

1 Alan Himmelfarb - SBN 90480  
2 KAMBEREDELSON, LLC  
3 2757 Leonis Boulevard  
4 Vernon, California 90058  
5 Telephone: (323) 585-8696

6 Joseph H. Malley  
7 TX SBN: 12865900  
8 LAW OFFICE OF JOSEPH H. MALLEY, P.C.  
9 1045 North Zang Boulevard  
10 Dallas, Texas 75208  
11 Ph. (214) 943-6100  
12 Fax (214) 943-6170

13 *Counsel for Plaintiffs*

14 **IN THE UNITED STATES DISTRICT COURT**  
15 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
16 **SAN JOSE DIVISION**

17 SEAN LANE, MOHANNAED SHEIKHA, SEAN  
18 MARTIN, , ALI SAMMOUR, MOHAMMAED  
19 ZIDAN, SARA KARROW, COLBY HENSON,  
20 DENTON HUNKER, FIRAS SHEIKHA, HASSEN  
21 SHEIKHA, LINDA STEWART, TINA TRAN,  
22 MATTHEW SMITH, ERICA PARNELL, JOHN  
23 CONWAY, AUSTIN MUHS, PHILLIP HUERTA,  
24 ALICIA HUNKER, individuals, on behalf of  
25 themselves and all others similarly situated, and  
26 MEGAN LYNN HANCOCK, a minor, by and  
27 through her parent REBECCA HOLEY,

28 Plaintiffs

v.

FACEBOOK, INC., a Delaware Corporation,  
BLOCKBUSTER, INC., a Delaware Corporation,  
FANDANGO, INC., a Delaware Corporation,  
HOTWIRE, INC., a Delaware Corporation, STA  
TRAVEL, INC., a Delaware Corporation,  
OVERSTOCK.COM, INC., a Delaware  
Corporation, ZAPPOS.COM, INC., a Delaware  
Corporation. GAMEFLY, INC., a Delaware  
Corporation. AND JOHN DOES 1-40,  
corporations

Defendants.

CASE No.

JURY DEMAND

COMPLAINT FOR:

1. Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510; AND
2. Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030; AND
3. Violation of Video Privacy Protection Act, 18 U.S.C. § 2710; AND
4. Violation of California's Consumer Legal Remedies Act, California Civil Code § 1750; AND
5. Violation of California's Computer Crime Law, Penal Code § 502

**CLASS ACTION COMPLAINT**

Plaintiffs, SEAN LANE, MOHANNAED SHEIKHA, SEAN MARTIN,, ALI

1 SAMMOUR, MOHAMMAED ZIDAN, SARA KARROW, COLBY HENSON, DENTON  
2 HUNKER, FIRAS SHEIKHA, HASSEN SHEIKHA, LINDA STEWART, TINA TRAN,  
3 MATTHEW SMITH, ERICA PARNELL, JOHN CONWAY, AUSTIN MUHS, PHILLIP  
4 HUERTA, ALICIA HUNKER, and MEGAN LYNN HANCOCK, by and through her parent  
5 REBECCA HOLEY (hereinafter, collectively, “Plaintiffs” ), on behalf of themselves and all  
6 others similarly situated, by and through their attorneys, KamberEdelson, LLC, and Law Office  
7 of Joseph H. Malley. P.C., as and for their complaint, allege as follows upon information and  
8 belief, based upon, inter alia, investigation conducted by and through their attorneys, which are  
9 alleged upon knowledge, sues Defendants FACEBOOK, INC, BLOCKBUSTER, INC.,  
10 FANDANGO, INC., HOTWIRE, INC., STA TRAVEL, INC., OVERSTOCK.COM, INC.,  
11 ZAPPOS.COM, INC., GAMEFLY, INC., and JOHN DOES, corporations and states:

#### 14 **NATURE OF THE ACTION**

15 1. This is a class action lawsuit, brought by, and on behalf of similarly situated  
16 individuals whose privacy was violated by the actions of Facebook, Inc., (“Facebook”), and  
17 corporations associated with Facebook, (“Facebook Beacon Activated Affiliates”), which were  
18 involved in a online marketing joint venture (“Facebook Beacon”).

19 2. Facebook members who accessed the websites of one (1) or more of the  
20 Facebook Beacon Activated Affiliates, and engaged in any of a number of predetermined online  
21 activities (“Beacon Trigger Activities”) found that their actions at the Facebook Beacon  
22 Activated Affiliates were disseminated to Facebook, Inc., published on their home and profile  
23 pages, and broadcast to any individuals the Facebook member had designated as a “user friend”  
24 on the Facebook website.

25 3. Facebook and the Facebook Beacon Activated Affiliates acted both  
26  
27  
28

1 independently and jointly in that they knowingly authorized, directed, ratified, approved,  
2 acquiescent, or participated by accessing and disclosing the personal information (“PI”) and/or  
3 personal identifying information (“PII”) derived from the activity of the Facebook member  
4 which had accessed the website of Facebook Beacon Activated Affiliate, without authority or  
5 consent of the Facebook member.  
6

7 4. The purpose of such actions by Facebook, Inc. and the Facebook Beacon  
8 Activated Affiliates, individually and jointly, was to solicit, advertise, and market business  
9 transactions to the Facebook user and the user’s friends without having obtained any of the  
10 user’s consent.  
11

12 5. The class action period, ( the “Class Period”), pertains to the date Facebook and  
13 the Facebook Beacon Activated Affiliates activated the Facebook Beacon to the date the  
14 Facebook default settings relating to the Facebook Beacon program were modified from “opt-  
15 out” to an “opt-in” setting, a period that roughly approximates on or about November 6, 2007 to  
16 December 5, 2007.  
17

18 6. This action does not include corporations which agreed to be a Facebook Beacon  
19 affiliate but did not activate Beacon.  
20

21 7. The conduct of Facebook, Inc. and Facebook Beacon Activated Affiliates,  
22 individually and jointly, violated one (1) or more of the following:

23 a) Electronic Communications Privacy Act, 18 U.S.C. § 2510 (the “ECPA”), against  
24 ALL DEFENDANTS;

25 b) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the “CFAA”), against ALL  
26 DEFENDANTS;

27 c) Video Privacy Protection Act, 18 U.S.C. § 2710, (the “VPPA”) against  
28

1 FANDANGO, BLOCKBUSTER, OVERSTOCK, GAMEFLY, AND DOE  
2 DEFENDANTS 1-20;

3 d) Aiding And Abetting / Civil Conspiracy To Violate The Video Privacy Protection  
4 Act, against DEFENDANT FACEBOOK, ALONE

5 e) Consumer Legal Remedies Act, California Civil Code § 1750 (the “CLRA”), against  
6 DEFENDANTS FACEBOOK, FANDANGO, HOTWIRE, STA, GAMEFLY, and  
7 DOES 21-40

8 f) California’s Computer Crime Law, Penal Code § 502 (the “CCCL”), against  
9 DEFENDANT FACEBOOK, FANDANGO, HOTWIRE, STA, GAMEFLY, and  
10 DOES 21-40.  
11

### 12 JURISDICTION AND VENUE

13  
14 8. This Court has personal jurisdiction over all defendants because (a) a substantial  
15 portion of the wrongdoing alleged in this complaint took place in this state, (b) all defendants  
16 are authorized to do business here, have sufficient minimum contacts with this state, and/or  
17 otherwise intentionally avail themselves of the markets in this state through the promotion,  
18 marketing and sale of products and services in this state, to render the exercise of jurisdiction by  
19 this Court permissible under traditional notions of fair play and substantial justice.  
20

21 9. The following corporations are Delaware corporations headquartered in  
22 California and are only citizens in California and Delaware. Plaintiffs assert claims of behalf of  
23 a proposed class whose members are scattered throughout the fifty states (including the 48  
24 states besides California and Delaware) and the U.S. territories: there is minimal diversity of  
25 citizenship between proposed class members and the Defendant. The aggregate of these claims  
26 exceed the sum or value of \$5,000,000:  
27  
28

- 1 1. Facebook, Inc.;
- 2 2. Fandango, Inc.;
- 3 3. Hotwire, Inc.;
- 4 4. STA Travel, Inc.;
- 5 5. GameFly, Inc.

