordinarily be required.

35. Plaintiffs bring this action to stop Defendant's illegal and intrusive scheme of collecting, storing and selling personal location data and Sensitive Information.

36. Plaintiffs seek a court order requiring Defendants to stop unnecessarily creating, storing, accessing and transmitting individual user location data and other Sensitive Information, and in addition, requiring Google to begin expressly and succinctly disclosing to prospective users that Google intends to accumulate their individual location data, and access their sensitive information such as income, sexual orientation, ethnicity, camera phone, pictures and the like. Defendants' tracking and storing of user location data and other Sensitive Information is material and Defendants are legally bound to disclose their intentions *before* potential device users consummate their Android device purchases, and their application purchases or downloads.

37. Defendants concealed their intent to gather user location data and Sensitive Information, veiled their marketing motives ó albeit thinly ó to accumulate that data and sell billions of dollars' worth of ads. Plaintiffs therefore seek a further injunction requiring Defendants to, through a corrective media campaign, affirmatively and candidly inform the public and the millions of Android device users of the true and full extent of Defendants' tracking behavior. Full page advertisements in the major national and international newspapers would be a start.

38. Google's and the other Defendants' acts and omissions have directly and proximately caused Plaintiffs and Class members' damages and losses:

- a. Exposing their location data and Sensitive Information to unauthorized recipients;
- b. Shortening the battery life of their devices by drawing power for the unauthorized creation and accumulation of individual location data through communication with cell towers, wireless hotspots and GPS infrastructure;
- c. Requiring more frequent recharges of device batteries and the expenses associated therewith;
- d. Reducing the storage capability of their devices by covertly allocating limited device resources to create and store a database of individual user location information;
- e. Creating longer processing times for legitimate device uses because of resources drawn on by Defendants' location data activities;
- f. Causing an increase in data transfer expenses for users with limited data packages.

39. Plaintiffs seek damages for violations of their statutory and common law rights in one class of plaintiffs, based on federal statutes that the U.S. government customarily applies to domestic perpetrators who have acted on computers in the U.S. or abroad,¹² and on state-law rights, against Google and the two defendant Classes.

CLASS ACTION ALLEGATIONS

Plaintiff Class

¹² See e.g. <http://www.justice.gov/criminal/cybercrime/palaSent.pdf>.

40. Plaintiffs bring this action on behalf of themselves and proposed plaintiff Class members under Rules 23(b)(2) and (3) of the Federal Rules of Civil Procedure. The proposed plaintiff Class consists of:

All persons worldwide who purchased, owned or carried around a device with the Android operating system between the time of Google's release of the Android operating system and the present. Excluded from the Class are those who purchased the products for resale; and Defendant's officers, directors and employees.

41. While the exact number of plaintiff Class members is unknown to the Plaintiffs at this time, there are likely tens of millions of members of the proposed Class, as over 67 million Android devices were sold worldwide in 2010.¹³ The plaintiff Class is so numerous that joinder of all members of the Class is impracticable.

42. This action involves questions of fact common to all plaintiff Class members because all purchased, own or use Android devices under uniform "privacy policies."

43. This action involves questions of law common to all Class members because:

- a. The federal laws violated here are not only national in scope, but are also routinely applied to domestic perpetrators like Defendants who have acted on devices outside the United States;
- b. Each state has enacted laws comparable to the Federal Trade Commission Act, known as "little FTC" acts, which provide private causes of action with sufficient uniformity that Defendant's standardized practices of collecting location information violated the

¹³ See <http://www.betanews.com/joewilcox/article/Gartner-Android-smartphone-sales-surged-8888-in-2010/1297309933>.

little FTC acts of each state in the same way; and

- c. Defendants' privacy invasions have violated Plaintiffs' and Class members' other state statutory and common law rights in uniform ways.

44. The claims of Plaintiffs are typical of those of other members of the Class as there are no material differences in the facts and law underlying the claims of Plaintiffs and the Class, and by prosecuting their claims Plaintiffs will advance the claims of Class members.

45. The common questions of law and fact among all Class members predominate over any issues affecting individual members of the Class, including but not limited to:

- a. whether Google obtained, stored or transmitted Plaintiffs' location information;
- b. whether Google obtained other sensitive information of Plaintiffs;
- c. whether the app-maker Defendants obtained Plaintiffs' location data or other sensitive information;
- d. whether the marketing Defendants obtained Plaintiffs' location data or other sensitive information;
- e. whether Google;
- f. whether the app-maker Defendants failed to disclose material terms in their privacy policies regarding their collection of users' location data or sensitive information;

- g. whether Defendants have, do or intend to market or otherwise exploit users' location data or sensitive information;
- h. whether the alleged conduct constitutes violations of the laws asserted herein;
- i. whether Plaintiffs and Class members are entitled to declaratory and injunctive relief;
- j. whether Plaintiffs and Class members have sustained monetary loss and the proper measure of that loss;
- k. whether Plaintiffs and Class members have sustained consequential loss, and to what measure; and
- l. whether Defendants' acts and omissions warrant punitive damages.

46. The Plaintiffs' claims are typical of the claims of the proposed plaintiff Class, and those Plaintiffs will fairly and adequately represent and protect the interests of the proposed Class. Plaintiffs have retained counsel competent and experienced in the prosecution of this type of litigation.

47. The questions of law and fact common to the Class members, some of which are set out above, predominate over any questions affecting only individual Class members.

48. Class treatment of the claims set forth herein is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed Class members to prosecute their claims individually. Absent a class action, a multiplicity of individual lawsuits would be required to address the claims between Class members and

Defendants, and inconsistent treatment and adjudication of the claims would likely result.

49. The litigation and trial of Plaintiffs' claims is manageable. Defendants' standardized privacy policies, Google's uniform deployment of operating systems that track each user in identical ways, the consistent provisions of the relevant laws, and the readily ascertainable identities of many Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a plaintiffs class action. Additionally, notice can be sent directly to the Class through a software update, or similar, of the Android devices.

50. Google and the other Defendants have acted or refused to act on grounds that apply generally to the Class so that final injunctive relief and corresponding declaratory relief are appropriate.

51. Unless a class-wide injunction is issued, Defendants will continue to commit the violations alleged, and the members of the plaintiff Class will continue to be tracked, unlawfully surveilled, and potentially endangered.

App-Makers Defendant Class I¹⁴

52. Plaintiffs propose a defendant Class under Rules 23(b) of the Federal Rules of Civil Procedure, led by named app-maker Defendant Pandora Media. The proposed defendant Class consists of:

All makers of any application and employees thereof for Google's Android operating system, which application created, collected or transferred any user location data or other sensitive user information from 2008 to the present. Excluded from the Class are those makers and employees thereof

¹⁴ See *The Overlooked Utility of the Defendant Class Action*, by Francis Shen, U. Denver L. Rev, v.88, Feb. 12, 2011, p. 72-181 (providing a summary and analysis of defendant class actions). Available at http://law.du.edu/documents/denver-university-law-review/v88-1/Shen_FinalProof_21111.pdf.

of applications that transfer only the data reasonably expected by ordinary users as necessary to make the applications function, and that do not transfer that data to third parties.¹⁵

53. While the exact number of app-maker defendant Class members is unknown to the Plaintiffs at this time, there are over 100,000 Google Android Market apps.¹⁶ The app-maker defendant Class is so numerous that joinder of all members of the Class is impracticable.

