

1 Lockridge Grindal Nauen P.L.L.P.
Richard Lockridge (not admitted)
2 Robert Shelquist (not admitted)
ralockridge@locklaw.com
3 rkshelquist@locklaw.com
100 Washington Avenue South, Suite 2200
4 Minneapolis, Minnesota 55401
Telephone: (612) 339-6900

5 Law Office of Joseph H. Malley
6 Joseph H. Malley (not admitted)
malleylaw@gmail.com
7 1045 North Zang Blvd
Dallas, TX 75208
8 Telephone: (214) 943-6100

9 William M. Audet (CA State Bar #117456)
waudet@audetlaw.com
10 Michael McShane (CA State Bar #127944)
mmcshane@audetlaw.com
11 Jonas P. Mann (CA State Bar #263314)
jmann@audetlaw.com
12 AUDET & PARTNERS, LLP
221 Main Street, Suite 1460
13 San Francisco CA 94105
Telephone: 415.568-2555
14 Facsimile: 415.568.2556

15 *Counsel for Plaintiffs*

16 IN THE UNITED STATES DISTRICT COURT
17 FOR THE NORTHERN DISTRICT OF CALIFORNIA

18 SAN JOSE DIVISION

19 DANIEL RODIMER, ARFAT ADIL, EMILI CLAR,
20 JEROD COUCH, BARBARA DAVIS, MATT HINES,
21 DIEGO LOPEZ, AARON MULVEY, ANNA M.
RUSTON, GENA TERRY; individuals, on behalf of
22 themselves and others similarly situated,

23 Plaintiffs,

24 v.

25 APPLE, INC., a California Corporation; FLURRY, INC.,
a Delaware Corporation; MEDIALETS, INC., a
26 Delaware Corporation; PINCH MEDIA, INC., a
Delaware Corporation; QUATTRO WIRELESS, INC., a
27 Delaware Corporation; IAC/INTERACTIVECORP, a
Delaware Corporation; GROUPON, INC., a Delaware
28 Corporation; NPR, a Washington, DC., Corporation;

FILED

FEB 15 2011

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PSG

CV 11

0700

CASE No.

JURY DEMAND

CLASS ACTION COMPLAINT FOR:

1. Violations of Computer Fraud and Abuse Act, 18 U.S.C. §1030;
2. Violations of the Electronic Communications Privacy Act 18 U.S.C. §2510;
3. Violations of California's Computer Crime Law, Penal Code § 502;

1 NEW YORK TIMES CO., a Delaware Corporation;
2 PANDORA MEDIA, INC., a Delaware Corporation;
3 WEBMD HEALTH SERVICES GROUP, INC, a
4 Delaware Corporation; YELP!, INC., a Delaware
5 Corporation; and Doe Corporations 1- 100 inclusive,

6 Defendants.

4. Violations of the California Invasion of Privacy Act, Penal Code § 630;
5. Violations of the Consumer Legal Remedies Act, ("CLRA") California Civil Code § 1750;
6. Violation of Unfair Competition, California Business and Professions Code § 17200;
7. Breach of Contract;
8. Conversion;
9. Trespass to Personal Property / Chattels; and
10. Unjust Enrichment

13 Plaintiffs, Daniel Rodimer, Arfat Adil, Emili Clar, Jerod Couch, Barbara Davis, Matt
14 Hines, Diego Lopez, Aaron Mulvey , Gena Terry, and Anna M. Ruston, on behalf of themselves
15 and all others similarly situated, by and through their attorneys, Audet & Partners, LLP,
16 Lockridge Grindal Nauen P.L.L.P., and Law Office of Joseph H. Malley, P.C., as and for their
17 complaint, and demanding trial by jury, allege as follows upon information and belief, based
18 upon, *inter alia*, investigation conducted by and through their attorneys, which are alleged upon
19 knowledge, sue Defendants Apple, Inc., Flurry, Inc., Medialets, Inc., Pinch Media, Inc., Quattro
20 Wireless, Inc., IAC/InterActiveCorp, Groupon, Inc., NPR, New York Times Co., Pandora
21 Media, Inc., WebMD, LLC, and YELP! Plaintiffs' allegations as to themselves and their own
22 actions, as set forth herein are based upon their personal knowledge, and all other allegations are
23 based upon information and belief pursuant to the investigations of counsel. Based upon such
24 investigation, Plaintiffs believe that substantial evidentiary support exists for the allegations
25 herein or that such allegations are likely to have evidentiary support after a reasonable
26 opportunity for further investigation and discovery.

27 The true names and capacities, whether individual, corporate, associate or otherwise, of
28 each of the Defendants designated as a DOE are unknown to Plaintiff at this time and therefore

1 Plaintiff sues Defendants by such fictitious names, pursuant to California Civil Code § 474.
2 Plaintiff will ask leave of the Court to amend this Complaint to show the true names and
3 capacities of the Doe Defendants when that information is ascertained. Plaintiff is informed and
4 believes, and thereon alleges that each of the Defendants designated herein as a DOE is legally
5 responsible in some manner, for the performance of the acts and omissions described below, and
6 is liable for the events and happenings alleged and, in such manner, proximately caused harm to
7 Plaintiff as further alleged.

8 Defendants, and the DOE Defendants, and each of them, are individually sued as
9 participants, co-conspirators, and aiders and abettors in the improper acts, plans, schemes, and
10 transactions that are the subject of this Complaint.

11 NATURE OF THE ACTION

12 1. Plaintiffs bring this consumer Class Action lawsuit pursuant to Federal Rules of
13 Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of themselves and a class of similarly
14 situated Internet users, each a "Class Member" of the putative "Class," as further described
15 herein, who were victims of privacy violations and unfair business practices; wherein their
16 privacy, financial interests, and security rights, were violated by the following Defendants:
17 Apple, Inc., (hereinafter referred to as "Apple"), Flurry, Inc., (hereinafter referred to as
18 "Flurry"), Medialets, Inc., (hereinafter referred to as "Medialets"), Pinch Media, Inc.,
19 (hereinafter referred to as "Pinch Media"), Quattro Wireless, Inc., (hereinafter referred to as
20 "QWAPI"), IAC/InterActiveCorp., (hereinafter referred to as "IAC"), Groupon, Inc., (hereinafter
21 referred to as "Groupon"), NPR, Inc., (hereinafter referred to as "NPR"), New York Times Co.,
22 (hereinafter referred to as "New York Times"), Pandora Media, Inc., (hereinafter referred to as
23 "Pandora Media"), WebMD, LLC, (hereinafter referred to as "WebMD"), and Yelp! Inc.,
24 (hereinafter referred to as "Yelp"), affiliated individually, and in concert, to gain unauthorized
25 access to, and unauthorized use of, Plaintiffs' and Class Members' mobile devices, referencing
26 electronic devices used for communication over a cellular network and include internet and
27 multimedia capabilities, which include specifically: iPhone, iPad, and iPod Touch; hereinafter
28 referred to collectively as "mobile devices," in order to access, collect, monitor, and remotely

1 store, electronic data derived, in whole or part, from the mobile devices', which includes but is
2 not limited to Unique Device Identifiers; hereinafter referred to as "UDIDs."

3 2. The nature of this action includes a sequence of events and consequences wherein
4 IAC/InterActiveCorp, Groupon, Inc., NPR, The New York Times Co., Pandora Media, Inc.,
5 WebMD, LLC, and Yelp! Inc., (hereinafter referred to collectively as "Application Developers")
6 and Pinch Media, Medialets, QWAPI, Flurry, (hereinafter referred to collectively as
7 "Application Developers Affiliates") gained individually, and in concert with Defendant Apple,
8 unauthorized access to, transmittal of, and use of data, which included but was not limited to, the
9 Plaintiffs' and Class Members' UDID, obtained from the Plaintiffs' and Class Members' mobile
10 devices, bypassing the technical and code based barriers intended to limit access, in addition to
11 bypassing the Plaintiffs' and Class Members' privacy and security settings. The Defendants
12 perpetuated this fraudulent activity knowingly, and with the intent to transmit and access data
13 obtained, in whole or part, by its use of the Plaintiffs' and Class Members' UDID for
14 unauthorized purposes, including but not limited to the Plaintiffs' and Class Members' mobile
15 browsing activities.

16 3. Apple acted independently, and in concert with Application Developers and
17 Application Developer's Affiliates, each knowingly authorized, directed, ratified, approved,
18 acquiesced in, or participated in conduct, made the basis of this Class action, which included, but
19 was not limited to, the unauthorized access to, and unauthorized use of the Plaintiffs' and Class
20 Members' mobile devices.

21 4. The Defendants' business plan involved unauthorized access to, and disclosure of,
22 Personal Information ("PI"), Personal Identifying Information ("PII"), Sensitive identifying
23 information ("SII"), hereinafter referred collectively to as User's Personal Information ("UPI"),
24 obtained from the Plaintiffs' and Class Members' mobile devices using their UDID, provided by
25 Defendant Apple, to aggregate all Plaintiffs and Class Member's data including but not limited
26 to, users' mobile device activities which Defendants accomplished covertly, without actual
27 notice, awareness, consent or choice of its users involving millions of consumers' mobile phones
28 circumventing Plaintiffs' and Class Members' privacy and security controls, for purposes not

1 disclosed within their Terms of Service and/or Privacy Policy, failing to protect Plaintiffs and
2 Class Members, involving their physical security, causing economic injury, obtained for
3 Defendants' commercial gain.

4 JURISDICTION AND VENUE

5 5. Venue is proper in this District under 28 U.S.C. §1391(b) and (c) against
6 Defendants. A substantial portion of the events and conduct giving rise to the violations of law
7 complained of herein occurred in this District and Defendants' conduct business with consumers
8 in this District. Defendant Apple, Inc.'s principle executive offices and headquarters, during the
9 class period, were located in this District at 1 Infinite Loop, Cupertino, CA, 95014.

10 6. This court has Federal question jurisdiction as the complaint alleges violation of
11 the following:

12 1) Computer Fraud and Abuse Act, 18 U.S.C. §1030; and

13 2) Electronic Communications Privacy Act 18 U.S.C. §2510

14 7. Subject-matter jurisdiction exists in this Court related to this action pursuant to 28
15 U.S.C. § 1332. The aggregate claims of Plaintiffs and the proposed Class Members exceed the
16 sum or value of \$5,000,000.00 exclusive of interests and costs.

17 8. Venue is proper in this district and vests jurisdiction in the California state and
18 federal courts in the district of the location of their principal corporate place of businesses. Thus,
19 mandatory jurisdiction in this U.S. District Court vests for any Class Member, wherever they
20 reside, for the mobile device activity made the basis of this action which occurred within the
21 United States. The application of the law of the State of California should be applied to any
22 mobile device activity made the basis of this action anywhere, within the United States, as if any
23 and all activity occurred entirely in California and to California resident. Thus, citizens and
24 residents of all states are, for all purposes related to this instant Complaint, similarly situated
25 with respect to their rights and claims as California residents, and therefore are appropriately
26 included as members of the Class, regardless of their residency, or wherever the mobile device
27 activity occurred made the basis of this action.

28 9. The following corporation is a California corporation headquartered in California,

1 during the class period, and Plaintiffs assert claims on behalf of a proposed class whose members
2 are scattered throughout the fifty states and the U.S. territories; there is minimal diversity of
3 citizenship between proposed Class Members and the Defendant, and the aggregate of these
4 claims exceed the sum or value of \$5,000,000.00 exclusive of interests and costs:

5 a. Apple, Inc.

6 10. The following corporations are non-California corporations, headquartered in
7 California, during the class period, and Plaintiffs assert claims on behalf of a proposed class
8 whose members are scattered throughout the fifty states and the U.S. territories; there is minimal
9 diversity of citizenship between proposed Class Members and the Defendant, and the aggregate
10 of these claims exceed the sum or value of \$5,000,000.00 exclusive of interests and costs:

11 a. Flurry, Inc.

12 b. Medialets, Inc.

13 c. Pandora Media, Inc.

14 d. Pinch Media, Inc.

15 e. Quattro Wireless, Inc.

16 f. YELP! Inc.

17 11. The following corporations are non-California corporations, were not
18 headquartered in California during the class period, and Plaintiffs assert claims on behalf of a
19 proposed class whose members are scattered throughout the fifty states and the U.S. territories;
20 there is minimal diversity of citizenship between proposed Class Members and the Defendant,
21 and the aggregate of these claims exceed the sum or value of \$5,000000.00 exclusive of interests
22 and costs:

23 a. WebMD, LLC

24 b. IAC/InterActiveCorp

25 c. Groupon, Inc.

26 d. NPR

27 e. The New York Times Co.

28 12. This Court has personal jurisdiction over the Defendant Apple which maintained

1 its corporate headquarters in, and the acts alleged herein, were committed in California, within
2 this district, during the class period.

3 13. Minimal diversity of citizenship exists in this action, providing jurisdiction as
4 proper in the Court, since Defendants are corporations headquartered in this District during the
5 class period, and Plaintiffs include citizens and residents of this District, and assert claims on
6 behalf of a proposed Class whose members are scattered throughout the fifty states and the U.S.
7 territories; thus there is minimal diversity of citizenship between proposed Class Members and
8 the Defendants.

9 14. This is the judicial district wherein the basis of the conduct complained of herein
10 involving the Defendants was devised, developed, implemented. The actual interaction of
11 information and data was activated from, and transmitted to and from this District; therefore all
12 evidence of conduct as alleged in this complaint is located in this judicial district.

13 PARTIES

14 15. Plaintiff Daniel Rodimer ("Rodimer") is a citizen and resident of Clearwater,
15 Florida, (Pinellas County, Florida).

16 16. Plaintiff Afat Adil ("Adil") is a citizen and resident of Los Angeles, California,
17 (Los Angeles County).

18 17. Plaintiff Emili Clar ("Clar") is a citizen and resident of Dallas, Texas, (Dallas
19 County, Dallas, Texas)

20 18. Plaintiff Jerod Couch ("Couch") is a citizen and resident of Ballinger, Texas,
21 (Runnels County, Ballinger, Texas).

22 19. Plaintiff Barbara Davis ("Davis") is a citizen and resident of Dallas, Texas,
23 (Dallas County, Dallas, Texas).

24 20. Plaintiff Matt Hines ("Hines") is a citizen and resident of Fort Worth, Texas,
25 (Tarrant County, Fort Worth, Texas).

26 21. Plaintiff Diego Lopez ("Lopez") is a citizen and resident of San Jose, California,
27 (Santa Clara County, San Jose, California).

28 22. Plaintiff Aaron Mulvey ("Mulvey") is a citizen and resident of Dallas, Texas,

1 (Dallas County, Dallas, Texas).

2 23. Plaintiff Anna M. Ruston ("Ruston") is a citizen and resident of Dallas, Texas,
3 (Dallas County, Dallas, Texas).

4 24. Plaintiff Gena Terry ("Terry") is a citizen and resident of Odessa, Texas, (Ector
5 County, Odessa, Texas).

6 25. Defendant Apple, Inc., ("Apple") is a California corporation headquartered in
7 California, during the class period, a privately owned corporation, which maintained its
8 headquarters at 1 Infinite Loop, Cupertino, CA 95014. Defendant Apple, Inc., did business
9 throughout the United States, and in particular, did business in State of California and in this
10 judicial district.

11 26. Defendant Flurry, Inc., ("Flurry") is a Delaware corporation headquartered in
12 California, during the class period, a privately owned corporation, which maintained its
13 headquarters at 282 2nd Street, Suite 202, San Francisco, CA 94105. Defendant Flurry, Inc., did
14 business throughout the United States, and in particular, did business in State of California and in
15 this judicial district.

16 27. Defendant Medialets, Inc., ("Medialets") is a Delaware corporation headquartered
17 in New York, during the class period, a privately owned corporation, which maintained its
18 headquarters at 450 W. 15th Street, Suite 200, New York, NY 10011. Defendant Medialets, Inc.,
19 did business throughout the United States, and in particular, did business in State of California
20 and in this judicial district.

21 28. Defendant Pinch Media, Inc., ("Pinch Media") is a Delaware corporation
22 headquartered in New Jersey, during the class period, a privately owned corporation, which
23 maintained its headquarters at 711 Adams St., Unit 5, Hoboken, NJ 07030. Defendant Pinch
24 Media, Inc., did business throughout the United States, and in particular, did business in State of
25 California and in this judicial district.

26 29. Defendant Quattro Wireless, Inc., ("QWAPI") is a Delaware corporation
27 headquartered in Massachusetts, during the class period, a privately owned corporation, which
28 maintained its headquarters at 260 Charles Street, 4th Floor, Waltham, MA 02453. Defendant

1 Quattro Wireless, Inc., did business throughout the United States, and in particular, did business
2 in State of California and in this judicial district.

3 30. Defendant IAC/InterActiveCorp, is a California Corporation with its principal
4 place of business in Oakland, California. Defendant is the maker of the iPhone App:
5 Dictionary.com

6 31. Defendant, Groupon, Inc., is a Delaware Corporation with its principal place of
7 business at 600 W. Chicago Ave., Suite 620, Chicago, Illinois. Defendant Groupon, is the maker
8 of the iPhone App: Groupon.

9 32. Defendant, NPR, is a Delaware Corporation with its principal place of business in
10 Washington, DC. Defendant, NPR, is the maker of the iPhone App: NPR.

11 33. Defendant, The New York Times CO., is a Delaware Corporation with its
12 principal place of business in Manhattan, NY. Defendant, New York Times Co., is the maker of
13 the iPhone App: N Y Times.

14 34. Defendant, Pandora Media, Inc., is a Delaware Corporation with its principal
15 place of business at 2101 Webster Street, Ste. 1650, Oakland, California 94612. Defendant,
16 Pandora, is the maker of the iPhone App: Pandora.

17 35. Defendant, WebMD, LLC, is a Delaware Corporation with its principal place of
18 business at 111 Eighth Avenue 7th Floor New York, NY 10011. Defendant, WebMD, LLC, is
19 the maker of the iPhone App: Medscape.

20 36. Defendant, YELP! Inc., is a Delaware Corporation with its principal place of
21 business in San Francisco, CA. Defendant, YELP!, is the maker of the iPhone App: YELP!.

22 **A. Plaintiff Daniel Rodimer's Experiences**

23 37. On information and belief, Plaintiff Daniel Rodimer's incorporates all allegations
24 within this complaint, and his experiences are the same to all Plaintiffs and Class Members.

25 38. At all relevant times herein, Rodimer owned a mobile device, used that mobile
26 device, and on one or more occasions during the class period, in the city of residence, accessed
27 the Defendant Apple's iTunes Store to download iTunes applications.

28 39. The downloaded iTunes Applications include, but are not limited to the following:

1 Messages, calendar, Photos, Camera, YouTube, Settings, Stocks, Maps, Weather, Compass,
2 lock, App Store, Tango, AOL Radio, Facebook, Ma...Mail, AZ_SB1070, Flashcards, Free WIFI,
3 Google Earth, iBooks, LawStock, Netflix, AllRecipes, BofA, Bible.

4 40. On information and belief, one (1) or more of the Defendants Application
5 Developers Application downloaded by Rodimer, is affiliated with one (1) or more of the
6 Defendant Application Affiliates.

7 41. As Rodimer accessed his applications, Defendant Apple then transmitted, and/or
8 allowed access to, without notice or authorization, his mobile device's UDID to the Defendant
9 Application Developers which then was transmitted to the Defendant Application Developers
10 Affiliates, acting in concert and individually, to access any and all available mobile device data
11 derived from Rodimer's mobile device.