6 This Court has personal jurisdiction over the Defendants listed in this paragraph under  
7 Cal. Code Civ. Proc. § 410.10 because each of the listed defendants maintains its corporate  
8 headquarters in, and the acts alleged herein were committed in California.

9 10. The following corporations are citizens of states other than California, however,  
10 each of the acts upon which liability is alleged herein were committed by the corporations listed  
11 in this paragraph in the state of California:

- 12 1. Blockbuster, Inc.,
- 13 2. Overstock.com, Inc.,
- 14 3. Zappos.com, Inc.

15 The heart of the conduct complained of involved the communication, transmission, and  
16 interception of personally identifying information and personal private data of the class  
17 members. The mechanism to effectuate this communication, transmission and interception was  
18 devised, developed, and implemented in this judicial district in California. The actual  
19 information and data from each of the Facebook Beacon Activated Affiliates was, without  
20 exception, transmitted to Facebook in California, therefore all evidence of wrongdoing as  
21 alleged in this complaint is located in this judicial district.

22 11. This Court also has subject matter jurisdiction over all causes of action and the  
23 defendants implicated therein pursuant to 28 U.S.C. § 1332(d), and because this action arises in  
24 part under a federal statute and this Court has jurisdiction pursuant to 18 U.S.C. § 2710(c)  
25 which confers jurisdiction in the United States District Court for actions related to the Video  
26 Privacy Protection Act.  
27  
28



1 more of the Beacon Trigger Activities. Lane believes and thereupon alleges that information  
2 related to Lane's engaging in one or more of the Beacon Trigger Activities was captured by the  
3 Beacon Program and communicated to Facebook and/or others, including Lane's Facebook  
4 "Friends." Lane accessed the following named Affiliate websites:

- 5 i. Hotwire, Inc.
- 6 ii. Overstock.com, Inc.
- 7 iii. Zappos.com, Inc.

8  
9 16. Plaintiff, MOHANNAED SHEIKHA; hereinafter "Sheikha" is a resident of  
10 Rockwall County, Texas. Sheikha was a member of Facebook during the Class Period. On one  
11 or more occasions during the Class Period, Sheikha visited one or more of the Named Affiliate's  
12 websites and engaged in one or more of the Beacon Trigger Activities. Sheikha believes and  
13 thereupon alleges that information related to Sheikha's engaging in one or more of the Beacon  
14 Trigger Activities was captured by the Beacon Program and communicated to Facebook and/or  
15 others, including Sheikha 's Facebook "Friends." Sheikha accessed the following named  
16 Affiliate websites:

- 17 i. Zappos.com, Inc.

18  
19 17. Plaintiff, SEAN MARTIN; hereinafter "Martin" is a resident of Dallas County,  
20 Texas. Martin was a member of Facebook during the Class Period. On one or more occasions  
21 during the Class Period, Martin visited one or more of the Named Affiliate's websites and  
22 engaged in one or more of the Beacon Trigger Activities. Martin believes and thereupon alleges  
23 that information related to Martin's engaging in one or more of the Beacon Trigger Activities  
24 was captured by the Beacon Program and communicated to Facebook and/or others, including  
25 Martin's Facebook "Friends." Martin accessed the following named Affiliate websites:

- i. Blockbuster, Inc.
- ii. Zappos.com, Inc.

18. Plaintiff ALI SAMMOUR hereinafter "Sammour" is a resident of Travis County, Texas. Sammour was a member of Facebook during the Class Period. On one or more occasions during the Class Period, Sammour visited one or more of the Named Affiliate's websites and engaged in one or more of the Beacon Trigger Activities. Sammour believes and thereupon alleges that information related to Sammour's engaging in one or more of the Beacon Trigger Activities was captured by the Beacon Program and communicated to Facebook and/or others, including Sammour's Facebook "Friends." Sammour accessed the following named Affiliate websites:

- i. Blockbuster, Inc.
- ii. Fandango, Inc.
- iii. Hotwire, Inc.
- iv. Overstock.com, Inc.
- v. STA Travel, Inc.
- vi. Zappos.com, Inc.
- vii. GameFly, Inc.

19. Plaintiff, MOHAMMED ZIDAN; hereinafter "Zidan" is a resident of Dallas County, Texas. Zidan was a member of Facebook during the Class Period. On one or more occasions during the Class Period, Zidan visited one or more of the Named Affiliate's websites and engaged in one or more of the Beacon Trigger Activities. Zidan believes and thereupon alleges that information related to Zidan's engaging in one or more of the Beacon Trigger Activities was captured by the Beacon Program and communicated to Facebook and/or others,



1 including Zidan's Facebook "Friends." Zidan accessed the following named Affiliate websites:

- 2 i. Blockbuster, Inc.
- 3 ii. Fandango, Inc.
- 4 iii. Hotwire, Inc.
- 5 iv. Overstock.com, Inc.

7 20. Plaintiff, SARA KARROW; hereinafter "Karrow" is a resident of Dallas County,  
8 Texas. Karrow was a member of Facebook during the Class Period. On one or more occasions  
9 during the Class Period, Karrow visited one or more of the Named Affiliate's websites and  
10 engaged in one or more of the Beacon Trigger Activities. Karrow believes and thereupon  
11 alleges that information related to Karrow's engaging in one or more of the Beacon Trigger  
12 Activities was captured by the Beacon Program and communicated to Facebook and/or others,  
13 including Karrow's Facebook "Friends." Karrow accessed the following named Affiliate  
14 websites:  
15

- 16 i. Zappos.com, Inc.

17  
18 21. Plaintiff, COLBY HENSON; hereinafter "Henson" is a resident of Lubbock  
19 County, Texas. Henson was a member of Facebook during the Class Period. On one or more  
20 occasions during the Class Period, Henson visited one or more of the Named Affiliate's  
21 websites and engaged in one or more of the Beacon Trigger Activities. Henson believes and  
22 thereupon alleges that information related to Henson's engaging in one or more of the Beacon  
23 Trigger Activities was captured by the Beacon Program and communicated to Facebook and/or  
24 others, including Henson's Facebook "Friends." Henson accessed the following named Affiliate  
25 websites:  
26

- 27 i. Overstock.com, Inc.

1           22. Plaintiff, DENTON HUNKER; hereinafter "Hunker" is a resident of Tarrant  
2 County, Texas. Hunker was a member of Facebook during the Class Period. On one or more  
3 occasions during the Class Period, Hunker visited one or more of the Named Affiliate's websites  
4 and engaged in one or more of the Beacon Trigger Activities. Hunker believes and thereupon  
5 alleges that information related to Hunker's engaging in one or more of the Beacon Trigger  
6 Activities was captured by the Beacon Program and communicated to Facebook and/or others,  
7 including Hunker's Facebook "Friends." Hunker accessed the following named Affiliate  
8 websites:  
9

- 10                   i. Hotwire, Inc.
- 11                   ii. Overstock.com, Inc.
- 12

13           23. Plaintiff, FIRAS SHEIKHA; hereinafter "F. Sheikha" is a resident of Rockwall  
14 County, Texas. F. Sheikha was a member of Facebook during the Class Period. On one or more  
15 occasions during the Class Period, F. Sheikha visited one or more of the Named Affiliate's  
16 websites and engaged in one or more of the Beacon Trigger Activities. F. Sheikha believes and  
17 thereupon alleges that information related to F. Sheikha's engaging in one or more of the  
18 Beacon Trigger Activities was captured by the Beacon Program and communicated to Facebook  
19 and/or others, including F. Sheikha's Facebook "Friends." F. Sheikha accessed the following  
20 named Affiliate websites:  
21

- 22                   i. Blockbuster, Inc.
- 23                   ii. Overstock.com, Inc.
- 24

25           24. Plaintiff, HASSEN SHEIKHA; hereinafter "H. Sheikha" is a resident of Dallas,  
26 Texas. H. Sheikha was a member of Facebook during the Class Period. On one or more  
27 occasions during the Class Period, H. Sheikha visited one or more of the Named Affiliate's  
28

1 websites and engaged in one or more of the Beacon Trigger Activities. H. Sheikha believes and  
2 thereupon alleges that information related to H. Sheikha's engaging in one or more of the  
3 Beacon Trigger Activities was captured by the Beacon Program and communicated to Facebook  
4 and/or others, including H. Sheikha's Facebook "Friends." H. Sheikha accessed the following  
5 named Affiliate websites:  
6

- 7 i. Overstock.com, Inc.