54. This action involves questions of fact common to all app-maker defendant Class members because all designed and marketed applications that collect unexpected information from users ó information that users could not reasonably anticipate would be collected ó and all fail to disclose the full extent of their creation, accessing or transferring of user location data or other Sensitive Information. Like Google's Android privacy policy and Pandora's privacy policy, these app-makers' privacy policies, if they exist at all, are deficient and inadequate in that they omit descriptions of the true extent of information that will be collected from users' Android devices.

55. Further, all app-maker Defendants were, and continue to be, enabled by ó at least ó Google's provision of the technical requirements for accessing individual user location data and other sensitive information through Android devices, by Google's hands-off policy in checking the functioning and data collection of apps that it makes available to the public through its Android Market website, and by Google's facilitating relationships between the app-maker Defendants, that unlawfully collected and transferred user data, and

¹⁵ For example, a map app that collects only location data, only during app use, and does not share that data with third parties would be excluded from the class.

¹⁶ *Watching You*, supra, fn. 4. Most apps are made available directly by Google at <http://market.android.com>.

the marketing-company Defendants, that unlawfully received and used that data.

56. This action involves questions of law common to all app-maker defendant Class members because:

- a. The federal laws violated here are not only national in scope, but are also routinely applied to domestic perpetrators like Defendants who have acted on devices within and outside the United States;
- b. Each state has enacted laws comparable to the Federal Trade Commission Act, known as "little FTC" acts, which provide private causes of action with sufficient uniformity that Defendants' standardized practices of collecting location data and Sensitive Information violated the "little FTC" acts of each state in the same way; and
- c. App-maker Defendants' privacy invasions have violated Plaintiffs' other state statutory and common law rights in uniform ways.

57. The defenses of the named app-maker Defendant Pandora are typical of those of other members of the app-maker defendant Class as there are no material differences in the facts and law underlying the claims of Pandora and the defendant Class, and by defending itself, named Defendant Pandora will advance the defenses of app-maker defendant Class members.

58. The common questions of law and fact among all app-maker defendant Class members predominate over any issues affecting only named Defendant Pandora, including but not limited to:

- a. Whether app-maker Defendants' accessing of Plaintiffs' and plaintiff Class members' individual location data or other sensitive information was unlawful;
- b. whether app-maker Defendants obtained, stored or transmitted Plaintiffs' location information;
- c. whether app-maker Defendants obtained other Sensitive Information of Plaintiffs and plaintiff Class members;
- d. whether Google enabled app-maker Defendants unlawful access to information;
- e. whether the app-maker Defendants failed to disclose material terms in their privacy policies regarding their collection of users' location data or sensitive information;
- f. whether the alleged conduct constitutes violations of the laws asserted herein;
- g. whether Plaintiffs and Class members are entitled to declaratory and injunctive relief against app-maker Defendants; and
- h. whether app-maker Defendants' acts and omissions warrant punitive damages.

59. Defendant Pandora's defenses are typical of the defenses of the proposed app-maker defendant Class, and Pandora, in defending itself, will fairly and adequately represent and protect the interests of the proposed app-maker defendant Class. Pandora can retain counsel competent and experienced in the prosecution of this type of litigation.

60. The questions of law and fact common to the app-maker defendant Class members, some of which are set out above, predominate over any questions affecting only individual app-maker defendant Class members.

61. Class treatment of the claims set forth herein is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed plaintiff Class members to prosecute their claims individually against the makers of over 100,000 Android applications. Joinder of app-maker defendant Class members under Federal Rules of Civil Procedure 19, or 20 is impracticable. Absent a defendant class, a multiplicity of individual lawsuits would be required to address the claims between plaintiff Class members and members of the defendant Class, and inconsistent treatment and adjudication of the claims would likely result.

62. The litigation and trial of Plaintiffs' claims and the defendant Class' defenses is manageable. Defendants' standardized privacy policies, Google's uniform deployment of operating systems that track each user in identical ways, the app-maker defendants exceeding user authorization in uniform ways, the consistent provisions of the relevant laws, and the readily ascertainable identities of all app-maker defendant Class members demonstrate that there would be no significant manageability problems with Pandora defending this lawsuit as an app-maker defendant class action. Additionally, notice can be sent directly to all app-maker defendant Class members inexpensively through email by Google which already has each app maker's contact information.

63. Google, Pandora and the other app-maker Defendants have acted or refused

to act on grounds that apply generally to the Class so that final injunctive relief and corresponding declaratory relief are appropriate.

64. Unless a class-wide injunction is issued, Defendants will continue to commit the violations alleged, and the members of the plaintiff Class will continue to be tracked, unlawfully surveilled, and potentially endangered.

Marketing Defendant Class II

65. Plaintiffs propose a second defendant Class under Rules 23(b) of the Federal Rules of Civil Procedure, led by named marketing Defendants AdMob and Traffic Marketplace. The proposed second defendant Class consists of:

All marketing companies and employees thereof who have received individual location data or other sensitive information from Google's Android operating system from 2008 to the present. Excluded from the Class are those makers and employees thereof of applications that transfer only the data reasonably expected by ordinary users as necessary to make the applications function, and do not transfer that data to third parties.¹⁷

66. While the exact number of marketing defendant Class members is unknown to the Plaintiffs at this time, there are over fifty companies within the definition of the Class. The marketer-defendant Class is so numerous that joinder of all members of the Class is impracticable.

67. This action involves questions of fact common to all marketer-defendant Class members because all received unauthorized data and Sensitive user Information from Google and the app-makers. These marketing Defendants never attempted to disclose to users their receipt of user data in Sensitive Information. Like Google's Android privacy

¹⁷ For example, a map app that collects only location data, only during app use, and does not share that data with third parties would be excluded from the class.

policy and Pandora's privacy policy, these marketing Defendants' privacy policies, if they exist at all, are deficient and inadequate in that they omit descriptions of the true extent of information that they will receive from users' Android devices.

68. Further, all marketing Defendants were, and continue to be, enabled by Google at least Google's provision of the technical requirements for accessing individual user location data and other Sensitive Information through Android devices, by Google's hands-off policy in checking the functioning and data collection of apps that it makes available to the public through its Android Market website, and by Google's facilitating relationships between the app-maker Defendants, that unlawfully collected and transferred user data, and the marketing-company Defendants, that unlawfully received and used that data.

69. This action involves questions of law common to all marketing-defendant Class members because:

- a. The federal laws violated here are not only national in scope, but are also routinely applied to domestic perpetrators like Defendants who have received transmission either directly or indirectly from devices within and outside the United States;
- b. Each state has enacted laws comparable to the Federal Trade Commission Act, known as "little FTC" acts, which provide private causes of action with sufficient uniformity that Defendants' standardized practices of receiving location data and Sensitive Information violated the "little FTC" acts of each state in the same way; and

- c. Marketing Defendants' privacy invasions have violated Plaintiffs' other state statutory and common law rights in uniform ways.

70. The defenses of the named marketing Defendants AdMob and Traffic Marketplace are typical of those of other members of the marketer-defendant Class as there are no material differences in the facts and law underlying the claims of AdMob and Traffic Marketplace and the marketer-defendant Class at large, and by defending themselves, named Defendants will advance the defenses of marketer-defendant Class members.