12 42. In January 2011, Rodimer became aware of information related to the tracking
13 activities of one (1) or more of iPhone applications he had downloaded. It is Rodimer's belief
14 that Defendant Apple's transmitting of, or allowing access to, his mobile devices' UDID
15 permitted one or more objects within his mobile device to be used for tracking by Defendant
16 Application Developers and Application Developers Affiliates, thus his mobile device data was
17 obtained in an effort to monitor and profile his Internet application activities. Rodimer did not
18 receive notice of the installation of such a tracking identifier, did not consent to the installation of
19 such a tracking identifier, and did not want such a tracking identifier to be installed on his mobile
20 device; moreover did not authorize Defendant Apple to transmit his UDID to iPhone
21 applications, nor the Defendants Application Developer's, nor the Defendants Application
22 Developers Affiliates without notice or his express consent.

23 43. Rodimer observed that his mobile device tended to operate more slowly and
24 sometimes froze when loading web pages and that the actions of all Defendants used his
25 bandwidth without authority or compensation. Plaintiff Rodimer spent time for maintenance on
26 his mobile device, attempting to address this condition. Plaintiff Rodimer believes that, if he
27 were to visit the Apple iTunes Store and download applications, and/or open the Defendant
28 Application Developers Apps, the tracking device used by Defendants to access, collect, monitor,

1 and remotely store his electronic data, including but not limited to, UDIDs that will be used
2 again by the Defendants.

3 44. Plaintiff Rodimer considers information about his mobile device activities to be in
4 the nature of confidential, personal information that he protects from disclosure, including by
5 controlling his browser settings for acceptance or rejection. Plaintiff Rodimer was not made
6 aware by Defendant Apple that it would create a Unique Device Identifier and “sell” such to
7 parties, without his knowledge or authorization.

8 **B. Plaintiff Arfat Adil’s Experiences**

9 45. On information and belief, Plaintiff Arfat Adil incorporates all allegations within
10 this complaint, and his experiences are the same to all Plaintiffs and Class Members, including
11 Plaintiff Daniel Rodimer’s experience.

12 46. At all relevant times herein, Adil owned a mobile device, used that mobile device,
13 and on one or more occasions during the class period, in the city of residence, accessed the
14 Defendant Apple’s iTunes Store to download iTunes applications.

15 47. The downloaded iTunes Application include, but are not limited to the following:
16 Wells Fargo, Ringtones, Mover, Facebook, Words Free, Echofon, Pocket Tanks, FallingBalls
17 Flashlight, Bump, Yelp, Fandango, Urbanspoon, Shazam, ESPN Streak, RunKeeper, imeem
18 Pandora, Remote, Sportacular.

19 48. On information and belief, one (1) or more of the Defendants Application
20 Developers Application downloaded by Adil, is affiliated with one (1) or more of the Defendant
21 Application Affiliates.

22 **C. Plaintiff Emili Clar’s Experiences**

23 49. On information and belief, Plaintiff Emili Clar incorporates all allegations within
24 this complaint, and her experiences are the same to all Plaintiffs and Class Members, including
25 Plaintiff Daniel Rodimer’s experience.

26 50. At all relevant times herein, Clar owned a mobile device, used that mobile device,
27 and on one or more occasions during the class period, in the city of residence, accessed the
28 Defendant Apple’s iTunes Store to download iTunes applications.

1 51. The downloaded iTunes Application include, but are not limited to the following:
2 Currency, WallpapersHD, WallpapersHD, IMDb, Flixster, Netflix, Pandora, Shazam, Google,
3 NYtimes, Evernote, TWC, Yelp, iBooks, Google Earth, RedLaser, Light, Dictation, AroundMe,
4 Find iPhone, Wi-Fi Finder, Monopoly, Words, Jumping Dog, Sudoku2, Tetris, Scrabble, UNO,
5 Angry Birds, EOW, Wordweb, Skype, Epicurious, American, BofA, myWireless, realtor.com,
6 Amazon.com, eBay, seafood, facebook, perfect dogs, GasBuddy, Dog Parks.

7 52. On information and belief, one (1) or more of the Defendants Application
8 Developers Application downloaded by Clar, is affiliated with one (1) or more of the Defendant
9 Application Affiliates.

10 **D. Plaintiff Jerod Couch's Experiences**

11 53. On information and belief, Plaintiff Jerod Couch incorporates all allegations
12 within this complaint, and his experiences are the same to all Plaintiffs and Class Members,
13 including Plaintiff Daniel Rodimer's experience.

14 54. At all relevant times herein, Couch owned a mobile device, used that mobile
15 device, and on one or more occasions during the class period, in the city of residence, accessed
16 the Defendant Apple's iTunes Store to download iTunes applications.

17 55. The downloaded iTunes Application include, but are not limited to the following:
18 Facebook, Monopoly, Shazam, Last.fm, TWC, UPS, Wells Fargo, ScoreCenter, Pandora,
19 Backgrounds, Scramble CE, Tango, GC, Angry Birds, sudoku2, Dog Whistler, Worldwide
20 Ringtone, FOX news, BingMusic, Qik Video Pro, Microsoft Ex, ScoreCenter, NYTimes
21 iMapMyRUN.

22 56. On information and belief, one (1) or more of the Defendants Application
23 Developers Application downloaded by Couch, is affiliated with one (1) or more of the
24 Defendant Application Affiliates.

25 **E. Plaintiff Barbara Davis' Experiences**

26 57. On information and belief, Plaintiff Barbara Davis incorporates all allegations
27 within this complaint, and her experiences are the same to all Plaintiffs and Class Members,
28 including Plaintiff Daniel Rodimer's experience.

1 58. At all relevant times herein, Davis owned a mobile device, used that mobile
2 device, and on one or more occasions during the class period, in the city of residence, accessed
3 the Defendant Apple's iTunes Store to download iTunes applications.

4 59. The downloaded iTunes Application include, but are not limited to the following:
5 Hey Taxi, iRec, IQ Test, Pulsar, National Debt, Public Radio, Medscape, Fixster, Percalculator,
6 Snpattell, Whocited, formulas, My Wireless, your rights.

7 60. On information and belief, one (1) or more of the Defendants Application
8 Developers Application downloaded by Davis, is affiliated with one (1) or more of the
9 Defendant Application Affiliates.

10 **F. Plaintiff Matt Hines' Experiences**

11 61. On information and belief, Plaintiff Matt Hines incorporates all allegations within
12 this complaint, and his experiences are the same to all Plaintiffs and Class Members, including
13 Plaintiff Daniel Rodimer's experience.

14 62. At all relevant times herein, Hines owned a mobile device, used that mobile
15 device, and on one or more occasions during the class period, in the city of residence, accessed
16 the Defendant Apple's iTunes Store to download iTunes applications.

17 63. The downloaded iTunes Application include, but are not limited to the following:
18 Facebook, linkedIn, Twitter, Hulu Plus, DocsToGo, Installous, Messenger, Skype, eBay, Selling,
19 DIRECTV, GV-iView, Air Horn, Backbreaker, DH: Safari, Dropbox, Gunclub2, How To Tie,
20 Draw Slasher, BFHunting, Fish Tycoon, NYTimes, Dynamite Fishing, FOX news, 5-0 Radio
21 Pro, iBooks, Map Quest, ResidentEvil4, SleepMachineLite, Tap Fish, TweetDeck, Tap Zoo
22 Pandora, USPS mobile, Y! Messenger, WBAPAM, NPR Addict, NPR news, AccuWeather,
23 Gangstar, CamViewer, Crash Kart, Doodle God, FileViewer USB, WinterBoard, Yelp,
24 Atomic Web, Fruit Ninja, Draw Slasher, System, WorldView, Craigs + DFW, Recommends,
25 A-List DFW, RxMindMe, WSJ, iBeer, Groupon, Skee-Ball, mviewer, VTT, Attack, Best of
26 YouTube, Extreme, Mix Tube, Doodle Jump, Doodle Army, Fall Guy, Flick Fishing, Google
27 Earth, Google, Night stand, Sleep Cycle, foursquare, monster, vtiger.

28 64. On information and belief, one (1) or more of the Defendants Application

1 Developers Application downloaded by Hines, is affiliated with one (1) or more of the Defendant
2 Application Affiliates.

3 **G. Plaintiff Diego Lopez's Experiences**

4 65. On information and belief, Plaintiff Diego Lopez incorporates all allegations
5 within this complaint, and his experiences are the same to all Plaintiffs and Class Members,
6 including Plaintiff Daniel Rodimer's experience.

7 66. At all relevant times herein, Lopez owned a mobile device, used that mobile
8 device, and on one or more occasions during the class period, in the city of residence, accessed
9 the Defendant Apple's iTunes Store to download iTunes applications.

10 67. The downloaded iTunes Application include, but are not limited to the following:
11 Imeem, Justin .tv, iheartradio, AOL radio, Shazam, Pandora, 3PtLite, DinerDashLite, Labyrinth
12 LE, PaperFootball, Vegas Lite, Sudoku, DoodleJump, iFighterLite, BClassicLite, iBowl,
13 BeerPong, Sharpshooter, Apartments, Urbanspoon, Flashlight, eBay, Chase, Smartvocab, iCall,
14 Aim, textPlus, Trapster, Bump, Facebook, Whacksy Taxi, Kik, Spin Bottle, Paper Toss.

15 68. On information and belief, one (1) or more of the Defendants Application
16 Developers Application downloaded by Lopez, is affiliated with one (1) or more of the
17 Defendant Application Affiliates.

18 **H. Aaron Mulvey's Experiences**

19 69. On information and belief, Plaintiff Aaron Mulvey incorporates all allegations
20 within this complaint, and his experiences are the same to all Plaintiffs and Class Members,
21 including Plaintiff Daniel Rodimer's experience.

22 70. At all relevant times herein, Mulvey owned a mobile device, used that mobile
23 device, and on one or more occasions during the class period, in the city of residence, accessed
24 the Defendant Apple's iTunes Store to download iTunes applications.

25 71. The downloaded iTunes Application include, but are not limited to the following:
26 Skype, Google, IAC/InterActiveCorp, Pandora, Y! Messenger, Southwest, Compass, Patents,
27 Settings, Bump.

28 72. On information and belief, one (1) or more of the Defendant Application

1 Developers Application downloaded by Mulvey, is affiliated with one (1) or more of the
2 Defendant Application Affiliates.

3 **I. Plaintiff Anna M. Ruston's Experiences**

4 73. On information and belief, Plaintiff Anna M. Ruston incorporates all allegations
5 within this complaint, and her experiences are the same to all Plaintiffs and Class Members,
6 including Plaintiff Daniel Rodimer's experience.

7 74. At all relevant times herein, Ruston owned a mobile device, used that mobile
8 device, and on one or more occasions during the class period, in the city of residence, accessed
9 the Defendant Apple's iTunes Store to download iTunes applications.

10 75. The downloaded iTunes Application include, but are not limited to the following:
11 Compass, Google, HeyTell, TMZ, Justin.tv, Y! Messenger, Broadcaster, IMDb, iTranslate,
12 Pandora, AOL Radio, iheartradio, Shazam, Flixster, AroundMe, TalkingCarl, Find iPhone
13 TKL, SpillDamilk, Paper Toss, PapiJump, Papimissle, A Snake, Bowl Lite, Hungry..Ptl,
14 Game Center, Tv Quizzle, 4 in a row, Words Free.

15 76. On information and belief, one (1) or more of the Defendants Application
16 Developers Application downloaded by Ruston, is affiliated with one (1) or more of the
17 Defendant Application Affiliates.

18 **J. Plaintiff Gena Terry's Experiences**

19 77. On information and belief, Plaintiff Gena Terry incorporates all allegations within
20 this complaint, and her experiences are the same to all Plaintiffs and Class Members, including
21 Plaintiff Daniel Rodimer's experience.

22 78. At all relevant times herein, Terry owned a mobile device, used that mobile
23 device, and on one or more occasions during the class period, in the city of residence, accessed
24 the Defendant Apple's iTunes Store to download iTunes applications.

25 79. The downloaded iTunes Application include, but are not limited to the following:
26 Lose it!, MySpace, PAC-MAN, Pandora, Scramble CE, Skee-ball, SleepMachine, Smash Fiesta,
27 Smurfs, ToDo+, TPRI2010, Tricky FREE, Trip Out, TWC, Waldo, Wallpapers,
28 IAC/InterActiveCorp, DreamBook, EZ-30!, EZ-30!, Fandango, FOX Sports, French LE, Game

1 of Life, Ghost Radar, Glow..Snake, Google Earth, Hangman, Horoscopes, iHoroscope, IMDb,
2 LetsTans dlx, Facebook, Tango, UMK3, , FatBooth, AgingBooth, Million WPs, WallpaperHD,
3 55k Quotes, Alarm Clock, Angry Birds, Blue Block, Brain Trainer, College FB, Converter+,
4 CryptoQuote, Wallpapers, Words Free, ToonCamera, PhotoStudio, CharMap, ColorSplash,
5 Words, iP Free, HeyTell, Craigsphone, MyFoodCalc, VirtualMonkey.

6 80. On information and belief, one (1) or more of the Defendants Application
7 Developers Application downloaded by Terry, is affiliated with one (1) or more of the Defendant
8 Application Affiliates.

9 **K. Sequence of Events and Consequences- Plaintiffs and Class Members**

10 81. The sequence of events, and consequences common to Plaintiffs and Class
11 Members, made the basis of this action, include, but are not limited to the following:

12 a) Plaintiffs and Class Members are individuals in the United States who own and
13 use their Defendant Apple mobile devices, and accessed the Apple iTunes Store.

14 b) Defendant application developers are approved by Defendant Apple as a
15 “Developer” and entered into a licensing agreement with Defendant Apple to host a platform for
16 iPhone user’s access to iPhone applications.

17 c) Defendant Application Developer’s Affiliates are Ad Networks and/or Web
18 Analytic Vendors that are affiliated with authorized Apple iTunes Application Developers, and
19 entered into a licensing agreement with one (1) or more of the Defendant Application
20 Developers.

21 d) Plaintiffs and Class Members accessed the Defendant Apple iTunes Store, entered
22 into a licensing agreement with one (1) or more of the Defendant Application Developers,
23 installed iPhone applications associated with one (1) or more of the Defendant Application
24 Developers, within the class period.

25 e) Defendant Apple then transmitted, and/or allowed access to, without notice or
26 authorization, the Plaintiffs’ and Class Members’ UDID, to one (1) or more of the Defendant
27 Application Developers which in turn transmitted or allowed access of the UDID to its
28 Defendant Application Developer Affiliate.

1 f) Defendant Application Developers and its associated Defendant Application
2 Developer Affiliates then took unprecedented liberties, without notice, or authorizations, with
3 obtaining at will, any and all mobile device data of the plaintiffs and Class Member's mobile
4 devices, using the mobile device's UDID to aggregate the mobile device data.

5 g) Defendant Application Developers Affiliates then created, individually and in
6 concert with Defendant Application Developers, a database related to Plaintiffs and Class
7 Member's mobile device data, which also revealed web browsing activities, to assist the
8 Defendants tracking scheme. Such tracking could not be detected, managed or deleted, and
9 provided, in whole or part, the collective mechanism to track Plaintiffs and Class Members,
10 without notice or consent.

11 h) Defendant Application Developer's Affiliates and Defendant Application
12 Developers then conducted systematic and continuous surveillance of the Plaintiffs' and Class
13 Members' mobile devices activity, which continues to date.

14 i) Defendant Application Developer's Affiliates and Defendant Application
15 Developers Affiliates then copied, used, and stored the mobile device UDID data derived from
16 the Plaintiffs' and Class Members' mobile devices, after it knowingly accessed, without
17 authorization, the Plaintiffs' and Class Members' mobile device.

18 j) Defendant Application Developer's then obtained Plaintiffs' and Class Members'
19 UPI, derived, in whole or part, from its monitoring the mobile application activities of Plaintiffs
20 and Class Members. The personal information Defendants compiled, and misappropriated,
21 includes details about Plaintiffs' and Class Members' profiles to identify individual users to track
22 them on an ongoing basis, across numerous applications, and tracking users when they accessed
23 applications from different mobile devices, at home and at work. This sensitive information may
24 include such things as users' video application viewing choices to obtain personal characteristics
25 such as gender, age, race, number of children, education level, geographic location, and
26 household income, what the Plaintiffs and Class Members viewed and what he/she bought, the
27 materials he/she read, details about his/her financial situation, his/her sexual preference, and
28 even more specific information like health conditions.

1 k) Defendant Application Developers then used Defendant Application Developers
2 analytics software to collect, use and disclose device data to a third parties, an act that violates
3 Plaintiffs' and Class Members' mobile device's agreement.

4 l) Defendant Apple then provided assurances to Plaintiffs and Class Members that
5 any and all iPhone authorized applications had been "vetted" and were safe for downloading.

6 m) Defendant Apple then failed to notify and warn Plaintiffs and Class Members of
7 its covert activities within their mobile devices, and the covert tracking activities of Defendants
8 Application Developers and Application Developers Affiliates before, during, and after notice, of
9 the unauthorized practices, made the basis of this action, so that Plaintiffs and Class Members
10 could take appropriate actions to opt-out of the unauthorized surveillance by Defendants, and/or
11 to delete any and all Defendant applications

12 n) Defendant Apple then failed to block access to, and void the licensing agreements
13 of Defendant Application Developers after it received notice of individual and concerted actions,
14 made the basis of this action.

15 o) Defendant Apple then failed to provide any terms of service, or privacy policy,
16 related to its use of UDIDs for tracking, or provide an updated privacy policy alerting it's users
17 of Defendant Application Developers and Defendant Application activity, made the bases of
18 these actions, thus Plaintiffs and Class Members had no notice of such activities, nor the ability
19 to mitigate their harm and damage after the fact.

20 p) Defendant Apple Developers then failed to provide any terms of service, or
21 privacy policy, related to its use of UDIDs for tracking, or provide an updated privacy policy
22 alerting it's users of Defendant Application Developer's involvement and Defendants
23 Application's activity, made the bases of these actions, thus Plaintiffs and Class Members had no
24 notice of such activities, nor the ability to mitigate their harm and damage after the fact.

25 q) Defendant Apple Developers Affiliates then failed to provide notice to Plaintiffs
26 and Class Members of its tracking activities in order to obtain authorization, thus Plaintiffs and
27 Class Members had no notice of such activities, nor the ability to mitigate their harm and damage
28 after the fact.

1 r) Defendant Apple then did not provide Plaintiffs and Class Members information
2 within its privacy policies concerning the affiliation of each iPhone application developer, its
3 Application Developer's Affiliates, and information related to the extent of its tracking, made the
4 basis of this action, nor adequate opt-out information, resulting in the following:

5 1) Plaintiffs and Class Members that desired to cease tracking by Defendants
6 by deleting the Defendants' application, had Defendant continue to track
7 their activities.

8 2) Plaintiffs and Class Members that became aware of Defendants
9 association with each Defendant were unable to also delete their UDID
10 from within their own mobile device to cease all tracking.

11 s) Plaintiffs and Class Members that became aware that Defendants had created a
12 database, and deleted the databases to cease any and all tracking, had the Defendants maintain
13 storage and use of all data derived from its unauthorized activity.

14 t) Defendants then converted the Plaintiffs' and Class Members' electronic data,
15 including but not limited to UDIDs, for commercial gain.