8 25. Plaintiff, LINDA STEWART; hereinafter "Stewart" is a resident of Kaufman  
9 County, Texas. Stewart was a member of Facebook during the Class Period. On one or more  
10 occasions during the Class Period, Stewart visited one or more of the Named Affiliate's  
11 websites and engaged in one or more of the Beacon Trigger Activities. Stewart believes and  
12 thereupon alleges that information related to Stewarts's engaging in one or more of the Beacon  
13 Trigger Activities was captured by the Beacon Program and communicated to Facebook and/or  
14 others, including Stewart's Facebook "Friends." Stewart accessed the following named Affiliate  
15 websites:  
16

- 17 i. Hotwire, Inc.
- 18 ii. Overstock.com, Inc.
- 19 iii. Zappos.com, Inc.

20 26. Plaintiff, TINA TRAN; hereinafter "Tran" is a resident of Dallas County, Texas.  
21 Tran was a member of Facebook during the Class Period. On one or more occasions during the  
22 Class Period, Tran visited one or more of the Named Affiliate's websites and engaged in one or  
23 more of the Beacon Trigger Activities. Tran believes and thereupon alleges that information  
24 related to Tran's engaging in one or more of the Beacon Trigger Activities was captured by the  
25 Beacon Program and communicated to Facebook and/or others, including Tran's Facebook  
26  
27  
28

1 "Friends." Tran accessed the following named Affiliate websites:

- 2 i. Overstock.com, Inc.

3 27. Plaintiff, MATTHEW SMITH; hereinafter "Smith" is a resident of Tarrant  
4 County, Texas. Smith was a member of Facebook during the Class Period. On one or more  
5 occasions during the Class Period, Smith visited one or more of the Named Affiliate's websites  
6 and engaged in one or more of the Beacon Trigger Activities. Smith believes and thereupon  
7 alleges that information related to Smith's engaging in one or more of the Beacon Trigger  
8 Activities was captured by the Beacon Program and communicated to Facebook and/or others,  
9 including Smith's Facebook "Friends." Smith accessed the following named Affiliate websites:  
10

- 11 i. Overstock.com, Inc.

12 28. Plaintiff, ERICA PARNELL; hereinafter "Parnell" is a resident of Kaufman  
13 County, Texas. Parnell was a member of Facebook during the Class Period. On one or more  
14 occasions during the Class Period, Parnell visited one or more of the Named Affiliate's websites  
15 and engaged in one or more of the Beacon Trigger Activities. Parnell believes and thereupon  
16 alleges that information related to Parnell's engaging in one or more of the Beacon Trigger  
17 Activities was captured by the Beacon Program and communicated to Facebook and/or others,  
18 including Parnell's Facebook "Friends." Parnell accessed the following named Affiliate  
19 websites:  
20

- 21 i. Blockbuster, Inc.

- 22 ii. Fandango, Inc.

- 23 iii. Hotwire, Inc.

- 24 iv. Overstock.com, Inc.

25 29. Plaintiff, JOHN CONWAY; hereinafter "Conway" is a resident of Los Angeles  
26  
27  
28

1 County, California. Conway was a member of Facebook during the Class Period. On one or  
2 more occasions during the Class Period, Conway visited one or more of the Named Affiliate's  
3 websites and engaged in one or more of the Beacon Trigger Activities. Conway believes and  
4 thereupon alleges that information related to Conway's engaging in one or more of the Beacon  
5 Trigger Activities was captured by the Beacon Program and communicated to Facebook and/or  
6 others, including Conway's Facebook "Friends." Conway accessed the following named  
7 Affiliate websites:  
8

9 i. Overstock.com, Inc.

10 ii. GameFly, Inc.

11  
12 30. Plaintiff, AUSTIN MUHS; hereinafter "Muhs" is a resident of Los Angeles  
13 County, California. Muhs was a member of Facebook during the Class Period. On one or more  
14 occasions during the Class Period, Muhs visited one or more of the Named Affiliate's websites  
15 and engaged in one or more of the Beacon Trigger Activities. Muhs believes and thereupon  
16 alleges that information related to Muhs' engaging in one or more of the Beacon Trigger  
17 Activities was captured by the Beacon Program and communicated to Facebook and/or others,  
18 including Muhs' Facebook "Friends." Muhs accessed the following named Affiliate websites:  
19

20 i. Blockbuster, Inc.

21 ii. Fandango, Inc.

22  
23 31. Plaintiff, PHILLIP HUERTA; hereinafter "Huerta" is a resident of Los Angeles  
24 County, California. Huerta was a member of Facebook during the Class Period. On one or more  
25 occasions during the Class Period, Huerta visited one or more of the Named Affiliate's websites  
26 and engaged in one or more of the Beacon Trigger Activities. Huerta believes and thereupon  
27 alleges that information related to Huerta's engaging in one or more of the Beacon Trigger  
28

1 Activities was captured by the Beacon Program and communicated to Facebook and/or others,  
2 including Huerta's Facebook "Friends." Huerta accessed the following named Affiliate websites:

- 3 i. Blockbuster, Inc.
- 4 ii. Hotwire, Inc.
- 5 iii. Overstock.com, Inc.

6  
7 32. Plaintiff, ALICIA HUNKER; hereinafter "A. Hunker" is a resident of Tarrant  
8 County, Texas. A. Hunker was a member of Facebook during the Class Period. On one or more  
9 occasions during the Class Period, A. Hunker visited one or more of the Named Affiliate's  
10 websites and engaged in one or more of the Beacon Trigger Activities. A. Hunker believes and  
11 thereupon alleges that information related to A. Hunker's engaging in one or more of the  
12 Beacon Trigger Activities was captured by the Beacon Program and communicated to Facebook  
13 and/or others, including A. Hunker's Facebook "Friends." A. Hunker accessed the following  
14 named Affiliate websites:

- 15 i. Overstock.com, Inc.

16  
17 33. Defendant Facebook, Inc. (hereinafter "FACEBOOK"), is a Delaware  
18 corporation which maintains its headquarters at 156 University Avenue, Palo Alto, CA 94301.  
19 Defendant Facebook, Inc., does business throughout the United States, and in particular, does  
20 business in State of California and in this County.  
21

22 34. Defendant Blockbuster Online is a registered trademark of Blockbuster, Inc. a  
23 Delaware corporation. Blockbuster, Inc. maintains its headquarters at 1201 Elm Street, Dallas,  
24 TX 75270. Blockbuster, Inc. launched Blockbuster Online in 2004 as its online subscription  
25 program. Defendant Blockbuster, Inc. (hereinafter "Blockbuster"), is a Delaware corporation  
26 which maintains its headquarters at 1201 Elm Street, Dallas, Texas 75270. Blockbuster, Inc. is a  
27  
28

1 provider of rental and retail movie and game entertainment with over 7,800 stores in the United  
2 States. Defendants Blockbuster Online and Blockbuster, Inc do business throughout the United  
3 States, and in particular, do business in State of California and in this County.

4  
5 35. Defendant Fandango, Inc. (hereinafter “Fandango”), is a Delaware corporation  
6 which maintains its headquarters at 12200 W. Olympic Boulevard, Suite 150, Los Angeles, CA  
7 90064. Formed in 2000, Fandango, Inc. “entertains and informs consumers with trailers,  
8 exclusive clips, celebrity interviews, fan reviews and news, while offering the ability to quickly  
9 select a film and conveniently buy tickets in advance.” Defendant Fandango, Inc. does business  
10 throughout the United States, and in particular, does business in State of California and in this  
11 County.

12  
13 36. Defendant Hotwire, Inc. (hereinafter “Hotwire”), is a Delaware corporation  
14 which maintains its headquarters at 333 Market Street, Suite 100, San Francisco, CA 94105.  
15 Founded in 2000, Hotwire, Inc. is a discount travel website offering airline tickets, hotel  
16 reservations, car rentals vacations packages and cruises. Defendant Hotwire, Inc. does business  
17 throughout the United States, and in particular, does business in State of California and in this  
18 County.