71. The common questions of law and fact among all marketer-defendant Class members predominate over any issues affecting only named Defendants AdMob and Traffic Marketplace, including but not limited to:

- a. Whether marketing Defendants receipt of Plaintiffs' and plaintiff Class members' individual location data or other Sensitive Information was unlawful;
- b. whether marketing Defendants obtained, stored or transmitted Plaintiffs' location information;
- c. whether marketing Defendants obtained other Sensitive Information of Plaintiffs and plaintiff Class members;
- d. whether Google and app-maker Defendants enabled marketing Defendants' unlawful access to information;
- e. whether the marketing Defendants unlawfully failed to disclose to Android users their collection of users' location data or Sensitive Information;

- f. whether the alleged conduct constitutes violations of the laws asserted herein;
- g. whether Plaintiffs and Class members are entitled to declaratory and injunctive relief against marketing Defendants; and
- h. whether Defendants' acts and omissions warrant punitive damages.

72. Defendants AdMob's and Traffic Marketplace's defenses are typical of the defenses of the proposed marketer defendant Class, and named Defendants, in defending themselves, will fairly and adequately represent and protect the interests of the proposed marketer-defendant Class. AdMob and Traffic Marketplace can retain counsel competent and experienced in the prosecution of this type of litigation.

73. The questions of law and fact common to the marketer-defendant Class members, some of which are set out above, predominate over any questions affecting only individual marketer-defendant Class members.

74. Class treatment of the claims set forth herein is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed plaintiff Class members to prosecute their claims individually against over fifty marketers, the names of most of which are known only by Google and app-maker Defendants. Joinder of marketer-defendant Class members under Federal Rules of Civil Procedure 19, or 20 is impracticable. Absent this defendant class, a multiplicity of individual lawsuits would be required to address the claims between plaintiff Class members and members of the defendant Class, and inconsistent treatment and adjudication of the claims would likely

result. Additionally, their receipt of individual location data and Sensitive Information from Google and the app-maker Defendants creates ample juridical connection between Plaintiffs and marketer-defendant Class members.

75. The litigation and trial of Plaintiffs' claims and the defendant Class' defenses is manageable. Defendants' standardized privacy policies, or absence thereof, Google's uniform deployment of operating systems that track each user in identical ways, the marketing defendants' unauthorized receipt of user location data and Sensitive Information, the consistent provisions of the relevant laws, and the readily ascertainable identities of all of the marketer-defendant Class members demonstrate that there would be no significant manageability problems with AdMob and Traffic Marketplace defending this lawsuit as marketer-defendant Class. Additionally, actual notice can be sent directly to all marketer-defendant Class members inexpensively through email by Google and app-maker Defendants, which already have each marketing defendant's contact information.

76. Google, AdMob, Traffic Marketplace and the other marketing Defendants have acted or refused to act on grounds that apply generally to the marketer-defendant Class so that final injunctive relief and corresponding declaratory relief are appropriate.

77. Unless a class-wide injunction is issued, Defendants will continue to commit the violations alleged, and the members of the plaintiff Class will continue to be tracked, impermissibly assailed with advertising on their phones, unlawfully surveilled, and potentially endangered.

78. Defendants' acts and omissions are the direct and proximate cause of damage as described in the following Counts:

COUNT I
(Injunction and Declaration)

79. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above as if fully set forth here.

80. Plaintiffs purchased, own, use and carry with them phones running Google's Android operating system and have done so at all times relevant to this action.

81. Plaintiffs relied on Google's "Privacy Policy," and where extant, the privacy policies of the other Defendants, which did not explain the pervasive location tracking and acquisition of Sensitive Information that Google and its co-defendants intended to undertake and did undertake.

82. Defendants knew that ordinary consumers acting reasonably would not understand the Google or other Defendants' privacy policies to include the location tracking, syncing, and acquisition of Sensitive Information at issue in this case.

83. Irreparable injury has resulted and continues to result from Defendants unauthorized tracking of millions of Americans and acquisition of their Sensitive Information. Once Plaintiffs began carrying their respective Android devices, Defendants began tracking their locations, and collecting and sharing their Sensitive Information. This has happened in the past and continues to happen all across the United States and around the world. It is unconscionable to allow Defendants to continue unlawfully and without proper consent tracking Plaintiffs and proposed Class members. If Defendants wanted to track the whereabouts of each of their products' users, they should have obtained specific, particularized informed consent such that Android consumers across America and around the world would not have been shocked and alarmed to learn recently of Defendants

practices.

84. Inadequate remedy at law exists because users of Defendants' products have no way to prevent Defendants from collecting this information because even if users disable the Android device GPS components, Defendants' tracking system remains fully functional.

85. Balance of the hardships favors Plaintiffs and the plaintiff Class because it is easier for Defendants to stop unlawfully tracking and storing the every move of users around the world, and their Sensitive Information, than it is for individual consumers to circumvent Defendants' sophisticated tracking programs. To require that Plaintiffs and the Class bear the consequences of Defendants' deceptive privacy policies, where extant, and unlawful acquisition of personal location data and Sensitive Information would be inequitable.

86. The public has an interest in being able to travel without being tracked, and without that data and their Sensitive Information being transmitted to third parties, either directly or indirectly. The public interest would not be disserved, and indeed would be advanced, by entering an injunction against Defendants. See eBay, Inc. v. MercExchange, LLC, 547 U.S. 388 (2006).

87. The injunction should require Google to reconfigure its software so that neither users' personal location data, nor their Sensitive Information, is collected, synced, or shared with other computers or third parties. In addition, the injunctive remedies sought above should be implemented and Defendants should be ordered to stop exploiting individual location data and Sensitive Information. Users have not agreed to volunteer as Defendants' data-gathering mules.

COUNT II
(Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

88. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

89. By secretly installing software that records users' every moves Defendants have accessed Plaintiffs' computers, in the course of interstate commerce, foreign commerce, or communication, in excess of the authorization provided by Plaintiffs as described in the Computer Fraud and Abuse Act (the "Fraud Act") 18 U.S.C. § 1030(a)(2)(C).

90. Plaintiffs' computers, and those of the plaintiff Class, are protected computers pursuant to 18 U.S.C. § 1030(e)(2)(B) because they were used in or affected interstate or foreign commerce or communication. Plaintiffs' computers were purchased in interstate or foreign commerce and have in turn facilitated additional purchases in interstate or foreign commerce.

91. Plaintiffs' smartphones running Google's Android operating system, are also protected computers pursuant to 18 U.S.C. § 1030(e)(2)(B) (stating that "the term 'protected computer' means a computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication").

92. By tracking individual location data, Defendants exceeded the scope of any authorized access provided by Plaintiffs. See 18 U.S.C. § 1030(e)(6).

93. Plaintiffs have suffered damages by the Defendants' impairment of the integrity of their privacy on their Android devices, by Defendants' creation of a database of Plaintiffs' location data, and other Sensitive Information, and by Defendants' transferring

that database or other protected user information to other computers and third parties. See 18 U.S.C. § 1030(e)(8).

94. Plaintiffs have suffered losses as a direct and proximate result of Defendants' acts and omissions as that term is defined by 18 U.S.C. § 1030(e)(11), including the cost of responding to Defendants' offenses, conducting damage assessments, and restoring the data, program, system, Sensitive Information and other information to its condition prior to the offense. Plaintiffs have also suffered consequential damages.

95. Defendants further violated the Fraud Act by causing the transmission of a program, information, code or command in (1) deploying the Android operating systems, (2) as a result of the syncing of user handheld devices with their laptop or desktop computers, and (3) by transferring user location data or Sensitive Information back to Google, other Defendants, and third parties and as a result caused harm aggregating at least \$5,000 in value. See 18 U.S.C. § 1030(c)(4)(i)(I).