16 u) Plaintiffs' and Class Members' allegations, made the basis of this action, are
17 supported in whole or part by the following recent studies:

- 18 1. Ashkan Soltani and David Campbell, Electric Alchemy.net, "The
19 Journal's Cellphone Testing Methodology," (last accessed January 25,
20 2011), online:
21 <http://online.wsj.com/article/SB1000142405274870403480457602595176>
22 [7626460.html](http://online.wsj.com/article/SB1000142405274870403480457602595176)
- 23 2. Eric Smith, "iPhone Applications & Privacy Issues: An Analysis of
24 Application Transmission of iPhone Unique Device Identifiers (UDIDs)"
25 (last accessed January 25, 2011), online: [http://www.pskf.us/wp/wp-](http://www.pskf.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf)
26 [content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf](http://www.pskf.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf); and
- 27 3. William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon
28 Jung, Patrick McDaniel, Anmol N. Sheth, "TaintDroid: An Information-

1 Flow Tracking System for Realtime Privacy Monitoring on Smartphones”

2 (last accessed January 25, 2011), online:

3 <http://www.appanalysis.org/tdroid10.pdf>

4 4. Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna,

5 “PiOS: Detecting Privacy Leaks in iOS Applications,” (last accessed

6 January 25, 2011), online:

7 <http://www.technologyreview.com/computing/27128/?pl=A2&a=f>

8 82. Plaintiffs and Class Members involved with the Defendants were harmed by its
9 practices, including but not limited to the following:

- 10 a) Violation of legally protected Federal, State and Common Law rights of
11 privacy.
- 12 b) Incurring time and expense to remedy the effects of Defendants’ actions to
13 their mobile devices.
- 14 c) Time and expense to repair their mobile device to remediate the impaired
15 operability caused by the Defendants.
- 16 d) Loss of property by the inability to re-sell Plaintiffs’ and Class Members’
17 mobile devices due to UDID tracking mechanism link to users’ browsing
18 data.
- 19 e) Financial Harm by the Defendants’ authorized use of Plaintiff and Class
20 Member’s mobile device’s Bandwidth used during the process of
21 Defendants obtaining mobile device data.

22 83. The conduct of the Defendants, individually and jointly, is a fraud that has been
23 perpetrated for years, facilitated, and coordinated, by some of the world’s largest application
24 developers, network advertising industry, and web analytic vendors, thereby costing the Class
25 upwards of tens of millions of dollars. Defendants has been systematically defrauding Class
26 Members in a covert operation of surveillance made possible by their gross misconduct,
27 negligence, apparent coordination, and actual fraud, and violating one (1) or more of the
28 following:

- 1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the “CFAA”);
- 2) Electronic Communications Privacy Act 18 U.S.C. §2510 (the “ECPA”);
- 3) California’s Computer Crime Law, Penal Code § 502;
- 4) California Invasion of Privacy Act, Penal Code § 630;
- 5) Consumer Legal Remedies Act, (“CLRA”) California Civil Code § 1750;
- 6) Unfair Competition, California Business and Professions Code § 17200;
- 7) Breach of Contract;
- 8) Conversion;
- 9) Trespass to Personal Property / Chattels; and
- 10) Unjust Enrichment

84. Defendants manipulated the Plaintiffs’ and Class Members’ mobile devices, which have computing functions used in and affecting interstate commerce and communication and were therefore protected computers, a conduct violation as defined in the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030(e)(2).

85. Defendants obtained Electronic Communications sent to the Plaintiffs’ and Class Members’ mobile device from defendant Apple, including but not limited to, the Plaintiffs’ and Class Members’ UDID, information sought to identify the Plaintiffs and Class Members, since such persisted across Internet sessions. Such provided in whole, or part, the ability to identify the user’s mobile device’s functions, a conduct violation of the Electronic Communications Privacy Act 18 U.S.C. §2510.

86. Defendants’ conduct, made the basis of this action, included but was not limited to, tampering, interference, unauthorized access to Plaintiffs’ and Class Members’ mobile device, a conduct violation of the California’s Computer Crime Law, California Penal Code § 502.

87. Defendants’ conduct, made the basis of this action, involved the unauthorized access to Plaintiffs and Class Members Electronic Communications with one (1) or more entities based in California, a conduct violation of the California Invasion of Privacy Act Penal Code § 630 et seq.

88. Defendants’ conduct, made the basis of this action, was an engagement in unfair

1 and deceptive acts and practices in the course of transactions with Plaintiffs and Class Members,
2 and such transaction were intended to and did result in the sale of services, a conduct violation of
3 the Consumer Legal Remedies Act, California Civil Code § 1750, et seq.

4 89. Defendants' conduct, made the basis of this action, resulted in acts of deception,
5 fraud, inconsiderable and unfair commercial practices, concealing, suppressing, and/or omitting
6 material facts with the intent to have Plaintiffs and Class Members rely upon such concealment,
7 oppression on omission. Defendants' unfair and deceptive trade acts caused damage and harm to
8 Plaintiffs' and Class Members', a conduct violation of the Unfair Competition Law, California
9 Business and Professions Code § 17200.

10 90. Defendant Apple's conduct, made the basis of this action, was a breach of contract
11 between Defendant Apple and Plaintiffs and Class Members, including but not limited to, failure
12 to abide by the licensing agreement which forbade release of personal information to third parties
13 without notice and express consent. Defendant Application Developers' contractual duties and
14 obligation to Defendant Apple do not release Defendant Apple from its liability to Plaintiffs and
15 Class Members.

16 91. Defendant Application Developers' conduct, made the basis of this action, was a
17 breach of contract between Defendant Apple and Plaintiffs and Class Members, including but not
18 limited to, failure to abide by the licensing agreement which forbade release of personal
19 information to third parties without notice and express consent. Defendant Apple and Defendant
20 Application Developer Affiliates contractual duties and obligation to Defendant Application
21 Developers do not release Defendant Application Developer from its liability to Plaintiffs and
22 Class Members.

23 92. Defendants' conduct, made the basis of this action, included acts of conversion
24 whereby the Plaintiffs' and Class Members' mobile device data, which included sensitive and
25 personal identifying information, was obtained by Defendants, exercising dominion over such
26 property, and providing to third parties for commercial gain:

27 • Plaintiffs and Class Members own the right to possess the personal property,
28 including but not limited to, Plaintiffs' and Class Members' data, obtained by the Defendants.

1 Defendants' intentionally exercised dominion and control over such user data, deprived the
2 Plaintiffs and Class Members of such possession and use, and caused damages to the Plaintiffs
3 and Class Members.

4 • Plaintiffs and Class Members sought to maintain the secrecy and confidentiality
5 of their personal information assets acquired by Defendants, which assets were Personal
6 Information ("PI"), Personal Identifying Information ("PII"), Sensitive identifying information
7 ("SII"), derived in whole or part from their Unique Device Identifiers ("UDIDs"), and/ or
8 Plaintiffs' and Class Members' Internet browsing activities.

9 • The means by which Defendants obtained such information and the reasons
10 Defendant engaged in its business practices made the basis of this action, demonstrate the
11 confidential character of such information, users' efforts to protect it, and the economic value of
12 Plaintiffs' and Class Members' data. Defendants acts of conversion include but are not limited to
13 the following,

14 • Defendants' conduct has caused economic loss to Plaintiffs and Class Members in
15 that, in a barter economy in which users' patronage (which is the subject of Defendants' traffic
16 measurement activities) is the currency with which users acquire ostensibly no-fee web services,
17 their patronage has independent economic value. In addition, inasmuch as Defendants'
18 wrongfully acquired Plaintiffs' and Class Members' patronage, Plaintiffs and Class Members
19 were deprived of the opportunity to contribute their patronage to web entities that did not engage
20 in such wrongful conduct,

21 • Further, the Plaintiffs' and Class Members' electronic data, misappropriated by
22 Defendants, and populated with their actual user data constitute assets with discernable values.
23 Certainly given Defendants' conduct, Defendants associate economic value with the Plaintiffs
24 and Class Members UDID derived data. In addition, even have specific valuations in criminal
25 markets. For example, Symantec reported that, in 2007, the illicit market value of a valid
26 Hotmail or Yahoo cookie was three dollars,

27 • The aggregated loss and damage sustained by Plaintiffs and Class Members,
28 individually and collectively, set forth above includes economic loss with an aggregated value of

1 at least \$5,000 during a one-year period. Defendants perpetrated the acts and omissions set forth
2 in this complaint through an organized campaign of deployment, which constituted a single act.

3 93. Defendants' conduct, made the basis of this action, resulted in an act of Trespass
4 to the Personal Property/ Chattel of the Plaintiffs and Class Members by obtaining user data and
5 a mobile device "Fingerprint," a practice of obtaining device information to perpetually identify
6 the mobile device. The Defendants' actions were surreptitious, without notice and so were
7 conducted without authorization and exceeding authorization. Defendants intentionally and
8 without consent, physically interfered with the use and enjoyment of personal property in the
9 Plaintiffs' possession, and the Plaintiffs and Class Members was thereby harmed. The
10 interference with the Plaintiffs' and Class Members' property/ chattel resulted in harm to their
11 interest in the physical condition, quality or value of the property/ chattel.

12 94. Defendants' conduct, made the basis of this action, individual improperly and
13 illegally profiting from the obtainment and/or sale of Plaintiffs' and Class Members' sensitive
14 and personal identifying information, committed intentionally and without notice to Plaintiffs
15 and Class Members such conduct provided Defendants an Unjust Enrichment:

16 **PRIVACY DOCUMENTS**

17 95. Defendant Apple does business online, using domains which include, but are not
18 limited to: <http://www.apple.com/itunes/>, and its business can be described as:

19 "An American multinational corporation that designs and markets consumer
20 electronics, computer software, and personal computers. The company's best-
21 known hardware products include the Macintosh line of computers, the iPod, the
22 iPhone and the iPad." As of January 21, 2011 Apple reports the Apple Store hits
23 10 billion downloads.

24 96. Defendant Apple's privacy documents entitled, Apple's "Privacy Policy," dated
25 October 25, 2010, (last accessed January 21, 2011), states in part:

26 • "We also collect non-personal information-data in a form that does not permit
27 direct association with any specific individual. We may collect, use, transfer, ad disclose non-
28 personal information for any purpose."

1 • “We may collect information such as occupation, language, zip code, area code,
2 unique device identifier, location, and the time zone where an Apple product is used so that we
3 can better understand customer behavior and improve our products, services, and advertising.”

4 • “If we do combine non-personal information with personal information the
5 combined information will be treated as personal information for as long as it remains
6 combined.”

7 • “Apple takes precautions-including administrative, technical, and physical
8 measures-to safeguard your personal information against loss, theft, and misuse, as well as
9 against unauthorized access, disclosure, alteration, and destruction.”

10 97. Defendant Apple’s Privacy Policy and Terms of Service intentionally, or in the
11 alternative, negligently, fails to reference its association with Defendant Application Developer’s
12 Affiliates, thus alleviating the possibility of its user opting-out of the Defendant Application
13 Developer’s Affiliates tracking, or in the alternative, negligently omits such association.

14 98. Defendant Apple’s Privacy Policy and Terms of Use intentionally or in the
15 alternative, negligently, fail to reference its association specifically with Defendant Application
16 Developers and Defendant Application Developer’s Affiliates, and its use of UDID Tracking. If
17 Plaintiffs and Class Members were adequately informed of Defendants’ Application Developer’s
18 Affiliates intrusive mobile tracking then they would not have downloaded the iPhone
19 applications.

20 99. Defendant Flurry does business online, using domains which include but are not
21 limited to: <http://www.flurry.com>, (last accessed January 25, 2011) Defendant Flurry’s business
22 involving web analytics. Defendant Flurry and Defendant Pinch Media merged on December 23,
23 2009.

24 100. Defendant Flurry’s privacy documents, entitled, “Flurry analytics privacy policy,”
25 dated October 1, 2008, (last accessed January 25, 2011), relate to commercial entities and not
26 individual web users, states in part:

27 • “Personal information does not include “aggregate” information, which is data
28 we collect about the use of the Sites or categories of Site users, from which any personal

1 information has been removed.”

2 • “Flurry may obtain information as a result of data being sent to our servers from
3 our software “agent” that may be embedded in an end user’s mobile application. We aggregate
4 that data, which tracks information such as use sessions, an end user’s handset, or an end user’s
5 country. Once the data is aggregated, we make it available for analysis by the developer of the
6 application.”

7 • “The “Analytics Service” means, collectively, the “Software”, the “Reports” and
8 the “Documentation”, all as defined below in this Agreement. Under this Agreement, Flurry may
9 allow you to access the Analytics Service by using Flurry's analytics site code and any fixes,
10 updates and upgrades provided to you (the “Agent”), provided that you have an active Flurry
11 account. In addition, Flurry may provide you with on-line access to a variety of analytics reports
12 (the “Reports”) generated by Flurry’s processing code and any fixes, updates and upgrades. The
13 Agent and Flurry’s processing code are defined collectively herein as “Software”. The
14 processing code analyzes the data collected by the Agent. This data concerns the characteristics
15 and activities of end users of your applications (“User Data”).

16 • “As a condition of your access to the Analytics Service, you agree that Flurry has
17 the right, for any purpose, to retain, use, and publish in an aggregate manner, subject to the terms
18 of its Privacy Policy located at <http://www.flurry.com/legal/privacy.do> (or such other URL that
19 Flurry may provide from time to time), information collected in your use of the Analytics
20 Service, including without limitation, User Data.”

21 101. Defendant Medialets does business online, using domains which include but are
22 not limited to: <http://www.Medialets.com>, (last accessed January 25, 2010) and describes its
23 business as follows:

24 • “Medialets is the most widely deployed rich media advertising solution for
25 mobile. Medialets brings unprecedented scale to mobile rich media campaigns by enabling the
26 delivery and measurement of the industry's highest-impact rich media across the broadest array
27 of top tier iPhone, iPad and Android apps. NPR, *The New York Times*, *Variety* and *The*
28 *Washington Post*, are just some of the top publishers that have enabled Medialets' cross-platform

1 rich media. Medialets' high-value formats are also available via leading ad networks, ad
2 mediators and ad servers through a preferred partner program,”

3 “Medialets to Enable Mobile Rich-Media Advertising in WeatherBug iPhone and iPad Apps”

4 (last accessed December 17, 2010), online:

5 <http://www.forbes.com/feeds/businesswire/2010/09/27/businesswire146044655.html>

6 • “Medialytics, – has been installed over 60 million times across more than 13
7 million unique devices to date. Medialytics measures behaviors in many of the top 20 highest
8 downloaded applications on the iPhone platform.”

9 “Medialets Surpasses One Billion Actions Processed from within iPhone Applications” (last
10 accessed December 17, 2010), online: <http://www.Medialets.com/blog/2009/04/>

11 102. Defendant Medialets’ privacy documents entitled, Medialets’ “Privacy Policy,”
12 dated January 9, 2009, (last accessed July 11, 2008), relate to commercial entities and not
13 individual web users, states in part:

14 • “Certain products or services offered by Medialets may require that we collect the
15 phone number and/or other unique identifiers of your users for their device. Some mobile phone
16 service providers are required to record the physical location of all devices that use their service.
17 It is possible that Medialets will receive this information, depending on the mobile phone service
18 provider policies.”

19 • “When users of your applications connect to Medialets services on their mobile
20 devices, we may receive the unique identification of their device or their phone number if
21 provided by their mobile phone service carrier.”

22 • “If users of your applications connect to Medialets services on their mobile
23 devices, Medialets may use the unique mobile device identification or phone numbers provided
24 by carriers to offer users extended services and/or functionality. In some circumstances,
25 Medialets may associate phone numbers or unique identifiers to other information we have
26 collected from and about these users. Medialets will not use phones or unique identifiers for
27 purposes of telemarketing.”

28 103. Defendant Medialets attempts to blur the line between the definition of PHI and

1 non- PII, including but not limited to its interpretation of the data collected by its use of
2 “Fingerprinting” technology on the Plaintiffs’ and Class Members’ mobile devices. Defendant
3 Medialets attempts to redefine PII by its method of collecting, in that, data anonymously
4 obtained, in whole or part, merged with additional data from other data mining sources, or
5 demographic or behavioral information that is connected to or correlated with an identified
6 individual is not PII.

7 104. Medialets’ “Privacy Policy,” dated July 11, 2008, (last accessed December 7,
8 2010), does not provide full disclosure as it relates to the purpose of Medialets’ affiliate
9 obtaining a user’s Unique Device ID (“UDID”), an unknown tracking device, as opposed to
10 cookies, a known tracking device.

11 105. Defendant Medialets’ Privacy Policy intentionally, or in the alternative,
12 negligently, fails to reference its association with any and all Application Developers or in the
13 alternative, negligently omits such association.

14 106. Defendant Medialets’ “Terms of Service for Developers,” no date noted, (last
15 accessed December 17, 2010), states in part:

16 • “Advertisements. The purpose and sole permitted use of the SDK is for you to
17 incorporate software instructions to allow Medialets to insert advertisements (“Ads”) from
18 Medialets-designated advertisers (“Advertisers”) that may be sourced directly by Medialets or
19 from third parties (“Advertising Agencies”) into your Applications. As a result of using the
20 SDK, you must embed Ad code into your Application at least once. Notwithstanding anything to
21 the contrary, all Ads, including those displayed within your Applications, are and shall remain
22 the property of the Advertiser. You obtain no rights in any Ads by virtue of utilizing the
23 Medialets Service.”

24 107. Medialets’ Terms of Use and Privacy Policy relate only to individuals that access
25 its website by choice and with actual notice, thus omitting the Plaintiffs and Class Members.

26 108. Defendant Pinch Media did business online, using domains which include but
27 were not limited to: <http://www.pinch-media.com>, (last accessed January 25, 2011 by accessing
28 www.waybackmachine.com) Defendant Pinch Media merged with Defendant Flurry on

1 December 23, 2009. Defendant Pinch Media's business involved web analytics.

2 109. Defendant Pinch Media's privacy documents entitled, Pinch Media's "Privacy
3 Policy," dated May 28, 2008, (last accessed January 25, 2011), relates to commercial services
4 provided to commercial entities and not mobile device users.

5 110. Defendant QWAPI does business online, using domains which include but are not
6 limited to: <http://www.quattrowireless.com>, (last accessed January 25, 2011) is now routed to
7 Defendant Apple's website since Defendant Apple purchased Defendant Quattro Wireless in
8 December 2009. QWAPI's CEO Andy Miller described its business as:

9 • "Unlike providers of advertising platforms only, Quattro Wireless works with
10 companies to create a complete mobile experience. This does not mean simply pushing text or
11 banner ads on to a website. What it means is that what Quattro Wireless does is re-create the
12 company website (leaving the .com/net URL) and re-create it for mobile. The company has
13 patent pending rendering solutions that recognizes how a consumer is viewing be it mobile or
14 online. The websites displayed will reflect (automatically) the device used. The advertising
15 comes into play after the website has been re-created. Then high quality sponsored ads from
16 Quattro's inventory are pushed to the site."

17 GoMo News, "Chat with Quattro Wireless CEO Andy Miller on differentiation in mobile
18 advertising," (last accessed December 7, 2010), online: [http://www.gomonews.com/chat-with-](http://www.gomonews.com/chat-with-quattro-wireless-ceo-andy-miller-on-differentiation-in-mobile-advertising/)
19 [quattro-wireless-ceo-andy-miller-on-differentiation-in-mobile-advertising/](http://www.gomonews.com/chat-with-quattro-wireless-ceo-andy-miller-on-differentiation-in-mobile-advertising/)

20 111. Defendant QWAPI's privacy documents entitled, QWAPI's "Privacy Policy,"
21 dated January 9, 2009, (last accessed January 25, 2011), states in part:

22 • "Personally Identifiable Information (PII)
23 Personally identifiable information (PII) is any information about consumers such as
24 name, address, or email address that is not otherwise available via public sources; provided,
25 anonymous information collected by aggregating volumes of users is not considered PII under
26 this policy. Quattro Wireless builds and hosts mobile websites for our clients; PII may be
27 collected in the course of a web site visit as part of the users' interactions with that site. When PII
28 is collected in this manner, this PII data is the property of our website partners and is subject to

1 their privacy policy. Quattro Wireless may not use this data in any way that is not authorized by
2 our website partners, and we will not use PII for ad targeting or for any other purpose.”