19  
20 37. Defendant STA Travel, Inc. (hereinafter “STA”), is a Delaware corporation  
21 which maintains its headquarters at 5900 Wilshire Boulevard, Suite 900, Los Angeles, CA  
22 90036 OR 750 State Hwy. 121, Suite 250, Lewisville, TX 75067. STA Travel, Inc. is a student  
23 travel organization that specializes in arranging air transportation, lodging, tours and ground  
24 transportation for college students. Defendant STA Travel, Inc., does business throughout the  
25 United States, and in particular, does business in State of California and in this County.

26  
27 38. Defendant Overstock.com, Inc. (hereinafter “Overstock”), is a Delaware  
28

1 corporation which maintains its headquarters at 6350 South 3000 East, Salt Lake City, UT  
2 84121. Launched in 1999, Overstock.com is an online retailer which sells companies' excess  
3 inventory. Defendant Overstock.com, Inc., does business throughout the United States, and in  
4 particular, does business in State of California and in this County.  
5

6 39. Defendant Zappos.com, Inc. (hereinafter "Zappos") is a Delaware corporation  
7 which maintains its headquarters at 2280 Corporate Circle, Suite 100, Henderson, NV 89074.  
8 Founded in 1999, Zappos.com, Inc. is an online retailer that sells shoes, clothing and  
9 accessories. Defendant Zappos.com, Inc., does business throughout the United States, and in  
10 particular, does business in State of California and in this County.  
11

12 40. Defendant GameFly, Inc. (hereinafter "GameFly"), is a Delaware corporation  
13 which maintains its headquarters at 5840 West Jefferson Boulevard, Suite J, Los Angeles, CA  
14 90016. Founded in 2002, GameFly, Inc. owns and operates a website offering an online video  
15 game rental subscription service. Defendant GameFly, Inc. does business throughout the  
16 United States, and in particular, does business in State of California and in this County.  
17

18 41. Defendants, John Does 1 - 40, are corporations or business entities whose  
19 specific identity is unknown to Plaintiffs. Plaintiffs therefore sue these Doe defendants by such  
20 fictitious names. These Doe defendants are corporations similarly situated to the Facebook  
21 Beacon Activated Affiliates, who activated and had operating on their website the Facebook  
22 Beacon that affected the Plaintiffs as detailed herein. The contractual obligations of Facebook  
23 may require Facebook to provide notice to the Facebook Beacon activated advertisers of this  
24 matter so as to appear and protect their interests, or these Facebook Beacon activated advertisers  
25 may provide notice to confirm their Beacon activity independent of Facebook. In either case,  
26 when the identity of these Facebook Beacon activated advertisers who are sued as Doe  
27  
28



1 defendants are identified, Plaintiffs will amend their complaint to name such parties as  
2 Facebook Beacon Activated Affiliates.

3 42. This action arises out of the Facebook Beacon Activated Affiliates' websites  
4 using Facebook Beacon. Facebook stated in its press release of November 6, 2007, that "44  
5 websites are using Facebook Beacon:  
6

7 **Leading Websites Offer Facebook Beacon for Social Distribution**

8 Users Gain Ability to Share their Actions from 44 Participating Sites with their  
9 Friends on Facebook

10 NEW YORK — Facebook Social Advertising Event, Nov. 6, 2007 — Facebook  
11 announced today that 44 websites are using Facebook Beacon to allow users to  
12 share information from other websites for distribution to their friends on  
13 Facebook. These sites are participating in the launch of Beacon, a new way to  
14 socially distribute information on Facebook. Beacon is a core element of the  
15 Facebook Ads system for connecting businesses with users and targeting  
16 advertising to the audiences they want.

17 The websites participating in Beacon can determine the most relevant and  
18 appropriate set of actions from their sites that users can distribute on Facebook.  
19 These actions can include posting an item for sale, completing a purchase,  
20 scoring a high score in an online game or viewing of video. When users who are  
21 logged into Facebook visit a participating site, they receive a prompt asking  
22 whether to they want to share those activities with their friends on Facebook. If  
23 they do, those friends can now view those actions through News Feed or Mini-  
24 Feed stories.

25 eBay plans to use Beacon so eBay.com sellers will be able to choose to include  
26 their eBay listings in their Facebook News Feeds. This will allow them to share  
27 the items they are selling with their network of friends. In doing so, eBay.com  
28 sellers can leverage a new way to drive potential bidders and buyers to their  
listings. eBay expects to make this feature available to sellers on eBay.com in  
early 2008.

"Beacon offers an interesting new way for us to deliver on our goal of bringing  
more bidders and buyers to our sellers' listings," said Gary Briggs, senior vice  
president and chief marketing officer, eBay North America. "In a marketplace  
where trust and reputation are crucial to success, giving sellers the ability to  
easily alert their network of friends – the people who already know and trust  
them – to an item for sale has the potential to be a powerful tool."

1 In keeping with Facebook’s philosophy of user control, Facebook Beacon  
2 provides advanced privacy controls so Facebook users can decide whether to  
3 distribute specific actions from participating sites with their friends.

4 Fandango, the nation’s leading moviegoer destination, is using Beacon so when  
5 Facebook users purchase a movie ticket on Fandango.com, they can share their  
6 movie plans with their friends on Facebook. Consumers gain a new way to tell  
7 their friends about their movie tastes, while Fandango is able to gain greater  
8 social distribution on Facebook.

9 “People love to share movies with their friends,” said Chuck Davis, CEO of  
10 Fandango. “When it comes to movies, everyone has an opinion. Fandango is  
11 excited to be selected as one of the first sites to implement Beacon, allowing  
12 Facebook users to share the excitement of moviegoing with their friends.”

13 A number of IAC brands, including CollegeHumor, Busted Tees, iWon,  
14 Citysearch, Pronto.com and echomusic will also be using Facebook Beacon to  
15 share actions taken on participating IAC sites from concert tickets to restaurant  
16 reviews with friends online. The sheer diversity and scale of IAC brands has the  
17 potential to enable Facebook friends to share the more interesting parts of their  
18 life online.

19 “IAC brands touch consumers in a multitude of different ways everyday.  
20 Bringing together great consumer services and products and the added ability to  
21 share individual actions with friends via Facebook can only add value to what we  
22 do and who we do it for,” said Doug Lebda, president and chief operating officer  
23 of IAC.

24 As a way to let travelers tell their Facebook friends about upcoming travel plans,  
25 Travelocity is implementing Facebook Beacon on its website. When Facebook  
26 users book travel on Travelocity, they can choose to share that information with  
27 their friends on Facebook.

28 “Travel is naturally a social activity that travelers enjoy discussing with the  
people they know,” said Jeff Glueck, chief marketing officer at Travelocity.  
“Using Beacon, Travelocity users can now easily choose to spread the news of  
their latest vacation plans on Facebook as a complement to their activities on the  
Travelocity website.”

Additional websites and companies participating in Beacon at launch include  
AllPosters.com, Blockbuster, Bluefly.com, CBS Interactive (CBSSports.com &  
Dotspotter), ExpoTV, Gamefly, Hotwire, Joost, Kiva, Kongregate, LiveJournal,  
Live Nation, Mercantila, National Basketball Association, NYTimes.com,  
Overstock.com, (RED), Redlight, SeamlessWeb, Sony Online Entertainment  
LLC, Sony Pictures, STA Travel, The Knot, TripAdvisor, Travel Ticker,  
TypePad, viagogo, Vox, Yelp, WeddingChannel.com and Zappos.com.

1 <http://www.facebook.com/press/releases.php?p=9166>

2 Some of the business entities identified in Facebook’s statement disputed that they had activated  
3 the Beacon program.

4  
5 **STATEMENT OF FACTS**

6 **The Facebook Service and Network**

7 43. Facebook owns and operates an online web site located at  
8 <http://www.facebook.com>.

9 44. Facebook began as an online social network for college, then eventually high  
10 school children, to exchange personal information confidentially with friends.