96. By tracking individual user location data, accessing users' Sensitive Information, and by transmitting it to unauthorized third parties, Defendants' actions have threatened public safety and welfare. Collecting and storing information pertaining to an individual's routine movements makes that individual more susceptible to stalking and other crimes. A user's "[l]ocation" is available to anyone with certain commercially available software, says Apple. *Apple Letter* at 6, 7. Collecting user Sensitive Information without permission is unethical, immoral and illegal. Plaintiffs' risks of adverse action or even crime, and that of the proposed Class, have been increased by Defendants' actions, creating a threat to public safety. See 18 U.S.C. § 1030(c)(4)(i)(IV).

97. Plaintiffs and the Class have suffered damages, and those damages have affected ten or more protected computers over the past one-year period. See 18 U.S.C. § 1030(c)(4)(i)(VI).

98. Plaintiffs bring this Count as a stand-alone cause of action under 18 U.S.C. § 1030(g), and as a predicate violation for other Counts asserted in this complaint on behalf of the plaintiff Class.

99. The Defendants' actions were knowing or reckless and, as described above, caused harm to Plaintiffs and proposed plaintiff Class members.

100. Plaintiffs seek recovery for these damages and losses, and those of the plaintiff Class, as well as injunctive and declaratory relief to prevent future harm.

COUNT III
(Wire and Electronic Communications Interception, 18 U.S.C. § 2510 *et seq.*)

101. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

102. Google's and Defendants' programmed communication between its users' Devices and cell towers, wireless hotspots, and GPS infrastructure and between users' Android devices and Defendants' own computers is either "wire communication" under 18 U.S.C. § 2510(1) because wires are required between the point of origin and the point of reception, or, is "electronic communication" under 18 U.S.C. § 2510(12) because data is transmitted by wire, radio, electromagnetic, photo-electronic or photo-optical systems, or the like, that affect interstate commerce or foreign commerce.

103. Plaintiffs and plaintiff Class members are "users" under 18 U.S.C. § 2510(13).

104. Defendants' communications are "readily accessible to the general public"

under 18 U.S.C. § 2510(16), in that even though they are unauthorized by users, they are not sufficiently encrypted, and are transmitted among Defendants and to third parties without user consent. Someone inclined to do so, such as a divorce attorney, private eye, or rogue government agent, could easily assemble a user's location data and Sensitive Information as a direct result of Defendants' actions.

105. Defendants intentionally intercept Plaintiffs' and Class members' wire or electronic communications, and to unlawfully access the Sensitive Information stored on users' devices. See 18 U.S.C. § 2511(1)(a).

106. Defendants intentionally disclose or endeavor to disclose users' location data and other Sensitive Information, all of which is content of wire or electronic communication, through marketing networks and otherwise. See 18 U.S.C. § 2511(1)(c).

107. Defendants intentionally use, or endeavor to use, the contents of Google's location data tracking, and Sensitive Information of their users in violation of 18 U.S.C. § 2511(1)(d).

108. Defendants know or have reason to know that the personal location data and Sensitive Information they obtained from their users was obtained through the interception of a wire or electronic communication because Google wrote the programming code to accomplish this result and specifically explained to app-maker Defendants how to access this user information, and the app-maker Defendants did access it. See 18 U.S.C. § 2511(1).

109. Defendants have intentionally sent or carried in interstate commerce Android-equipped devices, which are electronic, mechanical or other devices and the relevant programming code for the Android operating system and other applications. See 18 U.S.C. §

2512(1)(a).

110. Although consumers employ these devices for other uses, Defendants' primary use for them is to harvest individual user location data to market or sell for billions of dollars annually via their marketing networks. Defendants manufacture, assemble, possess, and sell electronic, mechanical or other devices, knowing or having reason to know that the design of such devices renders them primarily useful for the purpose of the surreptitious interception of wire or electronic communications.

111. These devices have been sent through the mail or transported in interstate commerce. See 18 U.S.C. § 2512(1)(b).

112. Defendants have advertised the surreptitious interception capabilities of their devices and application, or information thereby obtained, by electronic means to third-parties interested in using the personal location information for marketing and other purposes. Defendants have known the content of these advertisements and known that they would be transported interstate.

113. Plaintiffs' and Class members' location data and Sensitive Information created or accessed, and collected by Defendants was intentionally used or disclosed by Defendants to third parties for marketing purposes. See 18 U.S.C. § 2520(a).

114. Plaintiffs seek injunctive and declaratory relief to stop Defendants from creating or accessing, and collecting their personal location data and Sensitive Information.

115. Plaintiffs seek damages under 18 U.S.C. § 2520(c)(2).

116. Plaintiffs seek a reasonable attorney's fee and other litigation costs reasonably incurred.

117. Plaintiffs bring this Count as a stand-alone cause of action under 18 U.S.C. § 2520, and as a predicate violation for other Counts asserted in this complaint on behalf of the plaintiff Class.

COUNT IV
(Unlawful Access to Stored Communications, 18 U.S.C. § 2701)

118. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

119. Android devices and the applications thereon facilitate electronic communications services.

120. Defendants have knowingly and intentionally accessed, without authorization from users, the device facilities through which electronic communication services are provided.

121. Defendants have knowingly and intentionally exceeded their authorization to access users' devices, and have thereby obtained or altered a wire or electronic communication while it is in electronic storage on users' devices, on the computers with which users sync their devices, or other computers. Defendants have done this by creating, storing, and manipulating a database of Plaintiffs' location information without their authorization.

122. Plaintiffs did not authorize Defendants' conduct and are persons aggrieved by Defendants' violations, and bring this Count under 18 U.S.C. § 2707.

123. Plaintiffs seek an injunction to stop Defendants from continuing their violations.

124. Defendants' violations have directly and proximately damaged Plaintiffs and

Defendants have realized significant profits as a result of their violations.

125. Plaintiffs seek damages under 18 U.S.C. § 2707(c) of \$1000 or greater for each violation, where each plaintiff Class member is a person aggrieved and the quantity of each Defendant's violations equal the number of plaintiff Class members.

126. Plaintiffs seek reasonable attorney's fees and other litigation costs reasonably incurred.

127. Plaintiffs bring this Count as a stand-alone cause of action under 18 U.S.C. § 2701 *et seq.*, and as a predicate violation for other Counts asserted in this complaint on behalf of the plaintiff Class.

COUNT V
(Unauthorized Publication or Use of Communications, 47 U.S.C. § 605)

128. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

129. Defendants, through Android devices, willfully and purposefully received, assisted in receiving, transmitted, or assisted in transmitting interstate or foreign communication by wire or radio the individual location data it creates, stores, and shares or intended to share, of each device user.

130. Defendants have divulged or published the existence, contents, substance or effect of such user communications through unauthorized channels, including through individual location marketing.

131. Plaintiffs and Class members have proprietary rights in their location data and Sensitive Information that was intercepted by Defendants.

132. Defendants have collected and continue to collect Plaintiffs' location data and

Sensitive Information for their own private financial gain or commercial advantage.

133. Plaintiffs are aggrieved by Defendants' tracking of their location data, and acquisition of their Sensitive Information, and bring this Count under 47 U.S.C. § 605(e)(3)(A).

134. Plaintiffs seek an injunction to stop Defendants' interception of their location data and Sensitive Information.

135. Each Defendant's actions against each Plaintiff and each plaintiff Class member constitute separate violations.

136. Plaintiffs seek damages as calculated under 47 U.S.C. § 605(e)(3)(C) of \$1000 for each violation, up to \$100,000 for each violation because Defendants' actions were willfully and purposefully conducted for commercial advantage or private gain.