3 112. Defendant QWAPI attempts to blur the line between the definition of PII and non-
4 PII, including but not limited to its interpretation of the data collected by its use of
5 “Fingerprinting” technology on the Plaintiffs’ and Class Members’ mobile devices. Defendant
6 QWAPI attempts to redefine PII by its method of collecting, in that, data anonymously obtained,
7 in whole or part, merged with additional data from other data mining sources, or demographic or
8 behavioral information that is connected to or correlated with an identified individual is not PII.

9 113. QWAPI’s “Privacy Policy,” dated January 9, 2009, (last accessed January 25,
10 2011), does not refer to its use of a Global Unique ID (“GUID”) an unknown tracking device, as
11 opposed to cookies, a known tracking device.

12 114. Defendant QWAPI’s Privacy Policy intentionally, or in the alternative,
13 negligently, fails to reference its association with QWAPI Affiliates or in the alternative,
14 negligently omits such association.

15 115. QWAPI’s Terms of Use and Privacy Policy relate only to individuals that access
16 its website by choice and with actual notice, which excludes any method or means involving
17 browser hijacking; thus omitting the Plaintiffs and Class Members.

18 116. Defendant Application Developer’s Terms of Service and Privacy Policy do not
19 reference notice that iPhone user’s mobile devices’ UDID shall be obtained for tracking
20 purposes, provided to Application Developer Affiliates, and used to build a profile data collected
21 of any and all user’s mobile device activities. Many application developers do not even provide
22 any Terms of Service and/or privacy policies.

23 117. Some Application Developers have amended its Terms of Service and/or privacy
24 policy since studies revealed iPhone applications were obtaining UDIDs, including but not
25 limited to, Defendant Pandora, which omitted such within its prior privacy policy of April 18,
26 2010:

27 • “Information about your computer or device: We may also collect information
28 about the computer, mobile or other devices you use to access and listen to the Service. For

1 example, our servers receive and record information about your computer and browser, including
2 potentially your IP address, browser type, and other software or hardware information. If you
3 access the Service from a mobile or other device, we may collect a Unique device identifier
4 assigned to that device or other transactional information for that device.” Pandora Media, Inc.
5 privacy policy effective as of January 11, 2011.

6 FACTUAL ALLEGATIONS

7 A. Background

8 118. In 1999 Intel released the “Pentium 3” and each processor included a unique
9 serial number which could be read by any software installed on the system. Consumers, privacy
10 groups, and legislative authorities voiced outrage and privacy concerns and Intel was forced to
11 remove this function. In 2007 Apple released the iPhone and each included a unique software
12 visible serial number called a Unique Device Identifier (“UDID”). On July 10, 2008 Apple’s
13 “App Store” was launched as a service for the iOS devices, (the iPhone, iPod Touch and iPad),
14 and permitted users to download applications from the iTunes store. Recent studies though
15 revealed that Apple had transmitted, or allowed access to, user’s UDIDs, without authorization,
16 allowing Application Developers, and Application Developers Affiliates to obtain users’ UDIDs
17 for tracking users’ mobile device activity. As of January 21, 2011, Apple reported that 10 billion
18 applications had been downloaded. In light of the privacy concerns Apple should not have placed
19 this product in its current iteration into the marketplace at all and has failed to withdraw such
20 upon notice if privacy concerns, nor make adequate privacy and security alterations. The Intel’s
21 Pentium 3’s crisis pales in comparison to the recent Apple’s UDID privacy implications.

22 119. Consumers need products that provide strong security, offer robust and varied
23 authentication tools to support electronic commerce, and protect individual privacy and
24 anonymity. Apple unique identifier does not meet this standard, because, the privacy risks
25 inherent in this unique ID feature outweigh the benefit it potentially provides. The objective of
26 the Defendants’ business practices was the unauthorized transmittal, access, collection, and use
27 of, the mobile devices data, on a systematic and continuous basis, in order to perpetually harvest
28 the Plaintiffs’ and Class Members’ sensitive and personal identifying information from their

1 mobile device browsing activities.

2 120. This consumer class action involves a pattern of covert mobile device
3 surveillance, wherein the Defendants, operated individually, and in concert, associated in fact,
4 and targeted Internet users that visited the Apple iTunes Store and downloaded iPhone
5 applications, to knowingly, and without the user's knowledge or consent; commit unauthorized
6 transmittal, access, collection, and use of, a Unique Device Identifier ("UDID"), derived from
7 the Plaintiffs' and Class Members' mobile device, then transmitted a program, information, code,
8 and command, to collect, monitor, and remotely stored mobile device data aggregated by the
9 UDID, in order to obtain data for tracking the Plaintiffs and Class Members.

10 **B. Mobile Tracking**

11 121. Traditional online advertising practices, such as the tracking of individual users
12 across sessions and controlling the frequency and relevance of advertising presented to them,
13 simply do not exist in the mobile Internet today.

14 122. Mobile Internet advertising currently consists of streaming graphic files, in real
15 time, into content rendered by a user's mobile device browser. Image and text call to action
16 advertising tags that are embedded in the content at a publisher's content management system.
17 This occurs prior to delivery of the actual content to the user over the wireless network. Current
18 mobile practice for many of the server side include ad serving systems, so as to log delivery of
19 user impressions when the ad tags are transmitted from the ad server, across the Internet to the
20 publisher's content system.

21 123. Mobile advertising systems lack reliable browser tracking while traditional online
22 advertising relies on the use browser cookies, implementations inherent in conventional
23 implementations of mobile ad serving have effectively prevented mobile advertising from being
24 effective.

25 124. The lack of standard advertising metrics for mobile campaigns has discouraged
26 online advertisers from taking advantage of the unique personalized nature of mobile devices and
27 local content. Due in part from the inability of the mobile advertising industry to incorporate web
28 analytics.

1 125. There are basically two approaches to collecting web analytics data. The first,
2 “page tagging,” uses a small bit of JavaScript code placed on each web page to notify a third-
3 party server when a page has been viewed by a web browser. Etags can be used in place of
4 cookies. They are a part of caching in HTTP: The server sends the user the tag, and when the
5 user accesses the resource again their web browser sends the tag back. The server uses the tag the
6 browser sent to decide whether to send the user the data or provide data to the browser that the
7 data hasn’t changed, and to keep using the old copy.

8 126. The second and more traditional approach to web analytics is “log file analysis”,
9 where the log files that Web servers use to record all server transactions are also used to analyze
10 website traffic.

11 127. All Internet advertising, online or mobile, seeks “state maintenance” or the idea
12 that the person/browser/phone that saw the ad performs some later activity. Because most mobile
13 phones don’t support fully functional browsers, they also don’t obtain “uniqueness,” necessary to
14 obtain “state maintenance.” Obtaining the user’s IP address won’t work because most mobile
15 phones don’t have a public IP address. They access the web through Network Address
16 Translation at the carrier, meaning that many phones are seen by the entire web as all one IP.

17 128. In order to obtain “uniqueness” in mobile devices, the key was to obtain a Unique
18 Device Identifier or “UDID,” a special type of identifier used in software applications to provide
19 a unique reference number in mobile devices. Unlike traditional cookies, a user has no choice
20 whatsoever here. A user can’t opt-out, since it is always sent. It can’t be deleted since it always
21 stays the same. A user cannot use a block UDID transmitted, as they would in a browser, since it
22 is hard coded into a user’s phones software. Defendant Apple accomplished the task of obtaining
23 device uniqueness, and Defendants reaped the benefits.

24 129. Prior to Defendant Apple’s UDID, Application Developers were limited to a
25 unique identifier, hereinafter referred to as a Global Unique Identifier (“GUID”), which
26 originates from a device registering at a website, online store, Web Analytic Vendors or by the
27 ad networks. “GUID’s” created by application developers provides functionally that allows
28 application developers to uniquely identify the user for purposes such as storing application

1 preferences or video game high scores, playlists, etc. In some cases personal contact information
2 and authorization to other linked accounts is also provided. This is so users don't need to register
3 or log on. The GUID does facilitate the process of collecting and storing certain types of data,
4 but also provides a tempting opportunity for use as a tracking agent to correlate with other
5 personally-identifiable information but a GUID is not a UDID, nor does it have the benefits of a
6 UDID.

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

14 131. Advertising networks and mobile analytic companies obtain UDIDs to have
15 visibility across all of its applications, so tracking is consistent regardless of an individual's
16 location or connection. It is not anonymous tracking, since it runs at the application layer, the
17 same layer that a web-browser runs already therefore its stats involve information which has
18 nothing to do with user metrics or usage. Security violations occur when the device identifier is
19 combined with the following attributes: authenticated login information (e.g. a banking
20 application can link the UDID with a full banking consumer profile), (nick)name of iOS device
21 owner, type of connection (e.g. Wi-Fi versus 3G), model type (version of mobile device), home
22 address, phone number, and geo-location information. While the UDID does not exist for
23 nefarious reasons, its use can be for nefarious purposes.

24 132. The advertising and marketing industries have been strongly advancing technical
25 means of synchronizing tracking code so that information about individual consumer behavior in
26 cyberspace can be shared between companies and the UDID used in the majority of mobile
27 devices would be put to this purpose. The records of many different companies are merged
28 without the user's knowledge or consent to provide an intrusive profile of activity on the

1 computer. There are no practical limits on what can be collected or used.

2 133. Many advertising and behavioral tracking systems that use the UDID, without the
3 customer's knowledge or consent, brag about its ability to report on every action a user took
4 within an app: every button click, every page viewed, every table cell viewed, and the time a
5 person took between each action, all sent back to the server without any notification or customer
6 access to that information. Thus, UDIDs are most useful to people who want to track and collect
7 user behavioral data without user notification or permission (ad networks and behavioral
8 monitors). And since the UDID is the same for every app on a device, this is a boon to
9 advertisers and other data aggregators. The mobile advertising world will no longer have to place
10 a cookie to track a user across sites/apps, the UDID is like a permanent cookie that the user
11 cannot turn off.

12 134. Defendants' Application Developers and Application Developers Affiliates'
13 technology, made the basis of this action, is basically using some of the modern HTML5
14 capabilities of mobile browsers to perform the same tasks as a traditional cookie, but out of sight
15 of most users and while it is not technically a mobile cookie since it's not browser based, is on
16 the server side, thus it cannot be affected by anti-cookie technologies employed by carriers such
17 as gateway stripping (a technique that renders the cookies useless or unreliable for ad targeting),
18 and preventing users from deleting them. Wireless carriers typically prevent outside firms from
19 embedding such information in mobile devices. To get around the carriers, it embeds its digital
20 code in servers rather than browsers, since most mobile devices forbid the use of third party
21 software in Applications to collect and send Device Data to a third party for processing or
22 analysis, banning "Third Party" Analytics.

23 135. In a non-technical version, what Application Developer's Affiliates do is have its
24 application developers include a small JavaScript in its application. An invisible iFrame is
25 created which loads code from the iPhone application. It determines if it has seen the user before
26 and initiates a database (for the domain) and then communicates through iFrame message-
27 passing to its client that it should create a mirror of this database for the iPhone application
28 domain.

1 136. Application developer's affiliates develop and sell tools to track, collect (and
2 store) data and analyze mobile and Internet-enabled apps to facilitate advertising or assist
3 developers build applications. In the final analysis, the developer/application publisher should
4 also be held responsible for any and all data privacy violations.

5 137. By piggy backing on Applications, Defendant Application Developers Affiliates
6 gains access to the richest customer metrics with the shortest distance to customer purchase
7 decisions and the sales funnel. Web analytic vendors track app usage, but also attract advertisers
8 to both for third-party applications and for Application Developers Affiliates service itself. The
9 web analytics vendor is also involved in an ad-insertion technology in addition to involvement in
10 the ad network. Mobile analytics serves the purpose of an optimization tool to help increase app
11 downloads and sales.

12 138. Developing an account creation system is time consuming and costly, and thus the
13 majority of application developers who don't need multi-device accounts choose to use the
14 UDID instead of its own GUID to save time and money. As such, Apple incentivizes developers
15 to use the UDID by not providing them with a similarly useful privacy-enhanced customer
16 identification tool. The UDID privacy risks could have been mitigated though by Apple if an
17 identifier would have been used that was unique for the combination of application and device if
18 the device returned to a program different for each app.

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

1 140. The spectrum of mobile analytics involve “application analytics” aimed at
2 application developers, “campaign analytics” aimed at optimizing tools for media companies,
3 and “service analytics,” aimed at providing platforms for data mining networks or mobile device
4 data.

5 141. SDK’s though provided Application Developer Affiliates the access to
6 Application users when Application Developers downloaded the Application Developer
7 Affiliates’ SDK into its application; such provided the ability to obtain the Plaintiffs’ and Class
8 Members’ UDID and to conduct cross application tracking, activities made the basis of this
9 action. Application Developers Affiliates allowed application developers such access to as to
10 monetize its application:

11 • “Make dollars and sense from your apps. Medialytics™ is a powerful tool that
12 allows mobile app developers and advertisers to gain key insights into their apps and understand
13 their users like never before. Create an Account. It’s free! Make enlightened improvements to
14 your app based on measurable insights into user behavior. Use the comprehensive Dashboard to
15 monitor the metrics that matter most at a glance. Define Any Custom Events in your app that
16 you’d like to monitor and Medialytics™ delivers an even more intimate understanding of your
17 users’ behavior. Create an Account”

18 Medialytics, (last accessed February 8, 2011), online: <http://www.medialytics.com/>

19 142. The SDK’s also involve tracking libraries whose sole purpose is to collect and
20 compile statistics on application uses and usage, and send the device ID as part of their
21 functionality. Most of these libraries are used to display advertisements so as to provide revenue
22 for the application developer; and the mechanism for the libraries to also provide the mobile
23 device’s UDID once the user installed applications.

24 143. Client libraries available for iPhone were created using open source SDK for,
25 consistency and easy integration. The client libraries also provide flexibility for deeper
26 integrations and customization. Once integrated with an app, the client library sends function
27 calls (Required: open, upload, close. Optional: tagEvent, setOptIn / isOptIn.) to control a session.
28 These calls to the server can be uploaded upon start of the application (recommended) to place

1 one single server call with batched information or can be configured to fire more or less
2 frequently. Analytic data is written to persistent storage immediately after it's recorded and is
3 available within the user interface in real-time.

4 144. Basically, Web Analytics consist of a library that is compiled into and iPhone
5 application and a web service. Generally, when the application starts, it pings the web service
6 with a small amount of information and when the application is about to terminate, it pings the
7 service again. The developer may also choose to ping the service at other various points in the
8 application. These pings are then aggregated on the server into various reports. The UDID data
9 will also be sent in the ping so they know what app to count the ping on.

10 145. A user's UDID without user's mobile device data may not be linked directly to a
11 user; however "Libraries" of data exist, such as Facebook where an application developer can
12 use such to integrate Facebook library with the apps thus connecting the user's UDID to the user.
13 The Facebook connect on the iPhone allows the app developer to obtain a Facebook ID, once a
14 user is logged in, and then the app developer can link the UDID to a Facebook account in order
15 to link user to a mobile device.

16 146. Game app developers, using user's high scores, can also be tracked if a UDID is
17 obtained from a mobile device and related to an application instead of relying only on the UDID
18 itself. Such would prevent such analytic libraries from building usage profiles per mobile device.

19 147. Defendants Application Developers Associates collect mobile device data,
20 including the user's UDID, aggregate such into a variety of reports, merging data from all
21 associated applications, to produce reports by price point, application category, operating system
22 and various other criteria. The aggregated data is then impossible to determine which application
23 data supplied the specific processor data. Application developers then can claim they did not
24 provide all of the user's data, but only part of the data.

25 148. The SDKS enable application developers to track usage of its app in real time and
26 just as if it were a website. First, the application developer identifies the places in its app where it
27 would like to trigger a page view or an event, and then uses the SDK's to send these events to
28 Web Analytics Vendors.

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

7 150. Apple's iPhone is involved in the largest release, collection, and use of user data
8 in history. iPhone app's and ADA's are involved in a data mining feeding frenzy, like
9 pyromanias feeding on a prey, devouring user's data "To The Bone".

10 **C. Defendants' Release of UDIDs- Studies**

11 151. When Apple addressed a congressional inquiry on privacy in July, 2010 Apple
12 claimed its transactions were anonymous and thoroughly randomized. Recent Studies however
13 exposed that Apple's business practices with iPhone application developers and third party web
14 analytic vendors, such as Defendant Application Developer's Affiliates, does not confirm this
15 opinion.

16 152. On September 28, 2010, a joint study by Intel Labs, Penn State, and Duke
17 University was released which identified that publicly available cell-phone applications from
18 application markets were releasing consumers' private information to online advertisers. In a
19 study of 30 popular applications, TaintDroid revealed that 15 send users' geographic location to
20 remote advertisement servers. The study also found that seven of the 30 applications send a
21 unique phone (hardware) identifier.

22 • Our experimentation indicates these fifteen applications collect location data and
23 send it to advertisement servers. In some cases, location data was transmitted to advertisement
24 servers even when no advertisement was displayed in the application.

25 William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick
26 McDaniel, Anmol N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime
27 Privacy Monitoring on Smartphones" (last accessed September 28, 2010), online:
28 <http://www.appanalysis.org/tdroid10.pdf>

1 153. On October 1, 2010, a second study, written by Eric Smith, Assistant Director of
2 Information Security and Networking at Bucknell University, raised similar privacy questions
3 about how Unique Device Identifiers (“UDIDs”) could be used to track how customers use
4 applications associated with the device, how developers can access a device UDID, and correlate
5 it with personally identifiable information:

6 • A number of applications which have the potential to map UDID to user identity
7 were studied to determine if they are actively collecting UDID data. UDID collection by
8 applications requesting user credentials. Of the applications evaluated in this study that collected
9 UDIDs require users to log in, and have personally-identifiable information affiliated with user
10 accounts, 30% clearly transmit UDIDs; the rest used SSL to encrypt data transmission.

11 • Of those, 68 percent transmitted UDIDs to servers under the control of developers
12 or advertisers, while another 18 percent sent encrypted data that could have included the unique
13 serial number. Just 14 percent of the apps were confirmed not to send UDIDs.

14 • It is clear from this data that most mobile device application vendors are
15 collecting and remotely storing UDID data, and that some of these vendors also have the ability
16 to correlate the UDID to a real-world identity.

17 • A number of the applications considered in this study requested access to the on-
18 board GPS receiver. Several such applications – games, for example -- had no obvious need for
19 this information. In several cases, applications which transmitted UDIDs were observed to
20 transmit the mobile device’s latitude and longitude as well.

21 Eric Smith, “iPhone Applications & Privacy Issues: An Analysis of Application Transmission of
22 iPhone Unique Device Identifiers (UDIDs)” (last accessed January 20, 2010), online:

23 <http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf>

24 154. On December 17, 2010, a third study, by David Campbell and Ashkan Soltani
25 revealed that iTunes application were transmitting UDIDs:

26 • An examination of 101 popular smartphone “apps”—games and other software
27 applications for iPhone and Android phones—showed that 56 transmitted the
28 phone’s unique device ID to other companies without users’ awareness or

1 consent. Forty-seven apps transmitted the phone's location in some way. Five sent
2 age, gender and other personal details to outsiders.

- 3 • Many apps don't offer even a basic form of consumer protection: written privacy
4 policies. Forty-five of the 101 apps didn't provide privacy policies on their
5 websites or inside the apps at the time of testing. Apple requires app privacy
6 policies to?