11 45. Originally Facebook was self described as “free for use,” and free of advertising.  
12 Facebook still describes itself as “free for use.”

13 46. Facebook membership requires the user to provide their name, birth date, gender  
14 and email address.

15 47. Facebook requires users to register with a unique username and password in  
16 order to access to its computer network.

17 48. Facebook allows users to provide information about the user’s “hometown” to  
18 join a “network,” which generally is a high school or college.

19 49. The information described in Paragraphs 46, 47, and 48, above, can be used to  
20 identify the user of the site, and to locate any individual. Personally identifying information is  
21 information that can be used to distinguish or trace an individual’s identity, and when combined  
22 or used with other identifying information, is, or can be linked or linkable to a specific  
23 individual. The Chief Information Officer for the U.S. Department of Commerce defines  
24 personally identifying information as “..information that indentifies individuals directly or by  
25  
26  
27  
28

1 reference.”

2 50. Facebook members also have the option to provide additional personal  
3 identifiable information including sexual preference, political and religious convictions,  
4 telephone numbers, address, activities, interests, education, work, and to post photos.  
5

6 51. Facebook’s web site enables users to add “friends” to their profiles. This process  
7 connects one registrant’s profile to another registrant’s profile, giving each of the connected  
8 “friends” access to the other “friends” connected to the respective profiles. In this manner,  
9 Facebook’s web site creates a virtual social network of interconnected profiles. “Friends” can  
10 send messages to one another over Facebook’s proprietary computer network. Users may also  
11 send email to one another over the internet.  
12

13 52. Facebook user profiles are available for viewing and Facebook users may be  
14 contacted only by Facebook or persons who have a Facebook username and password.  
15

16 53. Initially when a user joins Facebook, his or her Profile is only viewable by other  
17 users who have been designated as the user’s friend on Facebook (a “Friend”). Friends of a user  
18 can see all personal information that the user has provided to Facebook for the user’s Profile.  
19 To restrict the information that is shared with Friends, a user must take further action and  
20 change his or her privacy settings.  
21

22 54. Facebook users can choose to join one or more networks, based on their school,  
23 workplace or region (a “Network”). Once a user joins a Network, Facebook automatically  
24 begins sharing some of that user’s information with the other users that have joined the same  
25 Network. The information that can be seen by other users in the Network is the same  
26 information that can be seen by a user’s Friend, except for any contact information. As with  
27 Friends, a user can also restrict information that is shared with other users in his or her Network.  
28

1 However, to do so, the user must take further action and change his or her privacy settings. The  
2 viewing of detailed profile data is restricted to users from the same network or confirmed  
3 friends.

4           55. Facebook’s “Privacy Settings” are set by default to “My networks and friends”  
5 which allows the user’s profile to be viewed by their friends and everyone in every network  
6 they join.

7           56. Facebook’s “Terms of Use” obligate individuals to be contractually bound once  
8 a person accesses or uses the website, even if they do not register as a member of Facebook.  
9 Prospective members who wish to review the “Terms of Use” prior to agreeing to any  
10 obligation must login and register in order to review “Platform Application Guidelines,”  
11 Application Terms of Use,” “Developer Terms of Use,” which are incorporated by reference in  
12 the “Terms of Use.”

13           57. Facebook’s “Privacy Policy” discusses a concern to protect the user privacy  
14 noting, “Our default settings limit the information displayed in your profile to your networks  
15 and other reasonable community limitations that we tell you about.” The Facebook privacy  
16 settings are, however, defaulted to share users’ personal information. If users wish to restrict  
17 the information that they share, they must opt-out of most of the sharing settings. It is important  
18 to note that users are not automatically directed to Facebook’s privacy settings upon registering  
19 for Facebook.

20           58. Facebook’s “Terms of Use,” states that it “is intended solely for users who are  
21 thirteen (13) years of age or older.” In addition, anyone between the ages of 13 and 18 who is  
22 not in high school or college is prohibited from using the website. Their use is “unauthorized,  
23 unlicensed and in violation of these Terms of Use.” Facebook’s “Customer Support: Security,”  
24  
25  
26  
27  
28

1 focuses on the safety and security of young people.

2 59. Facebook’s “Privacy Policy” forbids individuals under the age of 13 from  
3 registering as a member, but provides no age verification mechanism to confirm the age of its  
4 members and leaves self regulation to the children.  
5

6 60. Facebook’s “Privacy Policy” recommends that parents of children 13 years and  
7 older should consider whether their child should be supervised during the child's use of the  
8 Facebook site, however there are no age verification mechanisms to confirm the age of its  
9 members, leaving self regulation to the children, and parents do not have to provide “express  
10 consent” for their minor child to become a member, although there exists known privacy issues,  
11 concerns, and contractual obligations.  
12

13 61. Facebook’s “Terms of Use” include an assortment of “membership documents.”  
14 Membership documents for Facebook, which reveal the prospective member’s legal obligations  
15 are not located on one (1) page, but have sub-links within the documents to other documents  
16 incorporated by reference.  
17

18 62. In order to understand the Facebook Beacon program (only insofar as Facebook  
19 is concerned), a prospective Facebook member would need to download and interpret the  
20 following:  
21

**FACEBOOK DOCUMENTS:**

<i>Document:</i>	<i>Word Count:</i>	<i>Hard Copy Count</i>	<i>Screen Count</i>
Privacy Policy	3,716	6	11
Terms of Use	6,495	8	3
Code of Conduct	719	2	17
Copyright Policy	847	2	3
Terms of Sale	2,699	4	8
Marketplace Guidelines	1,381	2	5
Platform Application Guidelines	1,165	2	4
Application Terms of Use	1,700	2	5
Developer Terms of Use	9,255	11	26
<b>TOTAL:</b>	<b>27,977</b>	<b>39</b>	<b>82</b>

1  
2 63. In order to change the privacy default settings of a user’s account, a user would  
3 have to read, interpret and select 9 separate tabs displaying privacy options. The Facebook user  
4 would be obligated to read approximately 4 pages and 2,283 words in order to permit access  
5 only to their selected friends.

6 64. In addition to the privacy policies located on the Facebook website, the Beacon  
7 program implicated the privacy statements and terms and conditions of use at the websites of  
8 the Facebook Beacon Activated Affiliates.

9  
10 65. Facebook’s privacy policy concerns the collection and use of the user’s personal  
11 information, “when using Facebook, located at [www.facebook.com](http://www.facebook.com),” and “this privacy  
12 statement covers the site [www.facebook.com](http://www.facebook.com).” Interactions by Facebook users at the websites  
13 of Facebook Beacon Activated Affiliate are not included in the Facebook privacy policy.  
14

15 **The Beacon Program**

16 66. The Facebook Beacon program was launched on or about November 6, 2007. It  
17 was introduced to Facebook advertisers and affiliates as:

18  
19 “Allow your customers to share with their friends the actions they take on  
20 your website. For user actions you define, Facebook Beacon will publish a  
21 story in the user’s profile and to friends’ News Feeds with a link back to  
22 your site.”

23 **Add 3 lines of code and reach millions of users.**

24 Simply determine which user actions you would like publish to Facebook  
25 and add a few lines of code to your web page. Facebook Beacon actions  
26 include purchasing a product, signing up for a service, adding an item to a  
27 wish list, and more. When a user performs the action, they will be alerted  
28 that your website is sending a story to their profile and have a chance to  
opt out. No additional user action is needed for the story to be published  
on Facebook, and users remain in control of their information.

**Promote your business in an organic, social way.**

1 Facebook Beacon enables your brand or business to gain access to viral  
2 distribution within Facebook. Stories of a user's engagement with your site  
3 may be displayed in his or her profile and in News Feed. These stories will  
4 act as a word-of-mouth promotion for your business and may be seen by  
5 friends who are also likely to be interested in your product. You can  
6 increase the number of friends who see these stories with **Facebook  
7 Social Ads.**

8 **Enable effortless sharing while protecting user privacy.**

9 User privacy is extremely important to Facebook. We designed Facebook  
10 Beacon to enable effortless sharing, but we've also put in features to  
11 protect user privacy. When you send an action to Facebook, the user is  
12 immediately alerted of the story you wish to publish and will be alerted  
13 again when they sign into Facebook. The user must proactively consent to  
14 have a story from your website published.