137. Plaintiffs seek reasonable attorney's fees and other litigation costs and expenses.

138. Plaintiffs bring this Count as a stand-alone cause of action under 47 U.S.C. § 605, and as a predicate violation for other Counts asserted in this complaint on behalf of the plaintiff Class.

COUNT VI
(Privacy of Customer Information, 47 U.S.C. § 222)

139. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

140. If Google is, because of its extensive telecommunications service activities, considered a telecommunications carrier under Title 47 of the U.S. Code, then its users are customers and Defendants have violated additional laws and regulations, including 47

U.S.C. § 222.

141. Plaintiffs' individual location data created and collected by Defendants is "customer proprietary network information."

142. Plaintiffs and Class members did not provide Defendants with express prior authorization for Defendants' individual location tracking activities, and acquisition of Sensitive Information, and did not approve the use of, disclosure of, or access to their call location information concerning their use of commercial mobile services.

143. Defendants have a duty to protect the confidentiality of proprietary information of and relating to customers, but have breached this duty by collecting, accessing, and sharing individual user location data and Sensitive Information.

144. Defendants' collection of this information was not part of their service to users and was instead part of Defendants' location-based marketing applications.

145. Under this Count, Plaintiffs seek damages, and attorneys' fees and costs. See 47 U.S.C. §§ 206, 207.

146. Plaintiffs bring this Count as a stand-alone cause of action under 47 U.S.C. § 222, and as a predicate violation for other Counts asserted in this complaint on behalf of the Class.

**COUNT VII
(Violations of State Computer Crimes Acts)**

147. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

148. "Computer" means an internally programmed, automatic device that performs data processing." Fla. Stat. § 815.03(3).

149. "access" means to approach, instruct, communicate with, store data, retrieve data, or otherwise make use of any resources of a computer. Fla. Stat. § 815.03(10).

150. "Whoever willfully, knowingly, and without authorization modified equipment or supplies used or intended to be used in a computer commits an offense." Fla. Stat. § 815.05. This is a felony in Florida.

151. "Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system or computer network which in whole or part, is owned by another commits an offense against computer users." Fla. Stat. § 815.06.

152. In Texas, "a person commits an offense if the person knowingly accesses a computer without the effective consent of the owner." Tex. Penal Code § 33.02(a). For an aggregate amount involved, as here, over \$200,000, the offense is a first-degree felony. Tex. Penal Code § 33.02(b), (c).

153. Plaintiffs' devices are "computers" within the definitions of both Florida and Texas law.

154. Defendants "accessed" Plaintiffs' devices without authorization. This constituted unlawful or unauthorized interception, use or disclosure under Florida and Texas law, respectively.

155. Plaintiffs and plaintiff Class members were directly and proximately damaged by Defendants in the amounts they paid for their devices and applications, and seek any other or additional damages afforded under these laws.¹⁸

**COUNT VIII
(Violations of State Wiretapping Laws)**

¹⁸ The relevant laws of each state are at <http://www.ncsl.org/default.aspx?tabid=13492> (last visited 5/9/2011).

156. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

157. Defendants intentionally intercepted or endeavor to intercept the wire or electronic communications of Plaintiff Jon Pessano by surreptitiously creating, recording and transmitting Plaintiff's individual location data and other Sensitive Information.

158. Plaintiff Pessano's individual location data and Sensitive Information is content of wire or electronic communications.

159. Defendants intentionally disclose or have endeavored to disclose Plaintiff's individual location data or Sensitive Information to other parties, including other Defendants, knowing or having reason to know that the information was obtained through the interception of a wire or electronic communication in violation of Fla. Stat. § 934.03.

160. Defendants intentionally use, or have endeavored to use, Plaintiff Pessano's individual location data or Sensitive Information for purposes unrelated to the provision of services that Plaintiff has authorized, and specifically for the purposes of creating a database to sell or market Plaintiff's location or Sensitive Information to third parties so that they can market to Plaintiff.

161. Similarly, under Texas law, Defendants have unlawfully engaged in intercepting or accessing Plaintiffs Sid Lajzer's and Nick Lawrence's electronic communication by creating, storing or transferring Plaintiffs' individual location data or Sensitive Information. See Tex. Penal Code § 16.02 *et seq.*

162. Defendants' creation, storage or transmission of individual location data is "electronic communication" under Texas law because it requires the transfer of signs,

signals, writing, images, data, or intelligence of any nature, and is transmitted in whole or part by wire, radio, electromagnetic, photo-electronic or photo-optical system. Tex. Penal Code § 16.02.

163. In Texas, knowingly or intentionally intercepting, disclosing, or using the contents of “wire, oral, or electronic communications,” is a second-degree felony. Tex. Penal Code § 16.02 *et seq.*

164. Defendants’ interception, disclosure, accessing or use of Plaintiffs’ individual location data has directly and proximately damaged Plaintiffs and Class members in the ways described throughout this complaint, and Plaintiffs and Class members have suffered losses as a result.

COUNT IX
(Unfair or Deceptive Acts Violating Each State’s “Little FTC” Acts)

165. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

166. This cause of action is brought by Plaintiff Jon Pessano pursuant to Florida’s Deceptive and Unfair Trade Practices Act, and by Plaintiffs Sid Lajzer and Nick Lawrence pursuant to Texas’s deceptive business practices laws. See Fla. Stat. § 501.201; see also Tex. Bus. & Com. Code §§ 17.41 *et seq.*

167. This Count is brought on behalf of U.S. Class members pursuant to each state’s unfair or deceptive acts and practices (UDAP) statutes, i.e. the “Little FTC” Acts (hereafter “Acts”). The Act of each state follows the Federal Trade Commission Act and provides for a private cause of action.

168. “Consumer” means “an individual” .ö Fla. Stat. § 501.203(7).

169. Plaintiffs and U.S. Class members are consumers as defined under these Acts.

170. The FTC Act prohibits an act or practice that violates either the standards for "unfairness," or those for "deception" or the two are independent of each other. An act or practice may be found to be unfair where it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). An act or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances.

171. Google's inadequate privacy policy disclosures were both unfair and deceptive, as were app-maker Defendants' privacy policies, or lack thereof.

172. Defendants' tracking of Plaintiffs' and other users' personal information was both unfair and deceptive because Android users had no knowledge of Defendants' intent or actions.

173. The Acts of Florida and the other states substantially follow the FTC Act.

174. Florida's Act defines a violation:

-Violation of this part means any violation of this act or the rules adopted under this act and may be based upon any of the following:

(a) Any rules promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. ss. 41 et seq.;

(b) The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts;

(c) Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices.¹⁹

175. Defendants' privacy policies contained deceptive misrepresentations that are

¹⁹ Fla. Stat. § 501.203(3).

material and are likely to and did deceive ordinary consumers acting reasonably, including the Plaintiffs, into believing that their every move would and Sensitive Information (1) not be tracked by Defendants, (2) then stored for future use in an marketing database, and (3) transmitted to Defendants so that (4) they could make billions of dollars in bonus revenue by selling ads. The Defendants without privacy policies are similarly liable to the plaintiff Class due to their consequent failure to describe how pervasively they intended to access and use, and did in fact access and use, Plaintiffs' location data and other Sensitive Information.