7 David Campbell and Ashkan Soltani, Electric Alchemy.net, "The Journal's Cellphone Testing
8 Methodology," (last accessed January 20, 2011), online:

9 <http://online.wsj.com/article/SB10001424052748704034804576025951767626460.html>

10 155. On January 24, 2011, a fourth study by the Vienna University of Technology,
11 Austria was released which confirmed previous studies that iPhone applications were obtaining
12 UDIDs:

- 13 • "To show the feasibility of our approach, we have analyzed more than 1400
14 iPhone applications. Our results demonstrate that a majority of application leak the device ID."
- 15 • "While not directly written by an application developer, libraries that leak device
16 IDs still pose a privacy risk to users. This is because the company that is running the
17 advertisement or statistics service has the possibility to aggregate detailed application usage
18 profiles. In particular, for a popular library, the advertiser could learn precisely which subset of
19 applications (that include this library) are installed on which devices. For example, in our
20 evaluation data set, AdMob is the most-widely-used library to serve advertisements. That is, 82%
21 of the applications that rely on third-party advertising libraries include AdMob. Since each
22 request to the third-party server includes the unique device ID and the application ID, AdMob
23 can easily aggregate which applications are used on any given device."
- 24 • "Obviously, the device ID cannot immediately be linked to a particular user.
25 However, there is always the risk that such a connection can be made by leveraging additional
26 information. For example, AdMob was recently acquired by Google. Hence, if a user happens to
27 have an active Google account and uses her device to access Google's services (e.g., by using
28 Gmail), it now becomes possible for Google to tie this user account to a mobile phone device.

1 As a result, the information collected through the ad service can be used to obtain a detailed
2 overview of who is using which applications. Similar considerations apply to many other
3 services (such as social networks like Facebook) that have the potential to link a device ID to a
4 user profile (assuming the user has installed the social networking application). The
5 aforementioned privacy risk could be mitigated by Apple if an identifier would be used that is
6 unique for the combination of application and device. That is, the device ID returned to a
7 program should be different for each application.”

8 • “The unique device ID of the phone is treated differently and more than half of
9 the applications leak this information (often because of advertisement and tracking libraries that
10 are bundled with the application). While these IDs cannot be directly linked to a user’s identity,
11 they allow third parties to profile user behavior. Moreover, there is always the risk that outside
12 information can be used to eventually make the connection between the device ID and a user.”

13 Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna, “PiOS: Detecting
14 Privacy Leaks in iOS Applications” (last accessed January 24, 2011), online:

15 <http://www.iseclab.org/papers/egele-ndss11.pdf>

16 **iPhone Accessible Data**

17 *“It is a little known fact that, despite Apple’s claims, any applications*
18 *downloaded from the App Store to a standard iPhone can access a significant*
19 *quantity of personal data.”*

20 Nicolas Seriot, “iPhone Privacy” (last accessed January 6, 2011), online:

21 http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf

22 156. Traditional online advertising does not obtain a UDID of user’s mobile device.
23 The Defendants’ objective was not traditional and included, but was not limited to, obtaining a
24 mobile device “Fingerprint,” a practice of obtaining device information to perpetually identify
25 the mobile device as “indirect identification,” which can then be linked to additional data
26 elements to identify “personable identifiable information” (“PII”), personal information and/ or
27 sensitive information:

28 *“If we ask whether a fact about a person identifies that person, it turns out that*

1 *the answer isn't simply yes or no. If all I know about a person is their ZIP code, I*
2 *don't know who they are. If all I know is their date of birth, I don't know who they*
3 *are. If all I know is their gender, I don't know who they are. But it turns out that if*
4 *I know these three things about a person, I could probably deduce their identity!*
5 *Each of the facts is partially identifying."*

6 Electronic Frontier Foundation, Technical Analysis by Peter Eckersley, "A Primer on
7 Information Theory and Privacy" (last accessed October 15, 2010), online:
8 <http://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy>

9 157. The collection, use and disclosure of tracking data, such as obtaining a users'
10 UDID by Defendants to provide its services, implicates Plaintiffs' and Class Members' privacy
11 and physical safety. Such Information is afforded special attention due to the consequences for
12 both privacy and physical safety that may flow from its disclosure. The heightened privacy and
13 physical safety concerns generated by the collection, use and disclosure of location information
14 are apparent in U.S. law that creates restrictive consent standards for its use and disclosure in the
15 private sector in the context of telecommunications services.

16 158. "Apple's release of its users' UDID has the potential to transform the World Wide
17 Web from a largely anonymous environment into one where individuals are expected, or even
18 required, to identify themselves in order to participate in online activities, communicate, make
19 purchases, and would represent a grave erosion of consumer's online privacy. Many of the
20 activities that individuals engage in on the Web do not require the collection of identifiers or
21 personal information of any type. "Free" applications involve a user not paying for a product, but
22 a paying with their personal information, which becomes the actual product.

23 159. Due to Apple's market dominance, the UDID has the potential to become the
24 unique identifier for nearly everyone on the Internet -- fundamentally changing the Web
25 experience from one where consumers can browse and seek out information anonymously, to
26 one where an individual's every move is recorded. Our society's experience with unique
27 identifiers suggests that embedding the UDID into mobile devices will erode individual privacy.
28 The history of the Social Security Number reveals the unrelenting pressures to expand the use of

1 an identifier once it is created -- even where its use is initially curtailed by federal policy. Once a
2 unique identifier capable of identifying and tracking individuals in the online environment is
3 created, it will be far more difficult to limit its use. However, if an individual's browser is set not
4 to prompt prior to executing programs, then the alien program will read the UDID without the
5 individual's knowledge or consent. The Social Security Number (SSN) offers a compelling
6 example of how a unique identifier can undermine individual privacy and become a de facto
7 national identifier; the UDID has the potential though to further the surreptitious collection and
8 use of data without an individual's consent. Unlike a real world identifier, such as the Social
9 Security Number, the UDID, a virtual identifier, is capable of being collected without the
10 individual's knowledge and consent.

11 160. Defendant Apple has entered in a licensing agreement with a substantial amount
12 of application developers, numbering in the thousands that are without restraint or control by
13 Apple, accessing at will any and all Plaintiffs' and Class Members' mobile device data.
14 Interpretation of the Apple EULA is varied among Application Developers but provides insight
15 to present privacy concerns, made the basis of this action:

16 [Name and service redacted for privacy reasons] said on February 2nd, 2011 at 12:32 PM:

17 • "I myself am an iOS developer. You are running the app under the developers
18 EULA (which is really provided by apple). The EULA allows our apps to access your data. You
19 gave us permission to do so when you accepted the iTunes terms and conditions and when you
20 purchased the app."

21 [Name and service redacted for privacy reasons] said on February 2nd, 2011 at 12:54 PM:

22 • "I am thoroughly familiar with Apple's iOS developers' agreement, and it does
23 not permit developers' apps to access at least certain customer's information that is categorized
24 as personal information. To access that information through an app, the developers must ask the
25 customer's permission to do so in the app. If the customers refuse to consent, the only option for
26 the developer is to either change the terms or not provide the app."

27 161. While the Defendant's Apple's UDID provides an aggregate point of reference,
28 the secondary issue is the mobile device data that was obtained. The recent studies noting that

1 UDIDs were being provided from Defendant Apple to Defendant Application Developers and
2 Defendant Application Developer Affiliates revealed some, but not all, of the mobile device data
3 being transmitted and accessed by such parties. A study by Nicolas Seriot, "iPhone Privacy,"
4 describes a comprehensive list of potentially sensitive information that can be accessed by iOS
5 applications, methods to access such data, and comments:

- 6 • Access to the address book
- 7 • Current GPS coordinates of the device
- 8 • Unique Device ID
- 9 • Photo Gallery
- 10 • Email account information
- 11 • WiFi connection information
- 12 • Phone related information (Phone #, last called, etc.)
- 13 • Youtube application (watched videos and recent search)
- 14 • MobileSafari settings and history
- 15 • Keyboard cache

16 162. The Seriot study provides an in depth analyses of the entry points to obtain
17 sensitive and personal identifying information:

- 18 • "The first and easiest item of personal data to collect is the user's phone number.
- 19 • Another way to collect personal data is through the Address Book API. It turns
20 out that the full Address Book is readable without the user's knowledge or consent. It contains
21 names, users' phone numbers and email addresses, but also a "notes field", in which many Mac
22 users store sensitive data such as door codes or bank accounts.

- 23 • Next, we consider the data that can be read on the iPhone file system. A
24 sandboxing mechanism limits access to other application's data. Third party applications are
25 installed in /private/var/mobile/Applications/ and are prevented from seeing each other or
26 accessing specific location. About the sandboxing mechanism, Apple writes: Applications on the
27 device are "sandboxed" so they cannot access data stored by other applications. In addition,
28 system files, resources, and the kernel are shielded from the user's application space. It turns out

1 that, despite sandboxing, numerous system and application preference files are in fact readable
2 (see listing 2) by downloaded applications, and some of them contain personal data.

3 • Read the iPhone UUID (through a documented API), the ICCID (SIM card serial
4 number) and the IMSI (International Mobile Subscriber Identity), making it possible to track
5 users even when they change their device. IMSI reveals the country and the mobile operator.

6 • The keyboard cache contains all the words ever typed on the keyboard, except the
7 ones entered in password fields. This is supposed to help auto completion but this mechanism
8 effectively acts as a key-logger, storing potentially private and confidential names and numbers.

9 • Any application has read and writes access to the DCIM directory that contains
10 the photos stored in the iPhone. By default, these photos are tagged with the GPS coordinate.

11 • Another file keeps track of every time you join a WiFi network. Based on these
12 logs, it is possible to gain insights into the user recent' whereabouts.

13 • Safari recent searches (figure 3), YouTube history (figure 4) and your keyboard
14 cache (figure 8) give clues about your current interests. These interests are linked with your
15 name and your email addresses (figure 6), your phone number (figure 5) and your area (figure
16 12). Harvested from large numbers of users, such data have a huge value in the underground
17 market of personal data, and it must be assumed that trojans are in fact exploiting this on the App
18 Store.

19 • To be published on Apple's App Store, an application must be submitted by a
20 developer enrolled in the (paid) "iPhone Developer Program"²⁴. Apple only gets the executable
21 file, not the source code. Note that even if Apple had access to the source code, it probably could
22 not afford a full security code review.

23 • A breakout game is made available for free on Apple's App Store. While you are
24 playing breakout, it reads your email address, your recent Safari searches, your weather cities
25 and the words contained in your keyboard cache. When you submit your high score to the
26 application's server, stolen information is sent at the same time in an encrypted form. The
27 application also sends all the email addresses in your address book.
28

1 • First of all, Apple should stop claiming [1] that an application cannot access data
2 from other applications.

3 • There is no reason why the WiFi connection logs should be readable. The same
4 applies to the keyboard cache, which should be an OS service associated with text fields. It
5 should not be possible to retrieve their whole contents.

6 • The iPhone clearly lacks an optional outbound firewall similar to Little Snitch on
7 the Mac. Such a service would allow people to opt-out from the various analytics frameworks.

8 • At the end of the day, the fact that so many developers use analytics frameworks
9 may be a hint to Apple to give more usage information to developers, and provide users a setting
10 to opt-out.

11 • Users should be required to grant access to the Address Book (see 4.2.2)
12 individually for each application, as is currently the case for the Core Location framework. A
13 breakout game has no business accessing your contacts.

14 • Device unique identifier- The device unique identifier is currently available
15 through the official SDK's API. While it is not personal data since it cannot identify a physical
16 person, it may be used to aggregate data collected from various applications and analytics
17 frameworks. As a general rule, an application should not be able to know which other
18 applications you have run. Users merely accept cross-site cookies on the web; they probably
19 would not accept their computer's unique identifier to be transmitted to Google Analytics. A
20 possible solution for Apple would be to add something like an app device identifier or ADID.
21 This value would be unique for a given device and the requesting application. The current device
22 unique identifier could be kept, but the user should be asked to allow or deny its usage, as with
23 Core Location."

24 Nicolas Seriot, "iPhone Privacy" (last accessed January 28, 2011), online:

25 http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf

26 **D. "Bandwidth Hogs"-Economic Harm**

27 163. The Defendant's activities, made the basis of this action includes, but is not
28 limited to, economic harm due to the unauthorized use of Plaintiffs and Class Member's

1 Bandwidth.

2 164. Bandwidth is the amount of data that can be transmitted across a channel in a set
3 amount of time. Any transmission of information on the internet includes bandwidth. Similar to
4 utility companies, such as power or water, the “pipeline” is a substantial capital expenditure, and
5 bandwidth usage controls the pricing model. Hosting providers charge user’s for bandwidth
6 because their upstream provider charges them and so forth until it reaches the “back bone
7 providers”. Retail providers purchase it from wholesalers to sell its consumers.

8 165. “Unlimited” plans are not unlimited. Major provider plans may refer to its plans
9 as unlimited for marketing purposes, but the plans have limitations, usually noted in a footnote or
10 link to another page discussing its limitations as to usage amounts. Providers could not possibly
11 allow “unlimited” plans because servers do not have unlimited amounts of space. “Unlimited”
12 Data plans used to be unlimited until people started to figure out how to” tether”, a method for
13 connecting a computer to the internet via an internet-capable mobile phone. The term
14 “unlimited” then is used to define what is considered to be more than a reasonable amount of
15 data allotment.

16 166. Network provider’s data plans charge consumers based upon items such items as
17 usage and “caps”, ie \$30.00 per month for an unlimited plan is standard, but limited plans have
18 caps, such as: 256 GB per month. Some national providers charge \$1.00 per GB of bandwidth
19 exceeding a certain cap. Whether the data plan is marketed as “unlimited” or “limited”, the costs
20 for the plans are allocated based upon the bandwidth usage, thus as the standard use of
21 bandwidth increases, so too does the plan costs increase. Since plans are based upon user’s
22 average use, as consumer’s usage increases collectively, costs increase for all users, while
23 individual bandwidth overages can be costly:

24 “AT&T never mentions specific rates for data overages in its rate plan
25 terms, but the company does say that it will notify users before imposing
26 additional charges and that it will give users the right to terminate their service
27 beforehand if they don’t wish to pay the charges.

28 The company has also posted specific data overage rates for its

1 DataConnect plans. According to AT&T's Web page detailing available data rate
2 plans, users who pay \$60 for their DataConnect services get a monthly 5GB
3 bandwidth cap and are to pay \$0.00048 per additional kilobyte of data they
4 consume, or about \$500 per every gigabyte over the cap. Thus, a user who
5 consumed three times the amount of data allowed by the company's bandwidth
6 cap would be charged about \$5,000 extra per month."

7 Brad Reed, "User sues AT&T over \$5,000 Web bill" (last accessed January 14,
8 2011) online: <http://www.apple.com/legal/mobileme/en/terms.html>

9 167. Limitations on bandwidth use are also not only controlled by the providers, but
10 also mobile device providers such as Defendant Apple:

11 **"Limitations on Use"**

12 You agree to use the Service only for purposes as permitted by these TOS
13 and any applicable law, regulation, or generally accepted practice in the
14 applicable jurisdiction. Your MobileMe account is allocated certain levels of
15 storage capacity and bandwidth for network traffic and email as described in the
16 MobileMe feature pages. Exceeding any applicable limitation of bandwidth or
17 storage capacity (for example, iDisk or e-mail account space) is prohibited. To
18 view your current storage and data transfer or bandwidth allocations, log in to
19 your MobileMe account page at <http://secure.me.com/account>. In addition, if
20 there is Excessive Usage on your account or any Sub-account (as defined in
21 Section 3 below), Apple reserves the right to temporarily disable access to
22 information available from your account through a URI., or to "bounce" emails
23 back to senders. "Excessive Usage" as used herein, may apply to storage and/or
24 bandwidth capacities, and means your usage within a given month or day (as
25 applicable) greatly exceeds the average level of monthly or daily usage of
26 MobileMe's members generally. Repeated violations may result in termination of
27 your account Apple reserves the right to modify these limitations on use at any
28 time."

1 168. The technology behind the World Wide Web is the Hypertext Transfer Protocol
2 (HTTP) and it does not make any distinction as to the types of links, thus all links are
3 functionally equal. Resources may be located on any server at any location. When a web site is
4 visited, the browser first downloads the textual content in the form of an HTML document. The
5 downloaded HTML document may call for other HTML files, images, scripts and/or style sheet
6 files to be processed. These files may contain tags which supply the URL's which allow images
7 to display on the page. The HTML code generally does not specify a server, meaning that the
8 web browser should use the same server as the parent code. It also permits absolute URLs that
9 refer to images hosted on other servers. Once the application has stored the data, it will attempt
10 to send information back to application developer affiliate's servers. In most cases this is done
11 every time you open & close application. The data is continually tracked. An application
12 developer affiliate's enabled application does not take just one sample, it will record every use of
13 the application for the life of that application on your phone and your information is sent
14 automatically at a user's expense.

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

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

26 171. Defendant Application Developers and Defendant Application Developers
27 Affiliates used ad content, such as streaming video on audio, that required excessive Plaintiff and
28 Class Member's bandwidth, due in part, because there was no incentive to reduce the ad size

1 used for ads because it could directly pass costs for bandwidth and ad delivery content to
2 Plaintiff and Class Member's, without the Plaintiff and Class Member's from having any notice,
3 ie a Plaintiff and Class Member's playing a game application, and at the same time, Defendant
4 Application Developers and Defendant Application Affiliates were silently harvesting personal
5 data and sending it to remote servers using Plaintiff and Class Member's bandwidth.

6 172. The Defendant's use of the Plaintiffs and Class Member's bandwidth for its data
7 mining activities is similar in nature to a practice called "hot linking"; wherein one(1) server
8 users another server and its bandwidth to send data. While it slows down the server, it also
9 allows bandwidth costs to be transferred to another server. Any redirect of a user's browsing
10 capabilities to access or download Defendant's and/or data mining activities produces similar
11 unauthorized bandwidth use. While only the tech savvy individuals are aware that their mobile
12 devices are used as a server without their knowledge or consent, fewer individuals are aware of
13 the extent that Application Developers and Application Developer Affiliates make "calls", to
14 third parties, and amount of user's bandwidth used when a user merely accesses a site:

15 "Let's look at what the popular twitterfon app does:

- 16 b. App start
- 17 c. Calls videoegg.adbureau.net, reports an iPhone is being used, sends
18 UDID, app name & version.
- 19 d. Calls met.adwhirl.com, sends app ID, iPhone UDID, county
- 20 e. Calls twitter
- 21 f. Calls pagead2.google syndication.com
- 22 g. Calls beacon.pinchmedia.com, sends UDID, iPhone firmware, app ID &
23 version, crack & jailbreak status, start & stop times
- 24 h. App close"

25
26 Yobie Benjamin, "iBigBrother? iPhone privacy issues may interest FCC and FTC" (last accessed
27 January 25, 2011) online: [http://www.sfgate.com/cgi-](http://www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?entry_id=46054)
28 [bin/blogs/ybenjamin/detail?entry_id=46054](http://www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?entry_id=46054)

1 173. The unauthorized Bandwidth use of the Plaintiffs and Class Member's mobile
2 devices was compounded by Apple's introduction of its push-notification system. Initially,
3 Apple iPhone SDK's restricted all code except that which relies on Apple's own programming
4 interference to run. This restriction limited Application Developers from running on the iPhone
5 "as is" due to its uses of scripting language inside the software. Such limitations would affect
6 game applications that use interpretive language in the background, moreover third party
7 software that depended on persistence to work and software that polls the rest of the system.

8 174. With the advent of Apple's push-notification, the Defendant Application
9 Developer's and Defendant Application Affiliates could now conduct at will, their data mining
10 activities, in the "background" using Plaintiffs and Class member's bandwidth, without notice or
11 consent. Apple initially claimed that allowing "background activity" would be too much of a
12 drain on the handset's batteries and system resources, but once the push-notification system was
13 introduced Apple's concerns were apparently forgotten. Applications could now stay connected
14 to the apple server due to the persistent connection to the handset. This "background" connection
15 would automatically relay data from an application developer's server to apple, and in turn to the
16 iPhone application itself, allowing any program to continue to receive data, using in part, the
17 Plaintiffs and Class Member's bandwidth.