15 -----

16 **Cookies**

17 67. Under current web protocol, cookies are the principal method by which a website  
18 ‘recognizes’ a particular user. A cookie is supposed to be a secret string of information written  
19 by one website to a user’s browser and accessible only to that website. Under current web  
20 protocol, one should not be able to write a script that asks for information in a cookie set by  
21 another server. A cookie’s recognition can include the user’s identity, preferences, past history  
22 (including purchases), and navigation and use of the website. Cookies are created by the host  
23 website, and they communicate information back to the host website only when the browser is  
24 opened to the host website. Cookies, generally speaking, are passive and dormant unless and  
25 until the host website sends a query to the computer when the user visits the site.

26 68. Facebook’s privacy policy stated:

27 “When you enter Facebook, we collect your browser type and IP address. This  
28 information is gathered for all Facebook visitors. In addition, we store certain  
information from your browser using “cookies.” A cookie is a piece of data  
stored on the user’s computer tied to information about the user. We use session  
ID cookies to confirm that users are logged in. These cookies terminate once the



1 user closes the browser. By default, we use a persistent cookie that stores your  
2 login ID (but not your password) to make it easier for you to login when you  
3 come back to Facebook. You can remove or block this cookie using the settings  
in your browser if you want to disable this convenience feature.”

4 69. The default settings in a user’s web browser generally allows “first-party”  
5 cookies, described within the Facebook and Facebook Beacon Activated Affiliates’ “Terms of  
6 Use,” but not “third-party” cookies which originate from a website different than the site you  
7 are visiting. Facebook’s “Privacy Policy” states, “This privacy policy covers the use of cookies  
8 by Facebook and does not cover the use of cookies or other tracking technologies by any of its  
9 advertisers.”  
10

11 70. Both Facebook and all Facebook Beacon Activated Affiliates collected and  
12 retained personally identifiable information on persons who utilized their respective websites.  
13 The “cookies” used on both Facebook and Facebook Beacon Activated Affiliates could confirm  
14 the personal identity of the common member.  
15

16 71. “Personally Identifiable Information” is “information that links the customer or  
17 patron to particular materials or services.”

18 72. Facebook’s Beacon activities did not occur on www.facebook.com.  
19

20 **How Beacon Worked**

21 73. Every time someone visited a Facebook Beacon Activated Affiliate’s website  
22 and performed a pre-defined action, that action triggered a script that set the Beacon program  
23 into action. The Beacon script contacted Facebook notifying Facebook of the event or action  
24 taking place at the Facebook Beacon Activated Affiliate’s website. Facebook then initiated one  
25 of two actions, depending upon whether the user that initiated the event at the Facebook Beacon  
26 Activated Affiliate’s website was a Facebook member or not.  
27

28 74. Facebook Beacon’s press release of November 6, 2007, stated:

1 “The websites participating in Beacon can determine the most relevant and  
2 appropriate set of actions from their sites that users can distribute on Facebook.  
3 These actions can include posting an item for sale, completing a purchase,  
4 scoring a high score in an online game or viewing of video.”

5 75. The “Beacon Triggered Activities,” distinct to each Facebook Beacon Activated  
6 Affiliate, could have included, but were not limited to, a Facebook member engaging in any of  
7 the following activities : buy; wish\_list; queue; sign\_up; bid; review; add; book; comment;  
8 create; design; download; find; join; play; post; rate; rent; shop; subscribe; support; update;  
9 view; vote; watch; and/or order (hereinafter “Beacon Trigger Activities”).

10 76. Engaging in a Beacon Trigger Activity at a Facebook Beacon Activated  
11 Affiliates’ website resulted in a communication of the user’s activity to Facebook.

12 77. If the user was a Facebook member (as determined by the presence of Facebook  
13 cookies on the user’s computer), Facebook (in theory) generated a little Beacon pop-up alerting  
14 the user that information about his or her action was being sent to Facebook. That pop-up  
15 actually emanated from Facebook even though the person seeing it did not click through to  
16 Facebook. It was triggered by a tag on the Facebook Beacon Activated Affiliates’ webpage  
17 page known as an iFrame, which then told the user’s browser to load a page from Facebook  
18 within the Affiliate’s website the user happens to be visiting.

19 78. If the user was not a Facebook member, Facebook still obtained the notification  
20 from the Facebook Beacon Activated Affiliate. Facebook then undertook the same action of  
21 (theoretically) generating a pop-up on the Facebook Beacon Activated Affiliate website,  
22 however, the iFrame was slightly modified – it was a ghost iFrame, so-called because the  
23 information was rendered transparent and the viewer did not see anything. But the same data  
24 was still sent to Facebook, and Facebook still responded and interacted with the Facebook  
25 Beacon Activated Affiliate’s website with respect to the user’s transaction.  
26  
27  
28

1           79. For example, with respect to the Blockbuster website (a Facebook Beacon  
2 Activated Affiliate), any time any person bought or rented a movie, or even placed a movie in  
3 their queue for renting later, that action triggered the java script that sent notification of that  
4 action to Facebook, regardless of whether the person using the services of the Blockbuster  
5 website was a Facebook customer or not.  
6

7           80. What made the Beacon program distinguishable from other forms of website  
8 interaction, was the way in which a website that was not open in a user's browser (in this case,  
9 Facebook.com) had become actively involved in the exchange between a user and a third-party  
10 website. Beacon utilized cookies to obtain information from the user's computer, but used  
11 iFrames surreptitiously installed on third party websites to access the cookie information.  
12

13           81. With Beacon, however, information regarding user activities was being sent -- in  
14 real time -- to a third party website -- one which was not open or active in the user's browser,  
15 and one which, in many cases, the user may never even have visited or heard of. Further, this  
16 information was sent automatically and specifically, with respect to unique transactions engaged  
17 in by the user.  
18

19           **Problems with Beacon**

20           82. The Beacon program sent information regarding specific user transactions on  
21 Facebook Beacon Activated Affiliates' websites to Facebook regardless of whether the user was  
22 a Facebook member or not. Thus, no consent was sought, nor was any consent obtained from  
23 persons who utilize the Facebook Beacon Activated Affiliate's website who were not Facebook  
24 members. Thus, non-Facebook persons who utilized the Facebook Beacon Activated Affiliate  
25 websites were not told that their transaction, and indeed, every transaction they engaged in upon  
26 the website was being communicated to a third party (Facebook) with whom they had no  
27  
28

1 relationship whatsoever.

2 83. Even with respect to Facebook users, the Beacon program was not designed to  
3 obtain any consent, and indeed, did not obtain any consent prior to the communication of  
4 identifying transactional information to Facebook. By the time any user was notified that  
5 Facebook was (at a minimum), an observing party to the transaction, and that Facebook was  
6 asking for an approval to publicly broadcast identifying information regarding the event,  
7 personally identifying information had already been communicated to Facebook.  
8

9 84. Even with respect to the consent sought by Facebook and the Facebook Beacon  
10 Activated Affiliate websites, the proffer to obtain that consent made to the user was wholly  
11 inadequate, uninformed, misleading, untimely, and deceptive. It was *inadequate* because, on  
12 most Facebook Beacon Activated Affiliate websites, where it was operational at all, it was only  
13 available as a quick pop-up for approximately 10 seconds or even less, and if a user missed it,  
14 misunderstood it, had another window browser open, or even looked in the wrong direction  
15 when it was momentarily available, such actions and a host of other similar non-consensual  
16 occurrences were all interpreted as and defaulted to “consent.” It was *uninformed* because the  
17 pop up did not explain or specify how, which, or through what means the information  
18 concerning the transaction at the Facebook Beacon Activated Affiliate website would be  
19 broadcast both to Facebook and to the Facebook user’s friends list. It was *misleading* because it  
20 implied that the user was given some control over information to be communicated when, in  
21 fact, no such control was offered or available to the user. It was *untimely* because by the time  
22 the pop up asked for consent to communicate transactional information, the transactional  
23 information had already been communicated. Declining to provide consent only concealed the  
24 fact that the information had already been transmitted. It was *deceptive* because, in almost  
25  
26  
27  
28

1 every instance, the information sharing was contrary to the stated privacy policies of the  
2 Facebook website and every other Facebook Beacon Activated Affiliate that had signed up for  
3 the program.