176. Defendants' omission of their true intent to track users was material to terms and conditions under which Plaintiffs and plaintiff Class members purchased their devices. An act or practice is material if it is likely to affect a consumer's decision regarding the product. Plaintiffs and other users would not have purchased Android devices and app-maker Defendants' products and indeed would have purchased the products of competitors had they known that their every movement would be tracked and recorded.

177. Here, Defendants with privacy policies specifically omitted from those policies any indication that their products would track users, knowing that such disclosure would prevent consumers from consummating their Android device purchases or app downloads. The other Defendants' lack of privacy policies constitutes similar omissions.

178. Florida's Act declares the acts and omissions of Defendants to be unlawful.

The statute says:

(1) Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.

(2) It is the intent of the Legislature that, in construing subsection (1), due consideration and great weight shall be given to the interpretations of the Federal

Trade Commission and the federal courts relating to s. 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. s. 45(a)(1) as of July 1, 2006.

Fla. Stat. § 501.204.

179. Defendants' practices have caused substantial injury to Plaintiffs and plaintiff Class members by depriving them of money they would have spent elsewhere and by covertly delivering software that tracks users' every movements, and transmits that data and their Sensitive Information to Google and Defendants.

180. Defendants' unfair omissions injure both consumers and competition. Consumers are injured in all the ways that Plaintiffs have been injured, as described throughout this complaint, and competition suffers in several ways too: (1) honest companies that do not covertly track their customers' locations or amass their Sensitive Information have lost and continue to lose market share to Android products and Defendants' applications as already described; (2) Defendants are rewarded for their deceit with billions of dollars in revenues (which should all be disgorged); and (3) competitors behaving deceptively creates a "race to the bottom," wherein additional companies feel economic pressure to similarly track users' whereabouts to later sell and thereby avoid losing further market share in the rapidly growing and competitive market for precise consumer demographic, location data and other Sensitive Information. There are no countervailing benefits of Defendants' conduct: not to consumers, nor to competition.

181. Defendants violated and continue to violate the Acts of each state by engaging in the trade practices described above, that have caused and continue to cause substantial injury to consumers, which are not reasonably avoidable by the consumers themselves, in transactions with Plaintiffs and the plaintiff Class which were intended to result in, and did

result in, the sale of the Android devices and Defendants' applications.

182. There were reasonable alternatives available to further Defendants' legitimate business interests, other than the conduct described herein. Defendants, for example, could have abstained from unnecessarily tracking the exact locations of users of its products. Google also could have required a single sentence disclosure describing its rampant covert tracking of individual users' locations to be signed by purchasers — rather than or in addition to its vague "privacy policy."

183. This cause of action is brought by Plaintiffs Sid Lajzer and Nick Lawrence pursuant to Texas' Deceptive Trade Practices — Consumer Protection Act. Tex. Bus. & Com. Code § 17.41 *et seq.*

184. Texas prohibits "[d]eceptive acts or practices in the conduct of any trade or commerce." Tex. Bus. & Com. Code § 17.46.

185. Defendants' acts of tracking users and acquiring their Sensitive Information was "consumer-oriented" because it preys on Android device purchasers, and downloaders of Defendants' apps as it preyed on Plaintiffs.

186. Defendants' act of tracking its users is misleading in a material way because Defendants fail to disclose, or even hint at, the full extent of their user location tracking and Sensitive Information acquisition in their respective privacy policies, if any. Defendants' acts have a broad impact on consumers at large because Defendants' inadequate disclosures, coupled with their unlawful tracking, storing and transmitting of user location data, continue to impact prospective purchasers.

187. Plaintiffs and plaintiff Class members have suffered injury as a result of

Defendants' deceptive acts and omissions because Plaintiffs would not have bought Android devices or Defendants' apps had they known that they would be tracked.

188. Plaintiffs have suffered injury as a direct and proximate result of Defendants' deceptive acts, practices and omissions. Injury includes Plaintiffs' purchases of their Android devices and Defendants' applications. Actual injury to Plaintiffs also includes the collection of their private location data and Sensitive Information and the continued existence of databases of that same information or databases that are and accessible to the third parties or the public.

189. Defendants willfully and knowingly violated Texas law and are therefore subject to three times the actual damages suffered by Plaintiffs and the plaintiff Class. See Tex. Bus. & Com. Code § 17.50.

190. Defendants deceived Plaintiffs and consumers, and treated them unfairly by tracking their movements as described above, and violated the Acts of each state by omitting from its privacy policy the full extent of its tracking:

- a. Alabama's Deceptive Trade Practices Act declares deceptive practices unlawful. Ala. Code §§ 8-19-1 *et seq.*;
- b. Alaska's Unfair Trade Practices and Consumer Protection Act. Alaska Stat. §§ 44.50.471 *et seq.*;
- c. Arizona's Consumer Fraud Act. Ariz. Rev. Stat. §§ 44-1521 *et seq.*;
- d. Arkansas's Deceptive Trade Practices Act prohibits "false, or deceptive acts or practices in business, commerce, or trade." Ark. Code §§ 4-88-101 *et seq.*;
- e. California's Consumer Legal Remedies Act, and also the Unfair Competition Law. Cal Civ. Code §§ 1750 *et seq.*, and Cal. Bus. & Prof. Code §§ 17200 *et seq.*, respectively;
- f. Colorado's Consumer Protection Act. Colo. Rev. Stat. §§ 6-1-101 *et*

seq.;

- g. Connecticut's Unfair Trade Practices Act. Conn. Gen. Stat. §§ 42-110a *et seq.*;
- h. Delaware's Consumer Fraud Act, and also its Uniform Deceptive Trade Practices Act. Del. Code, Title 6 §§ 2511-2571, 2580-2584, and Title 6 §§ 2531-2536, respectively;
- i. District of Columbia's Act. D.C. Code §§ 28-3901 *et seq.*;
- j. Florida's Deceptive and Unfair Trade Practices Act. Fla. Stat. §§ 501.201 *et seq.*;
- k. Georgia's Uniform Deceptive Trade Practices Act, and also the Fair Business Practices Act. Ga. Code §§ 10-1-370 *et seq.*, and §§ 10-1-390 *et seq.*;
- l. Hawaii's Uniform Deceptive Trade Practices Act. Haw. Rev. Stat. §§ 480-24 *et seq.*, §§ 484A-1 *et seq.*;
- m. Idaho's Consumer Protection Act. Idaho Code §§ 48-601 *et seq.*;
- n. Illinois's Consumer Fraud and Deceptive Business Practices Act, and also its Uniform Deceptive Trade Practices Act. 815 Ill. Comp. Stat. 505/1 *et seq.*, and 815 Ill. Comp. Stat. 510/1 *et seq.*;
- o. Indiana's Deceptive Consumer Sales Act. Ind. Code §§ 24-5-0.5-1 *et seq.*;
- p. Iowa's Act. Iowa Code §§ 714.16 *et seq.*;
- q. Kansas's Consumer Protection Act. Kan. Stat. §§ 50-623 *et seq.*, 50-676 *et seq.*;
- r. Louisiana's Unfair Trade Practices and Consumer Protection Law. La. Rev. Stat. §§ 51:1401 *et seq.*;
- s. Maine's Unfair Trade Practices Act, and also its Uniform Deceptive Trade Practices Act. Me. Rev. Stat., Title 5 §§ 205-A *et seq.*, and Title 10 §§ 1211 *et seq.*, respectively;
- t. Maryland's Consumer Protection Act. Md. Code Com. Law §§ 13-101 *et seq.*;
- u. Massachusetts's Consumer Protection Act. Mass. Gen. Laws ch.