18 175. Excluding the amount that the Plaintiffs and Class members use by their own
19 activities, the Defendant's unauthorized data mining activities caused substantial bandwidth use
20 to the Plaintiffs and Class Members resulting in actual out of pocket expenditures, for
21 Defendant's activities which include, but are not limited to the following:

- 22 a) Transmittal of and access to Plaintiffs and Class Members UDID;
- 23 b) Loading of Ads first before content, bundling ads, and ads with excessive
24 bandwidth;
- 25 c) Use of SDK's, and its functions within Plaintiffs and Class Member's
26 mobile device;
- 27 d) "Harvesting" of Plaintiffs and Class Member's mobile device data;
- 28 e) "Background" Activities including "data mining".

1 **E. iPhone Application Developer License Agreement**

2 176. Application Developers that associate with Defendant Apple must initially
3 complete an “Apple’s iPhone Developer’s Licensee Agreement” and agree to its terms which
4 include the following:

5 “You and the Application must comply with all applicable privacy and data
6 collection laws and regulations with respect to any collection, transmission,
7 maintenance, processing, use, etc. of the user’s location data or personal
8 information by the Application. In addition, the use of any personal information
9 should be limited solely as necessary to provide services or functionality for Your
10 Application (e.g., the use of collected personal information for telemarketing
11 purposes is prohibited (unless expressly consented to by the user)). You and the
12 Application must also take appropriate steps to protect any such location data or
13 personal information from unauthorized disclosure or access.”

14 177. Application Developers must pay an initial fee and renewed fees per year, and
15 agree to a revenue of 70% to the application developer and 30% to Apple on sold applications.

16 178. Any application that a developer makes available to the Apple App store must
17 first be approved by Apple; the UDID allows Apple to track the apps on the iOS devices and
18 determine whether they are approved or not. A signed certificate is provided by Apple after the
19 application has been “vetted.” Due to the volume of new applications, and revenue earned by
20 Apple for accepting new applications, the revenue process though has shortened dramatically
21 during 2010.

22 179. The entire family of devices built on the iPhone OS (iPhone, iPod Touch, iPad)
23 have been designed to run only software that is approved by Apple—a major shift from the
24 norms of the personal computer market. Apple designed the iPhone platform so as to control all
25 software that was executed on the mobile device, thus the design did not allow full system (or
26 root) access to users.

27 180. Once an application is in compliance with Apple’s licensing agreement, it is
28 accepted, digitally signed, and made available through the iTunes App Store. Apple iTunes Store

1 users wanting to install applications on iOS must access the iTunes Store and initially agree to
2 licensing terms which include terms of use and a privacy policy.

3 181. Apple warranted to its users that it would provide protection from malicious
4 applications and offered a “vetting” process to review each and every application before offering
5 such to its users. The process is secretive, cannot be confirmed, but Apple did not require all
6 apps to have privacy policies due to the volume of new applications, incentivized by the revenue
7 earned by Apple for accepting new applications, the revenue process has shortened dramatically
8 during 2010.

9 182. The provisions in Apple’s user agreement that prohibited data transmissions in
10 whole or part, and data sharing without a consumer’s consent was not sufficient, due in part since
11 Apple failed to take steps to enforce these terms, nor terminated licensing agreements upon
12 Notice of Privacy Violations. Defendant’s applications platforms and content
13 collection/distribution media-mobile Web sites, applications, did not follow establish policies,
14 and allowed transactions to occur that were in violation of Defendant Apple policies;
15 furthermore Defendant Apple allowed such violations to occur after provided notice of such
16 activities and Apple had the ability to terminate all entities that violated its policies:

17 • “This Agreement shall terminate automatically upon Licensee’s breach of any of
18 the terms of this Agreement. Apple may terminate this Agreement at will upon 10 days’ written
19 notice.”

20 183. Defendant Apple, individually, and in concert with Defendant Application
21 Developers and Defendant Application Developer Affiliates violated the privacy
22 rights of Plaintiffs and Class Members; moreover such violations continue to date
23 although Defendant Apple has a “kill switch” to stop application which violate its
24 users’ privacy, obtaining mobile device data, without authorization or consent and
25 fails to act:

26 • “Steve Jobs, Apple’s chief executive, has confirmed there is a ‘kill switch’ built
27 into the iPhone that allows Apple to remotely delete malicious or inappropriate applications
28 stored on the device. However, Mr. Jobs insisted that the so-called ‘kill switch’ was there as a

1 precaution, rather than a function that was routinely used. “Hopefully we never have to pull that
2 lever, but we would be irresponsible not to have a lever like that to pull,” said Mr. Jobs.”

3 Claudine Beaumont, “Apple’s Jobs confirms iPhone ‘kill switch’” (last accessed January 28,
4 2011) online: [http://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-](http://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html)
5 [kill-switch.html](http://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html)

6 184. Defendant Apple enabled the business practices, of Defendants, made the basis of
7 this action, by “relaxing” its privacy policy as it related to third party networks, since stringent
8 privacy policies to enforce its privacy policies threatened its revenues.

9 185. Apple’s Privacy Policy and representatives provided assurances to its users that
10 they were protected when they downloaded apps, and Plaintiffs and Class Members that
11 downloaded iTunes Apps, believed they had a general expectation of anonymity:

12 • “Apple takes precautions- including administrative, technical, and physical
13 measures- to safeguard your personal information against loss, theft, and misuse, as well as
14 against unauthorized access, disclosure, alteration, and destruction.”

15 • “We have created strong privacy protections for our customers, especially
16 regarding location-based data,” says Apple spokesman Tom Neumayr. “Privacy and trust are
17 vitally important.”

18 186. Tracking and monitoring of mobile device usage will have a negative effect on
19 individuals’ access to information. The anonymity that the Internet affords individuals has made
20 it an incredible resource for those seeking out information. Particularly where the information
21 sought is on controversial topics such as sex, sexuality, or health issues such as HIV, depression,
22 and abortion; the ability to access information without risking identification has been critical. It
23 will result in increased pressure on individuals to permit the collection of the UDID, and other
24 information that can be tied to it, as a quid pro quo of engaging in transactions and interactions
25 online, placing a burden on individuals who choose to protect their privacy.

26 **F. Apple 4.0 PLA, Section 3.3.9.**

27 187. In January 2010 Defendant Flurry reported it had been tracking Defendant Apple
28 since October 2009, running an iPhone OS 3.2, revealing Defendant Apple’s data about its new

1 products; moreover providing geo-location data of Defendant Apple's activity. Defendant Flurry
2 analytics tools were providing too much info to the point that they detected the iPad and its
3 characteristics before the actual announcement. Plaintiffs and Class Members did not, nor could
4 possibly have had, notice of the activities of the Defendant Application Developers and
5 Application Developers Affiliates' activities, made the basis of this action, verified in whole or
6 part, by the inability of Apple to keep their device specifics protected when it failed to detect that
7 Flurry had been scanning its online actions.

8 188. Defendant Apple's CEO, Steve Jobs was outrage and voiced his concerns related
9 to Defendant Flurry obtaining mobile device data, without authorization. The ability of
10 Defendant Flurry analytics being able to covertly obtain such data from Defendant Apple
11 without Defendant Apple having notice provides insight as to similar outrage and concern from
12 Plaintiffs' and Class Members' for the identical acts, made the basis of this action:

13 "“It's violating every rule in our privacy policy,” Jobs boomed. “We went through
14 the roof about this. So we said: No, we're not going to allow this. It's violating
15 our privacy policies and its pissing us off that they're publishing data about our
16 new products.”

16 “So we said we are only going to allow these analytics that don't give device
17 information and therefore are solely for the purpose of advertising,” Jobs said.
18 “We're not going to be the only advertiser. There's others, and we're not banning
19 other advertisers from our platforms.”

19 “They can do that. But they can't send data out to an analytics firm who is going
20 to sell it to make money and publish it to tell everybody that we have devices on
21 our campus that we don't want people to know about. That,” Jobs said, “we don't
22 need to do.”

22 Jobs acknowledged that there are legitimate uses of data analysis by app
23 developers, if users are appropriately apprised of the fact that their data is being
24 shared. “After we calm down, we're willing to talk to some of these analytics
25 firms,” Jobs said. “But it's not today.”

25 Daniel Eran Dilger, “Jobs: iPhone ad SDK changes for user privacy, not anti-competitive” (last
26 accessed January 28, 2011), online:
27 [http://www.appleinsider.com/articles/10/06/02/jobs_iphone_ad_sdk_changes_for_user_privacy
28 not_anti_competitive.html](http://www.appleinsider.com/articles/10/06/02/jobs_iphone_ad_sdk_changes_for_user_privacy_not_anti_competitive.html)

189. From January 2010 until April 2010, Defendant Apple failed to provide notice to

1 Plaintiffs and Class Members of the activities of iPhone applications and affiliated ad networks
2 and/or web analytics vendors obtaining mobile device data, nor take appropriate action to cure
3 this security flaw; including but not limited to changing its privacy policy and licensing
4 agreements with any and all associated entities.

5 190. From July 2008 until April 2010, Defendant Apple provided no notice to
6 Plaintiffs and Class Members of Defendant Application Developer's Affiliates obtaining mobile
7 device data, such as their UDID and using such as a user's identifier of their mobile device data.

8 191. In April 2010 Defendant Apple changed its policy related to the collection of
9 mobile device data, aggregation of user data, and its use for web analytics:

10 192. Defendant Apple waited until June 21, 2010 to change its users' privacy policy.
11 Notice of such was provided only to those that attempted to update their apps via iTunes when a
12 page indicating Apple had changed its privacy policy, without specific reasons for any changes
13 non citation of specific changes. Users were notified only to the following:

iTunes Store Terms and Conditions have changed. Apple's
Privacy Policy

The changes we have made to the terms and conditions include the following

• Apple's Privacy Policy has changed in material ways. Please visit www.apple.com/legal/privacy or view below

17 "iAd Privacy Policy," (last accessed February 3, 2011), online:
18 <http://useyourloaf.com/blog/2010/6/21/iad-privacy-policy.html>

19 193. Defendant Apple's privacy policy failed to provide notice of Defendants'
20 Application Developer's Affiliates actions related to UDIDs and provided an opt out mechanism
21 that related only to Apple, and to opting out of Apple's iAds only:

22 • "Apple and its partners use cookies and other technologies in mobile advertising
23 services to control the number of times you see a given ad, deliver ads that relate to your
24 interests, and measure the effectiveness of ad campaigns. If you do not want to receive ads with
25 this level of relevance on your mobile device, you can opt out by accessing the following link on
26 your device: <http://oo.apple.com>. If you opt out, you will continue to receive the same number of
27 mobile ads, but they may be less relevant because they will not be based on your interests. You
28 may still see ads related to the content on a web page or in an application or based on other non-

1 personal information. This opt-out applies only to Apple advertising services and does not affect
2 interest-based advertising from other advertising networks.”

3 194. In May 2010, Defendant Flurry attempted to appease Defendant Apple and
4 released a new version of its SDK, citing its “privacy first initiation,” in an effort to comply with
5 Defendant Apple’s new policy related to use of mobile device data, such as UDIDs.

6 • “On the issue of device data,” Farago explains, “we are updating our analytics
7 service to comply with section 3.3.9 of the Apple 4.0 PLA. We will not collect device data.”

8 “Flurry: As Concerned About Privacy As Apple,” online:

9 [http://www.wirelessweek.com/News/2010/06/Policy-and-Industry-Flurry-Privacy-Apple-Safety-
10 and-Security/](http://www.wirelessweek.com/News/2010/06/Policy-and-Industry-Flurry-Privacy-Apple-Safety-and-Security/)

11 195. Defendant Flurry attempt through to revise its prior business activities by issuance
12 of its new policy actually provides insight, and confirmation of, its past data collection practices
13 by use of Plaintiffs and Class Members’ mobile device data, including their UDIDs:

14 • Defendant Flurry would now offer an opt-out switch for tracking. Many iTunes
15 applications do not have a privacy policy nor provide notice of any association with Defendant
16 Application Developer Affiliates, including Defendant Flurry, for users to be able to opt-out.

17 • Defendant Flurry would now provide the opt-out mechanism so users could delete
18 user data directly linked to a specific device. Defendant Flurry obtains data from 30-40,000 apps,
19 the cross application aggregation of user data linked specifically to a mobile devices’ UDID
20 provided substantial tracking data which Defendant Flurry continues to possess as noted,
21 Plaintiffs and Class Members will have no notice of Defendant Application Developer Affiliates
22 association with their applications, including Defendant Flurry.

23 • Defendant Flurry would now no longer obtain geographic data that was granular
24 enough to place a mobile device within close proximity to the user.

25 **G. Defendants’ Harmful Business Practices**

26 196. Defendants’ business practice unfairly wrests control from Plaintiffs and Class
27 Members who choose to block and delete any mobile tracking device on their mobile devices in
28 order to avoid being tracked. Plaintiffs and Class Members who are aware of being tracked may

1 attempt to delete any and all tracking devices periodically, believing that the new applications
2 they receive will not contain new unique identifiers, thus hindering the ability of advertising
3 networks to track their behavior across sites; however such shall be using a false theory. Using
4 databases overrides this attempt, with little available redress for users.

5 197. Defendants failed to disclose that its applied technologies, such as UDIDs provide
6 Defendants with the ability to surreptitiously intercept, access, and collect electronic
7 communications and information from unsuspecting Plaintiffs and the Class Members, obtaining
8 personal and private information, monitor their Internet activity, and create detailed personal
9 profiles based on such information.

10 198. Defendants intercepted Class Members' electronic communications for the
11 purpose of committing a tortious or criminal act, and violated the constitutional rights of
12 Plaintiffs and Class Members.

13 199. In all cases where some notice was provided, that notice was insufficient,
14 misleading, and inadequate. Consent under such circumstances was impossible.

15 200. Defendants failed to provide opt-out functionality for Plaintiffs and Class
16 Members, so that Plaintiffs and Class Members could set their security preferences.

17 201. Apple failed to implement a software program that would scramble the UDID,
18 creating a unique ID for each application.

19 202. In any case where the opportunity of 'opting out' of the Defendants service was
20 provided, such 'opt-out' rights were misleading, untrue, and deceptive.

21 203. In no case was the collection of all Internet communication data between the
22 consumer and the Internet halted or affected in any way. All data was still collected. The 'opt-
23 out' only affected what advertisements the consumer was shown. Thus, the provision of the
24 opportunity for opting-out was, itself, totally misleading.

25 204. Plaintiffs and the Class Members did not voluntarily disclose their personal and
26 private information to the Defendants' tracking, let alone their including their mobile device
27 surfing habits, to Defendants - and indeed never even knew that Defendant Application
28 developers Affiliates existed or conducted data collection and monitoring activities upon and

1 across its Plaintiffs' and Class Members' applications. Plaintiffs and the Class Members
2 provided such information, and had their Internet habits monitored, without their knowledge or
3 consent, and would not have consented having their personal and private information, including
4 their on-line profiles, used for Defendants' commercial gain.

5 205. Defendants did not obtain consent from Plaintiffs and Class Members for any
6 collection or use of any and all data derived in whole or part from use of a UDID and was not
7 allowed to decline consent at the time such statement was presented to the Class Members.

8 206. Defendants did not obtain consent from Plaintiffs and Class Members for any
9 disclosure of covered information to unaffiliated parties and was not allowed to decline consent
10 at the time such statement was presented to the Class Members.

11 207. Defendants intentionally accessed data, derived in whole part, from Plaintiffs' and
12 Class Members' mobile devices without authorization or exceeded authorized access to obtain
13 information from a protected mobile devices, involved in interstate communications.

14 208. Defendants sold, shared, and/or otherwise disclosed covered information of Class
15 Members to an unaffiliated party without first obtaining the consent of the Class Members to
16 whom the covered information related to.

17 209. At all relevant times, Plaintiffs' and Class Members' personal and private
18 information was electronically intercepted by and/or accessed by Defendants and transmitted to
19 it on a regular basis, without alerting Plaintiffs and Class Members in any manner. As a result,
20 Defendants was able to and did obtain data derived in whole or part from Plaintiffs' and Class
21 Members' mobile devices and/or intercept their electronic communications without
22 authorization. Defendants have obtained, compiled, and used this personal information for its
23 own commercial purposes.

24 210. Defendants intercepted Plaintiffs' and Class Members' electronic
25 communications for the purposes of obtaining mobile device data, using a UDID from Plaintiffs'
26 and Class Members' mobile devices; repeatedly accessing electronic communications without
27 Plaintiffs' and Class Members' knowledge and consent so as to profile such persons' web
28 browsing habits, secretly tracking Plaintiffs' and Class Members' activities on the Internet and

1 collecting personal information about consumers; and profiting from the use of the illegally
2 obtained information, all to Defendants' benefit and Plaintiffs' and Class Members' detriment.

3 211. Defendants intentionally intercepted, endeavored to intercept, or procured another
4 entity to intercept or endeavor to intercept the electronic communication of Plaintiffs and Class
5 Members.

6 212. Defendants have, either directly or by aiding, abetting and/or conspiring to do so,
7 knowingly, recklessly, or negligently disclosed, exploited, misappropriated and/or engaged in
8 widespread commercial usage of Plaintiffs' and the Class Members' mobile device data,
9 obtaining private and sensitive information for Defendants' own benefit from unauthorized use
10 of their UDID, without Plaintiffs' or the Class Members' knowledge, authorization, or consent.
11 Such conduct constitutes a highly offensive and dangerous invasion of Plaintiffs' and the Class
12 Members' privacy.

13 213. Defendants used and consumed the resources of the Plaintiffs' and Class
14 Members' mobile devices by gathering user information, adding such information to their mobile
15 database, and transferring such to Defendants.

16 214. Defendants caused harm and damages to Plaintiffs' and Class Members' mobile
17 devices finite resources, depleted and exhausted its memory, thus causing an actual inability to
18 use it for its intended purposes, and significant unwanted CPU activity, usage, and network
19 traffic, resulting in instability issues.

20 215. Defendants caused harm and damages to the Plaintiffs and Class Members
21 including but not limited to, consumption of their device's finite resources, memory depletion,
22 and bandwidth, which resulted in the actual inability to use if for its intended purposes.

23 216. Defendants' activity was not evident. Plaintiffs and Class Members assumed that
24 the issues related to hardware, Windows installation problems, or viruses, and resorted to
25 contacting technical support experts, or even buying a new mobile device because the existing
26 system mobile device posed privacy risks.

27 217. Defendants harmed Plaintiffs and Class Members by its actions which included,
28 but not limited to the following:

- a) Loss of valuable data by attempts to remove UDIDs and databases once discovered;
- b) Incurred economic losses accompanied by an interruption in service;
- c) Functionality of mobile device was interfered with, including an inability of applications visited once content was disabled;
- d) Information was deleted, otherwise made unavailable;
- e) Impaired the integrity and availability of data, programs and information.
- f) Mobile device bandwidth;
- g) Inability to resell the user's iPhone with a UDID associated with user's aggregate mobile device data.

218. Defendants impacted upon the Plaintiffs and Class Members ability to sell their mobile devices since the mobile device's UDID will have aggregated data linked to such device and be provided aggregated cross platform data. The new mobile device owner will then be provided tracking advertisements related to the past mobile device owner.

219. Plaintiffs and Class Members were personally injured, as that term is recognized within the cyber and technology industry, when Defendants intentionally, or in the alternative, negligently, obtained, processed, and disseminated content, obtained without authorization, invading Plaintiffs' and Class Members' right of privacy, which portrayed Plaintiffs and Class Members in a false light by publicly disclosing private facts by their intrusion upon seclusion of Plaintiffs' and Class Members' personal mobile browsing activity.