4 85. The Beacon program was further an invasion of privacy in that the program  
5 automatically linked identities and data sharing without user permission. Thus, Facebook  
6 Beacon Activated Affiliate websites automatically and instantly learned which of their users  
7 were Facebook users, even if the user employed an alias, or used different email address for  
8 different websites (a common practice to protect web identity).

9 86. The Beacon program was further flawed in that the program was not only  
10 designed to be defaulted in favor of communicating personal information, it was designed and  
11 introduced with no global opt-out: In other words, there was no way to turn off the Beacon  
12 program. Each Facebook Beacon Activated Affiliate website had to be manually blocked with  
13 a specific and non-global privacy selection, with no opportunity to simply decline participation  
14 in the entire program. Even if a Facebook user declined to share personal information through  
15 Beacon on each of the 44 identified “partner” websites, such action would have no effect upon  
16 any new Beacon “partner” websites added after the 44 Beacon partner sites were individually  
17 declined. In other words, the Beacon program was *designed* to be difficult, cumbersome, and  
18 time-consuming to block.

19 87. Plaintiff SEAN LANE’S experience with the Beacon program was typical of the  
20 various pitfalls and inadequate disclosures that made the program such an invasive violation of  
21 web privacy:

22 **“Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy”**

23 “Sean Lane's purchase was supposed to be a surprise for his wife. Then it  
24 appeared as a news headline -- "Sean Lane bought 14k White Gold 1/5 ct  
25  
26  
27  
28

1 Diamond Eternity Flower Ring from overstock.com" -- last week on the social  
2 networking Web site Facebook.

3 Without Lane's knowledge, the headline was visible to everyone in his online  
4 network, including 500 classmates from Columbia University and 220 other  
5 friends, co-workers and acquaintances.

6 And his wife.

7 The wraps came off his Christmas gift thanks to a new advertising feature  
8 called Beacon, which shares news of Facebook members' online purchases  
9 with their friends. The idea, according to the company, is to allow merchants  
10 to effectively turn millions of Facebook users into a "word-of-mouth  
11 promotion" service.

12 Lane called it "Christmas ruined," and more than 50,000 other users signed a  
13 petition in recent days calling on Facebook to stop broadcasting people's  
14 transactions without their consent."

15 For Lane, spoiling his wife's surprise was bad enough.

16 Within two hours after he bought the ring on Overstock.com, he received an  
17 instant message from his wife, Shannon: Who is this ring for?

18 What ring, he messaged back, from his laptop at work in Waltham, Mass.

19 She said that Facebook had just put an item on his page saying he bought a  
20 ring. It included a link to Overstock, which noted that the 51 percent discount  
21 on the ring.

22 Lane, 28, a technical project manager at an online printing company, was  
23 crestfallen. He had gone to lengths to keep the ring a secret, even telling  
24 Shannon he was not going to give her jewelry this year."

25 Lane complained to Overstock. Company spokesman Judd Bagley said this  
26 week that on Nov. 21, Overstock abandoned its Beacon feature until Facebook  
27 changes its practice so that users must volunteer if they want to participate.

28 "I was really disappointed because for me the whole fun of Christmas is the  
surprise," said Shannon Lane, 28, who married Sean a year ago in September.  
"I never want to know what I'm getting."

*Washington Post*, November 30, 2007.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html>

88. On November 29, 2007, the following article appeared in the [Weblog] New

1 York Times.

2 Facebook Executive Discusses Beacon Brouhaha

3 By [Brad Stone](#)

4 *Update: The interview below took place hours before Facebook announced a*  
5 *major change in its Beacon system, one that requires users to explicitly approve*  
6 *the sending of information to their friends' News Feeds. See [our article](#) for*  
7 *details.*

8 Facebook does not appear to be conceding much ground on Beacon — the  
9 program that informs a person's Facebook friends what he has purchased or  
10 posted on sites like Fandango.com, Yelp.com and NYTimes.com.

11 Earlier today I spoke with Chamath Palihapitiya, vice president of product  
12 marketing and operations at Facebook. Mr. Palihapitiya said the company was  
13 listening to its users and described three changes Facebook was making to  
14 Beacon. First, the opt-out boxes on Beacon partner sites, which let users specify  
15 if they do not want their Facebook friends to be notified of their purchases or  
16 online activity, will now load more quickly, ensuring that more users see them.

17 Second, Facebook will now be able to determine whether the opt-out notification  
18 has been properly loaded on the user's screen — an indication of whether the  
19 user has actually been given an opportunity to opt-out.

20 Finally, if users fail to approve or decline the Facebook alert on the partner site,  
21 Facebook will no longer assume the user is agreeing by omission. Instead, it will  
22 offer another, more visible opportunity to opt-out to users on Facebook itself. If  
23 no action is taken within two days, Facebook will assume the user complies and  
24 will publish the action in the news feed.

25 "We don't want to catch anyone off guard," Mr. Palihapitiya said. "We are  
26 giving them an explicit and clear way to know what has happened and for them  
27 to publish."

28 More information on Beacon from our conversation:

Q. Will Facebook ever make Beacon "opt-in" instead of "opt-out," as critics  
have suggested, or simply give users a single way to decline to participate in the  
service altogether?

A. Mr. Palihapitiya said the company learned from the similar controversy over  
the introduction of the News Feed last year that people need to be given a chance  
to try new features. "We think Beacon has the same potential" as News Feed, he  
said. "We want people to try it, to see it in action. If they don't like it they can  
easily turn it off. Our point of view is, let's give people the ability to sample it."

1 Q. Why not give people a universal opt-out of the Beacon service?

2 A. “We think the right way to offer this is on a site-by-site basis. We want people  
3 to see how the product behaves on different sites.”

4 Q. But some people are asking for a single opt-out.

5 A. “One of the things we try to do is listen to feedback as much as possible. Just  
6 to give you where a lot of this feedback is coming from, it’s coming more from  
7 the press than specific users,” he said. “Right now, the right thing to do is to  
8 make sure we speak to actual users, not the pundits.”

9 Q. It’s not pundits though — it is users and advocates concerned about privacy.

10 A. “I’m not trying to diminish that,” he said. “The feedback we’ve gotten from  
11 actual users using this product has allowed us to refine it, and here’s the first set  
12 of changes. If there is demand for a different set of features, we’ll do that as  
13 well.”

14 Q. If I buy tickets on Fandango, and decline to publish the purchase to my  
15 friends on Facebook, does Facebook still receive the information about my  
16 purchase?

17 A. “Absolutely not. One of the things we are still trying to do is dispel a lot of  
18 misinformation that is being propagated unnecessarily.”

19 Q. Were users properly informed about Beacon from the start?

20 A. “The way that we announce products is generally through blogging and  
21 through Rooster stories,” he said, referring to prominent alerts from Facebook  
22 that appear in users’ News Feeds. “We followed that exact same protocol for this  
23 product that we followed for many other product releases in the past. What we  
24 don’t do is proactively push e-mail or other things to users. What we try to do is  
25 use the service itself to communicate about improvements and features we make.  
26 But our takeaway is we need to make sure we do a better and better job on that.”

27 Q. I think MoveOn will see this as you guys digging in.

28 A. “The thing is, we haven’t dug in in any way. We have pretty markedly  
changed the product based on the feedback we’ve gotten. What I’m saying is, it’s  
still important that people have a chance to see it and make a decision for  
themselves.”

<http://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha>

89. On December 5, 2007, Facebook issued the following press release from Mark



1 Zuckerberg, founder of Facebook:  
2

3 **Announcement: Facebook Users Can Now Opt-Out of Beacon Feature**

4 Thoughts on Beacon

5 About a month ago, we released a new feature called Beacon to try to help  
6 people share information with their friends about things they do on the web.  
7 We've made a lot of mistakes building this feature, but we've made even more  
8 with how we've handled them. We simply did a bad job with this release, and I  
9 apologize for it. While I am disappointed with our mistakes, we appreciate all  
the feedback we have received from our users. I'd like to discuss what we have  
learned and how we have improved Beacon.