93A §§ 1 *et seq.*;

- v. Michigan's Consumer Protection Act. Mich. Comp. Laws §§ 445.901 *et seq.*;
- w. Minnesota's Uniform Trade Practices Act, and its False Statement in Advertising Act, and also its Prevention of Consumer Fraud Act. Minn. Stat. §§ 8.31, 325D.43 *et seq.*, and §§325F.68 *et seq.*;
- x. Mississippi's Consumer Protection Act. Miss. Code §§ 75-24-1 *et seq.*;
- y. Missouri's Merchandising Practices Act. Mo. Rev. Stat. §§ 407.010 *et seq.*;
- z. Montana's Unfair Trade Practices and Consumer Protection Act. Mont. Code §§ 30-14-101 *et seq.*;
- aa. Nebraska's Consumer Protection Act, and also its Uniform Deceptive Trade Practices Act. Neb. Rev. Stat. §§ 59-1601 *et seq.*, and §§ 87-301 *et seq.*;
- bb. Nevada's Trade Regulation and Practices Act. Nev. Rev. Stat. §§ 598.0903 *et seq.*, and § 41.6000;
- cc. New Hampshire's Consumer Protection Act. N.H. Rev. Stat. §§ 358-A:1 *et seq.*;
- dd. New Jersey's Consumer Fraud Act. N.J. Stat. §§ 56:8-1 *et seq.*;
- ee. New Mexico's Unfair Practices Act. N.M. Stat. §§ 57-12-1 *et seq.*;
- ff. New York's Act. N.Y. Exec. Law § 63(12), N.Y. Gen. Bus. Law §§ 349 *et seq.*;
- gg. North Carolina's Act. N.C. Gen. Stat. §§ 75-1.1 *et seq.*;
- hh. North Dakota's Consumer Fraud Act. N.D. Cent. Code §§ 51-15-01 *et seq.*;
- ii. Ohio's Consumer Sales Practices Act, and also its Deceptive Trade Practices Act. Ohio Rev. Code §§ 1345.01 *et seq.*, and §§ 4165.01 *et seq.*;
- jj. Oklahoma's Consumer Protection Act, and also its Deceptive Trade Practices Act. Okla. Stat., Title 15 §§ 751 *et seq.*, Title 78 §§ 51 *et*

seq., respectively;

- kk. Oregon's Unlawful Trade Practices Law. Or. Rev. Stat. §§ 646.605 *et seq.*;
- ll. Pennsylvania's Unfair Trade Practices and Consumer Protection Law. 73 Pa. Stat. §§ 201-1 *et seq.*;
- mm. Rhode Island's Unfair Trade Practices and Consumer Protection Act. R.I. Gen Laws §§ 6-13.1-1 *et seq.*;
- nn. South Carolina's Unfair Trade Practices Act. S.C. Code §§ 39-5-10 *et seq.*;
- oo. South Dakota's Deceptive Trade Practices and Consumer Protection Law. S.D. Cod. Laws §§ 37-24-1 *et seq.*;
- pp. Tennessee's Consumer Protection Act. Tenn. Code §§ 47-18-101 *et seq.*;
- qq. Texas's Deceptive Trade Practices and Consumer Protection Act. Tex. Bus. & Com. Code §§ 17.41 *et seq.*;
- rr. Utah's Unfair Practices Act, and its Consumer Sales Practices Act, and also its Truth in Advertising Act. Utah Code §§ 13-2-1 *et seq.*, 13-5-1 *et seq.*, and §§ 13-11-1 *et seq.*, and also §§ 13-11a-1 *et seq.*, respectively;
- ss. Vermont's Consumer Fraud Act. Vt. Stat., Title 9 §§ 2451 *et seq.*;
- tt. Virginia's Consumer Protection Act. Va. Code §§ 59.1-196 *et seq.*;
- uu. Washington's Consumer Protection Act. Wash. Rev. Code §§ 19.86.010 *et seq.*;
- vv. West Virginia's Consumer Credit and Protection Act. W. Va. Code §§ 46A-6-101 *et seq.*;
- ww. Wisconsin's Deceptive Trade Practices Act. Wis. Stat. §§ 100.18 *et seq.*;
- xx. Wyoming's Consumer Protection Act. Wyo. Stat. §§ 40-12-101 *et seq.*; and
- yy. the equivalent and applicable laws in the other remaining U.S. territories.

191. Defendants are liable for attorney's fees and reasonable costs pursuant to Fla. Stat. § 501.2105, and Tex. Bus. & Com. Code § 17.50, the comparable statutes of the other states, as described above, if Plaintiffs and plaintiff Class members prevail.

192. Plaintiffs also seek punitive damages.

193. Plaintiffs seek a declaratory judgment under the relevant statutes, including Fla. Stat. § 501.2105.

194. Violations of the relevant computer laws, both federal and state, serve as additional predicates for violations of these UDAP laws.

195. Plaintiffs and the plaintiff Class reserve the right to allege other violations of law which constitute other unlawful business acts or practices. Such conduct is ongoing and continues to this date.

COUNT X
(Fraudulent, Intentional Misrepresentation)

196. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

197. Google and Defendants represented to Plaintiffs and plaintiff Class members that it would not collect information about their every movement and location, or their Sensitive Information, and omitted disclosing otherwise to Plaintiffs. See Essex Ins. Co. v Universal Entertainment & Skating Center, Inc., 665 So. 2d 360 (Fla. 5th DCA 1995) (discussing fraud generally).

198. Google not only knew that its privacy terms and conditions policy was, and continues to be, false, deceptive and untrue, by omitting that Google will track users or access their Sensitive Information, but Google also intended for Plaintiffs and plaintiff Class

members to rely on its deceptive or omitted statements.

199. Defendants similarly intended for Plaintiffs to rely on their omissions of the same information that Google's privacy policy omitted.

200. Defendants' fraud is comprised both by the omissions of proper disclosures to users and by their illegal tracking of user movements or accessing Sensitive user Information.

201. Plaintiffs and Class members did not know about Defendants' omissions, assuming quite naturally that their information would not be unlawfully accessed or transmitted by Defendants.

202. Plaintiffs and Class members did not know that Google and Defendants have been tracking their movements, and accessing their Sensitive Information.

203. Plaintiffs and Class members, acting as ordinary consumers, reasonably relied on Defendants' omissions and representations. Plaintiffs had a right to rely on Defendants' representations. Plaintiffs' and Class members' reliance on Defendants' omissions was a substantial factor in causing their harm. Defendants' tracking of users was and is material, as is accessing and transmitting Plaintiffs' Sensitive Information, and Plaintiffs and Class members reasonably believed that their every movements would not be tracked and that their information would not be unlawfully accessed.

204. Plaintiffs and Class members were damaged in the amount of money required to purchase Android products, and those of app-maker Defendants, because they would have purchased other products had they been aware of the material fact that Defendants intended to and did in fact track their users' locations, and obtain users' Sensitive Information.

205. Plaintiffs and the Class seek punitive damages from Defendants.

206. Defendants had and continue to have a duty of good faith, which implicitly includes a duty not to deceive consumers, and also not to conduct this sort of covert digital surveillance on consumers. And they certainly have a duty not to stalk consumers or to facilitate others doing that. But that is exactly what Defendants have done and continue to do.

207. To remedy Defendants' intentional omission to consumers, and omission of clarifying statements during the sales process, Plaintiffs and Class members seek to rescind their contracts, and thereby disgorge all monies paid to Defendants for these products. Plaintiffs also seek all other damages sought in this complaint.