220. Defendants' impact upon the Plaintiffs' and Class Members' mobile devices was significant and a substantial reduction in available memory, processing power and database storage.

221. Defendants' interaction with the Plaintiffs' and Class Members' mobile device was not temporarily, but a permanent use of the mobile devices' storage resulting in a significant loss of use and potentially overwhelming the Plaintiffs' and Class Members' databases.

222. Plaintiffs and Class Members expended money, time, and resources investigating and attempting to mitigate their mobile devices diminished performance, in addition to

1 investigating and attempting to remove the Defendants' tracking mechanisms.

2 223. Plaintiffs and Class Members conducted a damage assessment once they became
3 aware of Defendants' practices, made the basis of this action, attempting to restore any affected
4 data, program, system or information.

5 224. Defendants' conduct caused outrage, mental suffering, harm, and humiliation to
6 Plaintiffs' and Class Members' privacy expectations.

7 225. Defendants intentionally disposed of the Plaintiffs' and Class Members' property
8 by using and intermeddling with their mobile devices so as to compare its condition, quality, and
9 value, disposing the Plaintiffs and Class Members of the use of their mobile devices for a
10 substantial time.

11 226. Defendants' Unique Device Identifier, remains identified with the Plaintiffs' and
12 Class Members' devices, thus the value of the device has been diminished, or now has no value
13 for resale.

14 227. Defendants' activities occurred throughout the United States, and have secretly
15 obtained personal and private information from Plaintiffs and the Class Members - a course of
16 action and a body of information that is protected from interception, access, and disclosure by
17 federal law.

18 228. Defendants used, interfered with, and intermeddled with Class Members'
19 ownership of their personal property, namely, their mobile devices, by, directly or indirectly,
20 secretly obtaining Plaintiffs' and Class Members' data derived from their UDID, secretly
21 accessing their mobile devices to obtain information contained in and enabled by the Unique
22 Device Identifier, and secretly collecting personal data and information regarding each Plaintiffs'
23 and Class Members' Internet surfing habits contained in electronic storage on his/her mobile
24 device.

25 229. Defendant Apple failed to disclose that its UDID software is used to track and
26 store information regarding consumers' Internet use and other forms of advertisements on
27 consumers' mobile devices based on such use. The installation of such tracking device would be
28 material to consumers in their decision whether to install the software offered by Defendant

1 Apple. Defendant's furthered their deceitful practices by storing the tracking files in locations on
2 consumers' mobile device that is rarely accessed by consumers.

3 230. Defendants' technology wrongfully monitored Internet users' activities at each
4 and every website users visited and the wrongfulness of this conduct is multiplied by the fact that
5 Defendants aggregates this information about users' habits across numerous applications and
6 unjustly enriched Defendants to the severe detriment of Plaintiffs and the Class Members.
7 Plaintiffs and the Class Members have been harmed, as they have been subjected to repeated and
8 unauthorized invasions of their privacy - violations which continue to this day.

9 231. Without remedy, Plaintiffs and Class Members will continue to be tracked by
10 dozens of companies — companies they've never heard of, companies they have no relationship
11 with, companies they would never choose to trust with their most private thoughts and reading
12 habits.

13 232. Defendants' privacy documents, which include, but are not limited to, its privacy
14 policy and terms of use, intentionally, or in the alternative, negligently, omit notice of any and all
15 of its activities made the basis of this action. Such omissions relate in whole or part, to
16 Defendant's intentional, or in the alternative, negligent, omission within its privacy documents to
17 any and all activities related to the basis of this action and notice of its activities with each
18 Affiliate.

19 233. Defendants' privacy documents fail to provide adequate notice that third parties,
20 made the basis of this action would be allowed access to personal behavioral data of their users,
21 including but not limited to, such data embedded with their applications, which in turn shares the
22 data with its marketing partners or corporate affiliates and subsidiaries, meaning that user
23 behavior will be profiled by any other entities with whom those sites may choose to share this
24 information. While Defendants' privacy documents state they do not share data with third
25 parties, but they do share data with affiliates, suggesting that they only share data with
26 companies under the same corporate ownership.

27 234. Defendant's privacy documents referenced the use of analytics, but state such is
28 used only for audience measurement and not behavioral ad-targeting.

1 235. Defendant Apple's privacy documents do not expressly state that if a user opts-
2 out that behavioral information will not be collected and shared, but only that the user will not
3 receive Internet based advertising content.

4 236. Defendant's privacy documents falsely imply some level of protection for the
5 user. Defendants' privacy documents are sufficiently vague so as to refrain from fully disclosing
6 information to their users about what information is collected through their applications and their
7 associated entities, how the information is used, and the purposes for the collection and use of
8 this information, negating the possibility for their users to provide informed and meaningful
9 consent to these practices. Without adequate notice and informed and meaningful user consent,
10 users had no control over their personal information, thus, the potential privacy dangers were not
11 readily apparent to most users.

12 237. Defendant's privacy documents require college-level reading skills for
13 comprehension and include substantial legalese, ambiguous and obfuscated language designed to
14 confuse, disenfranchise, and mislead the users.

15 238. Defendant's privacy documents incorporate a multitude of hedging and modality
16 markers so as to minimize their use of covert surveillance technology and data-gathering tools,
17 while sending mixed messages related to privacy controls, advising users that choosing to
18 exercise such controls would cause in whole, or part, diminished functionality of their
19 applications.

20 239. Defendant's privacy documents describe "associations," misleading the users
21 which interpret such to be associated corporate subsidiaries, withholding accurate information
22 that such includes other entities than advertising networks, such as: advertising networks, data
23 exchanges, traffic measurement service providers, marketing and analytic service providers.

24 240. Defendants' applications, and its tracking services, are owned by parent
25 companies that have many subsidiaries and fail to provide adequate information about third-party
26 information sharing, different than affiliate sharing, which is subject to more restrictions,
27 including opt-in or opt-out consent requirements. These restrictions are based upon the
28 heightened risk associated with sharing information with unrelated entities, which have different

1 incentives than the entity that collected the user data.

2 241. Defendants do not make adequate distinctions between sharing with affiliates,
3 contractors, and third parties, instead, vaguely stating that they do not share user data with
4 unrelated third parties and vaguely disclosing that they share data with affiliates. Users must
5 interpret an affiliate to be a third party, but given the actual usage of these terms of Affiliates'
6 privacy policies, that assumption would be mistaken.

7 242. Defendant do not users are unable to identify the corporate families to which its
8 applications belong, since they provide no privacy documents, which makes it difficult for a user
9 to discover exactly who such associated entities are, thus their practices are deceptive. A practice
10 is deceptive if it involves a representation, omission or practice that is likely to mislead a
11 consumer acting reasonably in the circumstances, to the consumer's detriment. The conflicting
12 statements in the privacy policies would most likely confuse or mislead a reasonable consumer.
13 The confusion would also likely be to their detriment, as surveys indicate that users do not want
14 companies to collect data about them without permission.

15 243. Defendant's privacy documents discuss that the data collection practices of
16 entities associated with their corporations are outside the coverage of their privacy policies. This
17 appears to be an attempt to create a critical loophole compounding their attempts to violate the
18 privacy protection of their users.

19 244. Defendant's privacy documents fail to adhere to an adequate notice and choice
20 regime, predicated on user choice, and informed by privacy policies. Defendant's privacy
21 documents provided nuanced situations that created conditional yes or no answers to these basic
22 questions about a site's data collection and sharing practices, thus it is unclear how an average
23 user could ever understand these practices since the nuances were not explained in the privacy
24 policy. Choice, therefore, cannot be inferred.

25 245. Defendant Apple's privacy documents carefully attempt to parse the definitions of
26 phrases related to their tracking activity. Their privacy documents are more nuanced than such
27 categorized analysis allows for, embedding any and all purposes for its use of surveillance
28 technology into the user's mobile device hardware, use of user's mobile device hardware to store

1 data, use of technology to allow the perpetual mobile device tracking and surveillance of any and
2 all mobile device Internet activity of the Defendant Apple users as evidenced by the attempt of
3 Defendant Apple to hide its covert activity by referring to their use of "other technologies," or
4 "similar technologies" than UDID tracking which would have perpetual existence on a user's
5 mobile device.

6 246. Defendant's privacy documents fail to provide notice that their data storage
7 practices as they relate to the period for which user data is stored, have no term period, and are
8 indefinite.

9 247. Defendant's privacy documents' verbiage was deceptive by design. This
10 deception is especially troubling when compared with the obligation imposed upon their mobile
11 device visitors to download, read, and comprehend the vast amount of documents required to
12 protect one's mobile device privacy, complicated by the cumulative effect of such task.

13 248. In addition to downloading, reading and comprehending all of Defendant Apple's
14 and Defendant Application Developers privacy documents, its users would be required to locate
15 and attempt to do the same for Defendant Application Developers Affiliates. To accentuate the
16 improbability of completing this task though, Plaintiff and Class Members were not provided
17 information of the identity of Defendant Application Developer's Affiliates, nor its association
18 with Apple.

19 249. Defendant Application Developer Affiliates privacy documents, reveal omissions
20 related to in whole or part, intentionally, or in the alternative negligently, omitting within the
21 Defendant Application Developers Affiliate privacy documents to any and all activities related to
22 the basis of this action and notice of its activities with Defendant Application Developers.

23 250. Defendants mobile device privacy protection was premised upon imposed
24 requirement to download, read, and comprehend the accumulation of all privacy documents of
25 all Defendants.

26 251. A millisecond was the time allotted for the Plaintiffs and Class Members
27 downloading a Defendant Apple iTunes Store application, before Defendant Application
28 Developers and Defendant Application Developer Affiliates intentionally, and without user's

1 authorization and consent, had Defendant Apple transmit, and/or allowed access to, data related
2 to whole or part, from the Plaintiffs' and Class Members' UDID. Such occurred without the
3 benefit of being advised of the association between Defendant Application Developer and its
4 Application Developer Affiliate, provided adequate time to access, read, and comprehend the
5 Terms of Service/Use and Privacy Policy for all Defendants which had privacy policies. While
6 only the most technical savvy mobile device users were familiar with UDIDs, a finite amount of
7 individuals even knew about "UDID," let alone could possibly comprehend the technical aspects
8 inherent within the Defendants' privacy documents.

9 Defendants sought a virtual "Forbidden Fruit", and it was Apple's UDID:
10 *"But of the fruit of the tree which is in the midst of the garden, God hath said, Ye shall*
11 *not eat of it, neither shall ye touch it, lest ye die"*
12 *Genesis 3:3*

12 **CLASS ALLEGATIONS**
13 **Allegations as to Class Certification**

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

17 a)U.S. Resident Class: All persons residing in the United States who have downloaded
18 and used one of the Defendants' apps on their iPhone, iPad, or iTouch from July 10, 2008
19 to the date of the filing of this complaint.

20 b)Injunctive Class: All persons after the date of the filing of this complaint, residing in
21 the United States, who have downloaded and used one of the Defendants' apps on their
22 iPhone, iPad, or iTouch after the date of the filing of this complaint.

23
24 253. The Class action period, (the "Class Period"), pertains to the dates, July 10, 2008
25 to the date of Class certification.

26 254. Plaintiffs reserve the right to revise this definition of the Class based on facts
27 learned in the course of litigation of this matter.

28 255. On behalf of the U.S. Resident Class, Plaintiffs seek equitable relief, damages

1 and injunctive relief pursuant to:

- 2 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- 3 b) Electronic Communications Privacy Act, 18 U.S.C. § 2510;
- 4 c) California's Computer Crime Law, Penal Code § 502;
- 5 d) California's Invasion of Privacy Act, Penal Code § 630;
- 6 e) Consumer Legal Remedies Act, ("CLRA") California Civil Code § 1750;
- 7 f) Unfair Competition, California Business and Professions Code § 17200;
- 8 g) Breach of Contract;
- 9 h) Conversion;
- 10 i) Trespass to Personal Property / Chattels; and
- 11 j) Unjust Enrichment

12 256. On behalf of the Injunctive Class, Plaintiffs seek only injunctive relief.

13 257. **Persons Excluded From Classes:** Subject to additional information obtained
14 through further investigation and discovery, the foregoing definition of the Class may be
15 expanded or narrowed by amendment or amended complaint. Specifically excluded from the
16 proposed Class are Defendants, their officers, directors, agents, trustees, parents, children,
17 corporations, trusts, representatives, employees, principals, servants, partners, joint ventures, or
18 entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities
19 related to or affiliated with Defendants and/or their officers and/or directors, or any of them; the
20 Judge assigned to this action, and any member of the Judge's immediate family.

21 258. Plaintiffs reserve the right to revise these Class definitions of the Classes based on
22 facts they learn during discovery.

23 259. **Numerosity:** The members of the Class are so numerous that their individual
24 joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that the
25 proposed Class contains tens of thousands of members. The precise number of Class Members is
26 unknown to Plaintiffs. The true number of Class Members is known by Defendants, however
27 and, thus, Class Members may be notified of the pendency of this action by first Class mail,
28 electronic mail, and by published notice. Upon information and belief, Class Members can be

1 identified by the electronic records of Defendants.

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

- 7 a) What was the extent of Defendants' business practice of transmitting,
8 accessing, collecting, monitoring, and remotely storing user's Unique Device
9 Identifiers ("UDIDs") and how did it work?
- 10 b) What information did Defendants collect from its business practices of
11 transmitting, accessing, collecting, monitoring, and remotely storing user's
12 Unique Device Identifiers ("UDIDs"), and what did it do with that
13 information?
- 14 c) Whether users, by virtue of their downloading the application, had pre-
15 consented to the operation of Defendant's business practices of transmitting,
16 accessing, collecting, monitoring, and remotely storing user's Unique Device
17 Identifiers ("UDIDs");
- 18 d) Was there adequate notice, or *any* notice, of the operation of Defendants'
19 business practices of transmitting, accessing, collecting, monitoring, and
20 remotely storing user's Unique Device Identifiers ("UDIDs") provided to
21 Plaintiffs and Class Members?
- 22 e) Was there reasonable opportunity to decline the operation of Defendants'
23 business practices of transmitting, accessing, collecting, monitoring, and
24 remotely storing user's Unique Device Identifiers ("UDIDs") provided to
25 Plaintiffs and Class Members?
- 26 f) Did Defendant's and business practices of obtaining, collecting, monitoring,
27 and remotely storing user's Unique Device Identifiers ("UDIDs") disclose,
28 intercept, and transmit personally identifying information, or sensitive
 identifying information, or personal information?
- g) Whether Defendants' devised and deployed a scheme or artifice to defraud or
 conceal from Plaintiffs and the Class Members Defendants' ability to, and
 practice of, intercepting, accessing, and manipulating, for its own benefit,
 personal information, and tracking data from Plaintiffs' and the Class'
 personal mobile device via the ability to; track their mobile device by
 tracking its UDID on their mobile device;
- h) Whether Defendants engaged in deceptive acts and practices in, connection
 with its undisclosed and systemic practice of transmitting, accessing and/or
 disclosing unique identifiers, tracking data, and personal information on
 Plaintiffs' and the Class' personal mobile device and using that data to track
 and profile Plaintiffs' and the Class Member's Internet activities and personal
 habits, proclivities, tendencies, and preferences for Defendants' use and

benefit;

- i) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, and remotely storing user's Unique Device Identifiers ("UDIDs") violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030?
- j) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510?
- k) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") violate the Violations of California's Computer Crime Law, Penal Code § 502;
- l) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") violate the Violations of the California Invasion of Privacy Act, Penal Code § 630;
- m) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") violate the Violations of the Consumer Legal Remedies Act, ("CLRA") California Civil Code § 1750;
- n) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") violate the Violation of Unfair Competition, California Business and Professions Code § 17200;
- o) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") involve a Breach of Contract;
- p) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") involve a Conversion;
- q) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") involve a Trespass to Personal Property / Chattels;
- r) Did the implementation of Defendants' business practices of transmitting, accessing, collecting, monitoring, remotely storing user's Unique Device Identifiers ("UDIDs") result in Unjust Enrichment;
- s) Are any of the Defendants liable under a theory of aiding and abetting one (1) more of the remaining Defendants for violations of the statutes listed herein?
- t) Are the Defendants' liable under a theory of civil conspiracy for violations of the statutes listed herein?
- u) Are the Defendants' liable under a theory of unjust enrichment for violations of the statutes listed herein?

- 1 v) Whether Defendants' participated in and/or committed or is responsible for
2 violation of law(s) complained of herein;
- 3 w) Are Class Members entitled to damages as a result of the implementation of
4 Defendants' marketing scheme, and, if so, what is the measure of those
5 damages?
- 6 x) Whether Plaintiffs and members of the Class have sustained damages as a
7 result of Defendants' conduct, and, if so, what is the appropriate measure of
8 damages;
- 9 y) Whether Plaintiffs and members of the Class are entitled to declaratory and/or
10 injunctive relief to enjoin the unlawful conduct alleged herein; and
- 11 z) Whether Plaintiffs and members of the Class are entitled to punitive damages,
12 and, if so, in what amount?

13 261. **Typicality:** Plaintiff's claims are typical of the claims of all of the other members
14 of the Class, because his claims are based on the same legal and remedial theories as the claims
15 of the Class and arise from the same course of conduct by Defendants.

16 262. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the
17 interests of the members of the Class. Plaintiffs have retained counsel highly experienced in
18 complex consumer Class action litigation, and Plaintiffs intend to prosecute this action
19 vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

20 263. **Superiority:** A Class action is superior to all other available means for the fair
21 and efficient adjudication of this controversy. The damages or other financial detriment suffered
22 by individual Class Members is relatively small compared to the burden and expense that would
23 be entailed by individual litigation of their claims against the Defendants. It would thus be
24 virtually impossible for the Class, on an individual basis, to obtain effective redress for the
25 wrongs done to them. Furthermore, even if Class Members could afford such individualized
26 litigation, the court system could not. Individualized litigation would create the danger of
27 inconsistent or contradictory judgments arising from the same set of facts. Individualized
28 litigation would also increase the delay and expense to all parties and the court system from the
issues raised by this action. By contrast, the Class action device provides the benefits of
adjudication of these issues in a single proceeding, economies of scale, and comprehensive
supervision by a single court, and presents no unusual management difficulties under the
circumstances here.

1 264. In the alternative, the Class may be also certified because:

- 2 a) the prosecution of separate actions by individual Class Members would create
3 a risk of inconsistent or varying adjudication with respect to individual Class
4 Members that would establish incompatible standards of conduct for the
5 Defendants;
- 6 b) the prosecution of separate actions by individual Class Members would create
7 a risk of adjudications with respect to them that would, as a practical matter,
8 be dispositive of the interests of other Class Members not parties to the
9 adjudications, or substantially impair or impede their ability to protect their
10 interests; and/or
- 11 c) Defendants have acted or refused to act on grounds generally applicable to the
12 Class thereby making appropriate final declaratory and/or injunctive relief
13 with respect to the members of the Class as a whole.

14 265. The claims asserted herein are applicable to all persons throughout the United
15 States that meet the class definition & class period.

16 266. The claims asserted herein are based on Federal law and California law, which is
17 applicable to all Class Members throughout the United States.

18 267. Adequate notice can be given to Class Members directly using information
19 maintained in Defendants' records or through notice by publication.

20 268. Damages may be calculated from the information maintained in Defendants'
21 records, so that the cost of administering a recovery for the Class can be minimized. The amount
22 of damages is known with precision from Defendants' records.

23
24
25
26
27
28

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

29 269. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

30 270. Plaintiffs assert this claim against each and every Defendant named herein in this
31 complaint on behalf of themselves and the Class.