COUNT XI
(Negligent Misrepresentation)

208. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

209. Defendants omitted material facts ó that users would be tracked at all times and their Sensitive Information accessed ó during their sale of Android devices and Defendants' applications to consumers.

210. Google and Defendants were negligent in making the omissions because they should have known that whether their every movements would be tracked, recorded and stored for later use was material to consumers, as is the Defendants' accessing of their Sensitive Information.

211. Defendants, in making their omission intended, or expected, that Plaintiffs and Class members would rely on the omissions.

212. Plaintiffs justifiably relied on Defendants' omissions about their tracking of purchasers, and would not have purchased Android devices or Defendants' applications but for the omissions.

213. Plaintiffs were damaged in amounts equal to the prices they paid for Android devices and products.

214. Defendants' omissions were material and directly and proximately caused ordinary consumers acting reasonably, Plaintiffs and Class members included, to buy the Android devices and Defendants' applications. Without Defendants' omissions of the material fact that users' location data would be collected, the products would not have been purchased, and Plaintiffs would not have suffered damages.

215. Plaintiffs seek punitive damages from Defendants.

COUNT XII
(Unjust Enrichment, Money Had and Received)

216. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

217. Unjust enrichment results from a transfer that is ineffective to conclusively alter ownership rights.²⁰ Here, Defendants' omissions made Plaintiffs and Class members believe that a term material to the contract was different than it actually was. Defendants intended to track its users, storing their location data and Sensitive Information and transferring that data back to themselves to build databases to sell billions of dollars in location-based advertisements. Plaintiffs did not agree to be Defendants' mules or they did not agree to be tracked, nor to collect data for Defendants, nor to allow Defendants access to

²⁰ See Restatement, Third, of Restitution and Unjust Enrichment, § 1, comment b (Discussion Draft 2000).

their Sensitive Information. Morally and ethically and therefore, in equity Defendants have gained a benefit for which they have not exchanged consideration. Defendants promised products capable of certain tasks, but instead, like the Trojan Horse, delivered products to spy on Plaintiffs and Class members and to sell their personal location information at a future date. This constitutes at least a partial failure of consideration.

218. Defendants, through the omission of their true intentions, cultivated in consumers a mistake of fact that would not have existed but for Defendants' omissions.

219. Because of Defendants' omissions, Plaintiffs and Class members conveyed a benefit to Defendants by purchasing their products and applications, and then having their subsequent movements tracked, stored and transmitted, along with their Sensitive Information, to Defendants. Defendants appreciated the benefit conferred on it by Plaintiffs through these transactions because Google was enriched in the amount Plaintiffs paid for the devices, and the app-maker Defendants by the amounts paid for the apps, and also in the amounts received by Defendants from selling ads based on access to Class members' individual location data or other Sensitive Information.

220. Defendants were enriched through their unlawful acquisition of user location data from Plaintiffs and the Class, whether or not Defendants have yet realized pecuniary proceeds from the sale of this information.

221. Plaintiffs have no adequate remedy at law due to the difficulty of quantifying losses and damages caused by being tracked, and having their Sensitive Information stored or downloaded without their consent. Defendants are responsible for unknown increases in disclosures, or risks of such disclosures, about private location data and Sensitive

Information of Plaintiffs, their families, plaintiff Class members and future purchasers, as a direct consequence of near constant recording of their locations.

222. Plaintiffs and Class members lacked the requisite intent to form a contract for the products that they actually received. There can be no valid contract without intent.

223. Products supplied were inadequate consideration for the monies paid and the value of Plaintiffs' individual location data and Sensitive Information created, stored and misappropriated by Defendants. These contracts fail for want of consideration.

224. Defendants accepted and retained money paid to them by Plaintiffs, and Plaintiffs' individual location data and Sensitive Information. The affirmative, knowing and intentional misrepresentations and omissions of Defendants, which Plaintiffs reasonably relied upon, in combination with Defendants' blatant breach of Plaintiffs' privacy, constitute circumstances that make it inequitable for Defendants to retain Plaintiffs' money or the benefit of Plaintiffs' location data or Sensitive Information.

COUNT XIII (Negligence)

225. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

226. Defendants had duties to Plaintiffs not to track, collect, or transmit their individual location data or Sensitive Information because Defendants lacked authorization from Plaintiffs to undertake those activities.

227. Defendants breached their duties to Plaintiffs by tracking, collecting, and transmitting their individual location data and Sensitive Information.

228. Defendants' breach of their duties to Plaintiffs directly and proximately

caused the Plaintiffs damages in the forms of:

- a. Exposing their location data and Sensitive Information to unauthorized recipients, and making it susceptible to access by third parties;
- b. Shortening the battery life of their Android devices by drawing power for the unauthorized creation, accumulation and transmittal of individual location data through communication with cell towers, wireless hotspots and GPS infrastructure;
- c. Requiring more frequent recharges of device batteries and the expenses associated therewith;
- d. Reducing the storage capability of their devices by covertly allocating limited device resources to create and store a database of individual user location information;
- e. Creating longer processing times for legitimate device uses because of resources drawn on by Defendants' location data and Sensitive Information transmittal activities;
- f. Causing an increase in data transfer expenses for users with limited data packages.

229. Further, Google and app-maker Defendants are subject to a heightened standard of care towards users if they are common carriers by virtue of their transporting information initiated by, and sent to, users of Android devices.

COUNT XIII
(Invasion of Privacy)

230. Plaintiffs re-allege and incorporate by reference the allegations contained in the paragraphs above, and those that come after as if fully set forth here.

231. Google and Defendants intruded on U.S. Plaintiffs' affairs or seclusion by prying into Plaintiffs' individual location several times a minute, and into their Sensitive Information, and sharing that information with third parties, and sending targeted ads to Plaintiffs on their devices at their unique locations.

232. This intrusion is objectionable to Plaintiffs and would be objectionable to a reasonable person. Plaintiffs' location, UDID and other Sensitive Information, and acts and transactions on their devices are within their own private domain and are private.

233. Defendants' acts and omissions have directly and proximately damaged Plaintiffs as described throughout this complaint.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs pray for judgment against Defendants as follows:

- A. For an order certifying the plaintiff Class and the two defendant Classes, as defined herein, appointing undersigned counsel as Class Counsel, approving Plaintiffs as Class representatives, approving all app-maker Pandora as app-maker defendant Class representative, approving marketers AdMob and Traffic Marketplace as marketer-defendant Class representatives, and requiring that notice be provided to the Classes at Google's expense, pursuant to Fed. R. Civ. P. 23;
- B. For declaratory and injunctive relief, including enjoining Google and Defendants from continuing to omit their true intentions about tracking

purchasers of their products, and requiring Defendants to stop tracking their products' users;

- C. For judgment on behalf of the plaintiff Class as defined herein for the amount of any payments made to Defendants with interest thereon;
- D. For exemplary, treble or punitive damages;
- E. For reasonable attorneys' fees and costs; and
- F. For such other and further relief as this Court deems equitable or just under the circumstances of Defendants' ongoing activities and omissions.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a trial by jury on all issues so triable against Defendants.

Respectfully submitted,

s/ Aaron Mayer
Aaron C. Mayer
FBN: 0076983
MAYER LAW GROUP, LLC
18 Carolina St., Suite B
Charleston, SC 29403
T: (843) 376-4929
F: (888) 446-3963
aaron@mayerlawgroup.com

Trial Counsel for Plaintiffs