32 271. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA,"
33 regulates fraud and relates activity in connection with computers, and makes it unlawful to
34 intentionally access a computer used for interstate commerce or communication, without
35 authorization or by exceeding authorized access to such a computer, thereby obtaining

1 information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

2 272. Defendants violated 18 U.S.C. § 1030 by intentionally accessing Plaintiffs' and
3 Class Members' mobile computing device, without authorization by exceeding access, thereby
4 obtaining information from such a protected device.

5 273. At all relevant times, Defendants engaged in business practices of transmitting
6 code from within the Plaintiffs' and Class Members' downloaded iPhone Applications so as to
7 access their mobile devices to obtain a UDID and mobile device data. Such acts were conducted
8 without authorization and consent of the Plaintiffs and Class Members.

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

11 275. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(i), makes it
12 unlawful to "knowingly cause[s] the transmission of a program, information, code, or command
13 and as a result of such conduct, intentionally cause[s] damage without authorization, to a
14 protected computer," of a loss to one or more persons during any one-year period aggregating at
15 least \$5,000 in value.

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

18 277. Defendants violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing a
19 Plaintiffs' mobile computing device, without authorization or by exceeding access, thereby
20 obtaining information from such a protected mobile computing device.

21 278. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the
22 transmission of a command embedded within their webpage's, downloaded to Plaintiffs' mobile
23 computing device, which are protected mobile computing devices as defined in 18 U.S.C. §
24 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs' viewing habits, Defendants
25 intentionally caused damage without authorization to those Plaintiffs' mobile computing devices
26 by impairing the integrity of the computer.

27 279. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing
28 Plaintiffs' and Class Members' protected mobile computing devices without authorization, and

1 as a result of such conduct, recklessly caused damage to Plaintiffs' and Class Members' mobile
2 computing devices by impairing the integrity of data and/or system and/or information.

3 280. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing
4 Plaintiffs' and Class Members' protected mobile computing devices without authorization, and
5 as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

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

9 282. Plaintiffs have suffered loss by reason of these violations, as defined in 18 U.S.C.
10 § 1030(e)(11), by the "reasonable cost ... including the cost of responding to an offense,
11 conducting a damage assessment, and restoring the data, program, system, or information to its
12 condition prior to the offense, and any revenue lost, cost incurred, or other consequential
13 damages incurred because of interruption of service."

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

18 284. As a result of these takings, Defendants' conduct has caused a loss to one or more
19 persons during any one-year period aggregating at least \$5,000 in value in real economic
20 damages.

21 285. Plaintiffs and Class Members have additionally suffered loss by reason of these
22 violations, including, without limitation, violation of the right of privacy.

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

28

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

1
2
3 287. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

4 288. Plaintiffs assert this claim against each and every Defendant named herein in this
5 complaint on behalf of themselves and the Class.

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

11 290. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring and/or
12 intercepting, by device or otherwise, Plaintiffs' and Class Members' electronic communications,
13 without knowledge, consent, or authorization.

14 291. At all relevant times, Defendants engaged in business practices of intercepting
15 the Plaintiffs' and Class Members' electronic communications which included endeavoring to
16 intercept the transmission of a UDID from within their mobile device. Once the Defendants
17 obtained the UDID they used such to aggregate mobile device data of the Plaintiffs and Class
18 Members as they used their mobile device, browsed the Internet, and activated downloaded
19 iPhone applications.

20 292. The contents of data transmissions from and to Plaintiffs' and Class Members'
21 personal computers constitute "electronic communications" within the meaning of 18 U.S.C.
22 §2510.

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

25 294. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting,
26 endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept
27 Plaintiffs' electronic communications.

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

5 296. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or
6 endeavoring to use, the contents of Plaintiffs' electronic communications, knowing or having
7 reason to know that the information was obtained through the interception of Plaintiffs'
8 electronic communications.

9 297. Defendants' intentional interception of these electronic communications without
10 Plaintiffs' or Class Members' knowledge, consent, or authorization was undertaken without a
11 facially valid court order or certification.

12 298. Defendants intentionally used such electronic communications, with knowledge,
13 or having reason to know, that the electronic communications were obtained through
14 interception, for an unlawful purpose.

15 299. Defendants unlawfully accessed and used, and voluntarily disclosed, the contents
16 of the intercepted communications to enhance their profitability and revenue through
17 advertising. This disclosure was not necessary for the operation of Defendants' system or to
18 protect Defendants' rights or property.

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

22 301. Defendants are liable directly and/or vicariously for this cause of action.
23 Plaintiffs therefore seek remedy as provided for by 18 U.S.C. §2520, including such preliminary
24 and other equitable or declaratory relief as may be appropriate, damages consistent with
25 subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a
26 reasonable attorney's fee and other litigation costs reasonably incurred.

27 302. Plaintiffs and Class Members have additionally suffered loss by reason of these
28 violations, including, without limitation, violation of the right of privacy.

1 309. Pursuant to California Penal Code § 502(b)(6), "Data means a representation of
2 information, knowledge, facts, concepts, computer software, computer programs or instructions.
3 Data may be in any form, in storage media, or as stored in the memory of the computer or in
4 transit or presented on a display device."

5 310. Defendants have violated California Penal Code § 502(c)(1) by knowingly
6 accessing and without permission, altering, and making use of data from Plaintiffs' mobile
7 devices in order to devise and execute business practices to deceive Plaintiffs and Class
8 members into surrendering private electronic communications and activities for Defendants'
9 financial gain, and to wrongfully obtain valuable private data from Plaintiffs.

10 311. Defendants have violated California Penal Code § 502(c)(2) by knowingly
11 accessing and without permission, taking, or making use of data from Plaintiffs' mobile devices.

12 312. Defendants have violated California Penal Code § 502(c)(3) by knowingly and
13 without permission, using and causing to be used Plaintiffs' mobile computing devices'
14 services.

15 313. Defendants have violated California Penal Code § 502(c)(6) by knowingly and
16 without permission providing, or assisting in providing, a means of accessing Plaintiffs'
17 computers, computer system, and/or computer network.

18 314. Defendants have violated California Penal Code § 502(c)(7) by knowingly and
19 without permission accessing, or causing to be accessed, Plaintiffs' computer, computer system,
20 and/or computer network.

21 315. California Penal Code § 502(j) states: "For purposes of bringing a civil or a
22 criminal action under this section, a person who causes, by any means, the access of a computer,
23 computer system, or computer network in one jurisdiction from another jurisdiction is deemed
24 to have personally accessed the computer, computer system, or computer network in each
25 jurisdiction."

26 316. Plaintiffs have also suffered irreparable injury from these unauthorized acts of
27 disclosure, to wit: their personal, private, and sensitive electronic data was obtained and used by
28

1 Defendants. Due to the continuing threat of such injury, Plaintiffs have no adequate remedy at
2 law, entitling Plaintiffs to injunctive relief.

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

5 318. As a direct and proximate result of Defendants' unlawful conduct within the
6 meaning of California Penal Code § 502, Defendants have caused loss to Plaintiffs in an amount
7 to be proven at trial. Plaintiffs are also entitled to recover their reasonable attorneys' fees
8 pursuant to California Penal Code § 502(e).

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

11 **Fourth Cause of Action**
12 **Violation of the California Invasion of Privacy Act**
13 **Penal Code § 630 *et seq.***

14 320. Plaintiffs incorporate the above allegations by reference as if set forth herein at
15 length.

16 321. Plaintiffs assert this claim against each and every California Defendant named
17 herein in this complaint on behalf of themselves and the Class.

18 322. California Penal Code section 630 provides, in part:

19 "Any person who, . . . or who willfully and without the consent of all parties to the
20 communication, or in any unauthorized manner, reads, or attempts to read, or to learn the
21 contents or meaning of any message, report, or communication while the same is in transit or
22 passing over any wire, line, or cable, or is being sent from, or received at any place within this
23 state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in
24 any way, any information so obtained, or who aids, agrees with, employs, or conspires with any
25 person or persons to unlawfully do, or permit, or cause to be done any of the acts or things
26 mentioned above in this section, is punishable . . ."

27 323. At all relevant times, Defendants business practices of accessing the mobile
28 device data of the Plaintiffs and Class Members was without authorization and consent;
including but not limited to obtaining any and all communications involving their UDID.

1 324. On information and belief, each Plaintiff, and each Class Member, during one or
2 more of their interactions on the Internet during the Class Period, communicated with one or
3 more web entities based in California, or with one or more entities whose servers were located
4 in California.

5 325. Communications from the California web-based entities to Plaintiffs and Class
6 Members were sent from California. Communications to the California web-based entities from
7 Plaintiffs and Class Members were sent to California.

8 326. Plaintiffs and Class Members did not consent to any of the Defendants' actions
9 in intercepting, reading, and/or learning the contents of their communications with such
10 California-based entities.

11 327. Plaintiffs and Class Members did not consent to any of the Defendants' actions
12 in using the contents of their communications with such California-based entities.

13 328. Defendants are not a "public utility engaged in the business of providing
14 communications services and facilities . . ."

15 329. The actions alleged herein by the Defendants were not undertaken: "for the
16 purpose of construction, maintenance, conduct or operation of the services and facilities of the
17 public utility."

18 330. The actions alleged herein by the Defendants were not undertaken in connection
19 with: "the use of any instrument, equipment, facility, or service furnished and used pursuant to
20 the tariffs of a public utility.

21 331. The actions alleged herein by the Defendants were not undertaken with respect to
22 any telephonic communication system used for communication exclusively within a state,
23 county, city and county, or city correctional facility.

24 332. The Defendants directly participated in the interception, reading, and/or learning
25 the contents of the communications between plaintiffs, Class Members and California-based
26 web entities.

1 information and email privacy but were unlikely to be aware of the manner in which Defendant
2 failed to fulfill its commitments to respect consumers' privacy. Defendant is therefore in
3 violation of the "unfair" prong of the UCL.

4 341. Defendant's acts and practices were fraudulent within the meaning of the UCL
5 because they are likely to mislead the members of the public to whom they were directed.

6 342. Plaintiffs, on behalf of themselves and on behalf of each member of the Class,
7 shall seek individual restitution, injunctive relief, and other relief allowed under the UCL as the
8 Court deems just and proper.

9 343. This cause of action is brought pursuant to the California Consumers Legal
10 Remedies Act, Cal. Civ. Code § 1750 *et seq.* (the "CLRA"). This cause of action does not seek
11 monetary damages at this point, but is limited solely to injunctive relief. Plaintiff will amend
12 this Class Action Complaint to seek damages in accordance with the CLRA after providing the
13 Defendants with notice pursuant to California Civil Code § 1782.

14 344. At this time, Plaintiffs seek only injunctive relief under this cause of action.
15 Pursuant to California Civil Code, Section 1782, Plaintiffs will notify Defendant in writing of
16 the particular violations of Civil Code, Section 1770 and demand that Defendant rectify the
17 problems associated with its behavior detailed above, which acts and practices are in violation
18 of Civil Code § 1770.

19 345. If Defendant fails to respond adequately to Plaintiff's above-described demand
20 within 30 days of Plaintiff's notice, pursuant to California Civil Code, Section 1782(b),
21 Plaintiffs will amend the complaint to request damages and other relief, as permitted by Civil
22 Code, Section 1780.

23 **Sixth Cause of Action**
24 **Unfair Competition**
California Business and Professions Code § 17200

25 346. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

26 347. In violation of California Business and Professions Code § 17200 *et seq.*,
27 Defendant's conduct in this regard is ongoing and includes, but is not limited to, unfair,
28 unlawful and fraudulent conduct.

1 348. Defendant misled consumers by continuously and falsely representing during the
2 Class Period that they would not make personally identifiable information available to third
3 parties as alleged herein.

4 349. At all relevant times, Defendants' business practices of merging Defendant
5 Apple's mobile devices and Defendant Application Developer's applications and services to
6 Plaintiffs and Class Members by way of, *inter alia*, commercial marketing and advertising,
7 misrepresented and/or omitted the truth about the extent to which Defendants would obtain and
8 share Plaintiffs' and Class Members' sensitive and personal identifiable information with third
9 parties.

10 350. Defendants engaged in these unfair and fraudulent practices to increase their
11 profits. Had Plaintiff know that Defendants would share his personally identifiable information
12 with third parties; he would not have purchased or used the Defendants' services, which in turn,
13 forced him to relinquish, for free, valuable personal information.

14 351. By engaging in the above-described acts and practices, Defendant has committed
15 one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs
16 and the Class have suffered injury-in-fact and have lost money and/or property—specifically,
17 personal information and/or registration fees.

18 352. Defendant's business acts and practices are unlawful, in part, because they
19 violate California Business and Professions Code § 17500, et seq., which prohibits false
20 advertising, in that they were untrue and misleading statements relating to Defendant's
21 performance of services and with the intent to induce consumers to enter into obligations
22 relating to such services, and regarding statements Defendant knew were false or by the exercise
23 of reasonable care Defendant should have known to be untrue and misleading.

24 353. Defendant's business acts and practices are also unlawful in that they violate the
25 California Consumer Legal Remedies Act, California Civil Code, Sections 1647, et seq., 1750,
26 et seq., and 3344, California Penal Code, section 502, and Title 18, United States Code, Section
27 1030. Defendant is therefore in violation of the "unlawful" prong of the UCL.

28

1 373. Defendants engaged in deception and concealment in order to gain access to
2 Plaintiffs' and Class Members' mobile devices.

3 374. Defendants undertook the following actions with respect to Plaintiffs' and Class
4 Members' mobile devices:

- 5 a) Defendants accessed and obtained control over the user's mobile device;
- 6 b) Defendants obtained user's UDID from a tracking code the user's mobile
7 device;
- 8 c) Defendants used the user's UDID to obtain without notice or consent, mobile
9 browsing activities of the mobile device, and outside of the control of the
10 owner of the mobile device.

11 375. All these acts described above were acts in excess of any authority any user
12 granted when he or she visited the Defendant Apple's iTunes Store and downloaded one (1) or
13 more of the Defendant application and none of these acts was in furtherance of users viewing the
14 Defendant applications. By engaging in deception and misrepresentation, whatever authority or
15 permission Plaintiffs and Class Members may have granted to Defendant Apple and/or
16 Defendant Application Developers was visited.

17 376. Defendants' installation and operation of its program used, interfered, and/or
18 intermeddled with Plaintiffs' and Class Members' mobile devices. Such use, interference and/or
19 intermeddling was without Class Members' consent or, in the alternative, in excess of Plaintiffs'
20 and Class Members' consent.

21 377. Defendants' installation and operation of its program constitutes trespass,
22 nuisance, and an interference with Class Members' chattels, to wit, their mobile devices.

23 378. Defendants' installation and operation of its program impaired the condition and
24 value of Class Members' mobile devices.

25 379. Defendants' trespass to chattels, nuisance, and interference caused real and
26 substantial damage to Plaintiffs and Class Members.

27 380. As a direct and proximate result of Defendants' trespass to chattels, nuisance,
28 interference, unauthorized access of and intermeddling with Plaintiffs' and Class Members'

1 property, Defendants has injured and impaired in the condition and value of Class Members'
2 mobile devices, as follows:

- 3 a) By consuming the resources of and/or degrading the performance of
4 Plaintiffs' and Class Members' mobile devices (including space, memory,
5 processing cycles, Internet connectivity, and unauthorized use of their
6 bandwidth);
- 7 b) By diminishing the use of, value, speed, capacity, and/or capabilities of
8 Plaintiffs' and Class Members' mobile devices;
- 9 c) By devaluing, interfering with, and/or diminishing Plaintiffs' and Class
10 Members' possessory interest in their mobile devices;
- 11 d) By altering and controlling the functioning of Plaintiffs' and Class Members'
12 mobile devices;
- 13 e) By infringing on Plaintiffs' and Class Members' right to exclude others from
14 their mobile devices;
- 15 f) By infringing on Plaintiffs' and Class Members' right to determine, as owners
16 of/or their mobile devices, which programs should be installed and operating
17 on their mobile devices;
- 18 g) By compromising the integrity, security, and ownership of Class Members'
19 mobile devices; and
- 20 h) By forcing Plaintiffs and Class Members to expend money, time, and
21 resources in order to remove the program installed on their mobile devices
22 without notice or consent.

23
24 **Eleventh Cause of Action**
25 **Unjust Enrichment**

26 381. Plaintiff hereby incorporates by reference the allegations contained in all of the
27 paragraphs of this complaint.

28 382. By engaging in the conduct described in this Complaint, Defendants have
knowingly obtained benefits from the Plaintiff under circumstances that make it inequitable and
unjust for Defendants to retain them.

383. Defendants have received a benefit from Plaintiff and Defendants have received
and retain money from advertisers and other third-parties as a result of sharing the personal
information of Defendants' users' with those advertisers without Plaintiffs' knowledge or
consent as alleged in this Complaint.

384. Plaintiff did not expect that Defendants would seek to gain commercial advantage
from third-parties by using his personal information without his consent.

- 1 f) Unfair Competition, California Business and Professions Code § 17200;
2 g) Breach of Contract;
3 h) Conversion;
4 i) Trespass to Personal Property / Chattels; and
5 j) Unjust Enrichment

6 C. As applicable to the Classes *mutatis mutandis*, awarding injunctive and equitable
7 relief including, *inter alia*: (i) prohibiting Defendants from engaging in the acts
8 alleged above; (ii) requiring Defendants to disgorge all of its ill-gotten gains to
9 Plaintiffs and the other Class Members, or to whomever the Court deems
10 appropriate; (iii) requiring Defendants to delete all data surreptitiously or
11 otherwise collected through the acts alleged above; (iv) requiring Defendants to
12 provide Plaintiffs and the other Class Members a means to easily and permanently
13 decline any participation in any data collection activities; (v) awarding Plaintiffs
14 and Class Members full restitution of all benefits wrongfully acquired by
15 Defendants by means of the wrongful conduct alleged herein; and (vi) ordering an
16 accounting and constructive trust imposed on the data, funds, or other assets
17 obtained by unlawful means as alleged above, to avoid dissipation, fraudulent
18 transfers, and/or concealment of such assets by Defendants;

13 D. Award damages, including statutory damages where applicable, to Plaintiffs and
14 Class Members in an amount to be determined at trial;

15 E. Award restitution against Defendants for all money to which Plaintiffs and the
16 Classes are entitled in equity;

17 F. Restrain Defendants, their officers, agents, servants, employees, and attorneys,
18 and those in active concert or participation with them from continued access,
19 collection, and transmission of Plaintiffs' and Class Members' personal
20 information via preliminary and permanent injunction;

19 G. Award Plaintiffs and the Classes:

20 a) their reasonable litigation expenses and attorneys' fees;

21 b) pre- and post-judgment interest, to the extent allowable;

22 c) restitution, disgorgement and/or other equitable relief as the Court deems
23 proper;

24 d) compensatory damages sustained by Plaintiffs and all others similarly situated
25 as a result of Defendants' unlawful acts and conduct;

26 e) statutory damages, including punitive damages;

27 f) permanent injunction prohibiting Defendants from engaging in the conduct
28 and practices complained of herein;

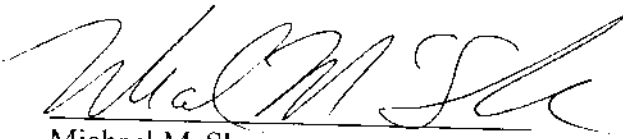
H. For such other and further relief as this Court may deem just and proper.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY TRIAL DEMAND

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

Dated this 15th day of February 2011


By: Michael McShane

Audet & Partners, LLP
Michael McShane
Jonas P. Mann
221 Main Street
Suite 1460
San Francisco, CA 94105
Telephone: (415) 568-2555

Lockridge Grindal Nauen P.L.L.P.
Richard Lockridge
Robert Shelquist
Suite 2200
100 Washington Avenue South
Minneapolis, Minnesota 55401
Telephone: (612) 339-6900

Law Office of Joseph H. Malley
Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100