10 When we first thought of Beacon, our goal was to build a simple product to let  
11 people share information across sites with their friends. It had to be lightweight  
12 so it wouldn't get in people's way as they browsed the web, but also clear  
13 enough so people would be able to easily control what they shared. We were  
14 excited about Beacon because we believe a lot of information people want to  
share isn't on Facebook, and if we found the right balance, Beacon would give  
people an easy and controlled way to share more of that information with their  
friends.

15 But we missed the right balance. At first we tried to make it very lightweight so  
16 people wouldn't have to touch it for it to work. The problem with our initial  
17 approach of making it an opt-out system instead of opt-in was that if someone  
18 forgot to decline to share something, Beacon still went ahead and shared it with  
19 their friends. It took us too long after people started contacting us to change the  
20 product so that users had to explicitly approve what they wanted to share.  
Instead of acting quickly, we took too long to decide on the right solution. I'm  
not proud of the way we've handled this situation and I know we can do better.

21 Facebook has succeeded so far in part because it gives people control over what  
22 and how they share information. This is what makes Facebook a good utility,  
23 and in order to be a good feature, Beacon also needs to do the same. People  
need to be able to explicitly choose what they share, and they need to be able to  
turn Beacon off completely if they don't want to use it.

24 This has been the philosophy behind our recent changes. Last week we changed  
25 Beacon to be an opt-in system, and today we're releasing a privacy control to  
26 turn off Beacon completely. You can find it here. If you select that you don't  
27 want to share some Beacon actions or if you turn off Beacon, then Facebook  
won't store those actions even when partners send them to Facebook.  
28

1 On behalf of everyone working at Facebook, I want to thank you for your  
2 feedback on Beacon over the past several weeks and hope that this new privacy  
3 control addresses any remaining issues we've heard about from you.

4 Thanks for taking the time to read this.

5 Mark

6 -----  
7 **CLASS ALLEGATIONS**  
8 **Allegations as to Class Certification**

9 90. Plaintiffs bring this Complaint on behalf of themselves and the following class  
10 with respect to Plaintiff's claims for violation of the Electronic Communications Privacy Act  
11 ("ECPA"), and Violation of the Federal Computer Fraud And Abuse Act ("CFA") against *ALL*

12 *DEFENDANTS:*

13 All Facebook members who, during the period of November 7, 2007 to  
14 December 5, 2007 (the "Class Period"), visited one or more the Facebook  
15 Beacon Activated Affiliates' websites and engaged in one or more  
16 activities that triggered the Beacon program to communicate with  
17 Facebook regarding the activity.

18 (Hereinafter, "ECPA / CFA CLASS.")

19  
20  
21 91. Plaintiffs bring this Complaint on behalf of themselves and the following class  
22 with respect to Plaintiff's claims for Aiding And Abetting Violations Of The Video Privacy  
23 Protection Act, Civil Conspiracy To Violate The Video Privacy Protection Act, Violation Of  
24 Consumer Legal Remedies Act, Violation Of California's Computer Crime Law, and Unjust  
25 Enrichment against *DEFENDANT FACEBOOK, ALONE:*

26 All Facebook members who, during the period of November 7, 2007 to  
27 December 5, 2007 (the "Class Period"), visited one or more the Facebook  
28

1 Beacon Activated Affiliates' websites and engaged in one or more  
2 activities that triggered the Beacon program to communicate with  
3 Facebook regarding the activity.

4 (Hereinafter, "FACEBOOK CLASS.")  
5

6 92. Plaintiffs bring this Complaint on behalf of themselves and the following class  
7 with respect to Plaintiff's claims for violation of the Video Privacy Protection Act ("VPPA"),  
8 against DEFENDANTS *FANDANGO, BLOCKBUSTER, GAMEFLY, AND OVERSTOCK*  
9 (hereinafter "VPPA Defendants"):

10 All Facebook members who, during the period of November 7, 2007 to  
11 December 5, 2007 (the "Class Period"), visited one or more the VPPA  
12 Defendants websites and engaged in one or more activities that triggered  
13 the Beacon program to communicate with Facebook regarding the activity.

14 (Hereinafter, "VPPA CLASS.")  
15

16 93. Plaintiffs bring this Complaint on behalf of themselves and the following class  
17 with respect to Plaintiff's claims for violation of the Consumer Legal Remedies Act ("CLRA"),  
18 and Violation Of California's Computer Crime Law ("CCCL"), against DEFENDANTS  
19 *FANDANGO, HOTWIRE, , GAMEFLY, AND STA* (hereinafter "CLRA / CCCL Defendants"):

20 All Facebook members who, during the period of November 7, 2007 to  
21 December 5, 2007 (the "Class Period"), visited one or more the CLRA /  
22 CCCL Defendants websites and engaged in one or more activities that  
23 triggered the Beacon program to communicate with Facebook regarding the  
24 activity.

25 (Hereinafter, "CLRA / CCCL CLASS.")  
26  
27  
28

1           94.     Plaintiffs reserve the right to revise these definitions of the classes based on facts  
2 they learn during discovery.

3           95.     The classes are brought pursuant to Federal Rule of Civil Procedure 23 (the  
4 “Classes”). Excluded from the Classes are i) any Judge or Magistrate presiding over this action,  
5 and the court personnel supporting the Judge or Magistrate presiding over this action, and  
6 members of their respective families; ii) Defendant, Defendant's subsidiaries, parents,  
7 successors, predecessors, and any entity in which a Defendant or its parent has a controlling  
8 interest and their current or former employees, officers and directors; and iii) persons who  
9 properly execute and file a timely request for exclusion from the class and iv) the legal  
10 representatives, successors or assigns of any such excluded persons.  
11

12           96.     **Numerosity:** Individual joinder of all members of the Class is impracticable.  
13  
14 When Facebook introduced the Beacon program, Facebook had more than 60 million members.  
15 The Facebook Beacon Activated Affiliates are in many cases, themselves heavily trafficked  
16 websites. Defendant Blockbuster alone has more than 1.6 million users for its online video  
17 rental service. There are estimated to be tens of thousands of Class members. Upon  
18 information and belief, class members can be identified by the electronic records of defendants.  
19

20           97.     **Class Commonality:** Common questions of fact and law exist as to all Class  
21 members and predominate over the questions affecting only individual Class members. All  
22 class members were Facebook users during the Class Period. All Facebook users who engaged  
23 in a Beacon Trigger Activity at one of the Facebook Beacon Activated Affiliate’s websites  
24 during the class period had their information and activities disclosed to Facebook and others.  
25 This disclosure took place automatically because the Beacon program was designed to send  
26 such information as soon as a Facebook member engaged in one or more of the pre-specified  
27  
28

1 activities that triggered the Beacon script.

2 98. Common questions include:

- 3 a. What was the Beacon program and how did it work;
- 4 b. What information did the Bacon program collect and what did it do with that
- 5 information;
- 6 c. Was there proper *or any* notice, of the operation of the Beacon program to
- 7 consumers?
- 8 d. Was there proper *or any* opportunity to decline the operation of the Beacon
- 9 program provided to consumers?
- 10 e. Whether Facebook members, by virtue of their membership, had pre-consented
- 11 to the operation of the Beacon program on the non-Facebook websites:
- 12 f. Did the operation, function, and/or implementation of the Beacon program
- 13 violate the ECPA?;
- 14 g. Did the operation, function, and/or implementation of the Beacon program
- 15 violate the VPPA?
- 16 h. Did the implementation of the Beacon program by the CLRA Defendants violate
- 17 the CLRA?
- 18 i. Did the operation, function, and/or implementation of the Beacon program
- 19 violate the CCCL?
- 20 j. Did the operation, function, and/or implementation of the Beacon program
- 21 violate the CFAA?
- 22 k. Is Facebook liable under a theory of aiding and abetting, or conspiracy, for the
- 23 Affiliate Defendant's violations of the VPPA?
- 24
- 25
- 26
- 27
- 28

- 1           1. Did the Beacon program send back to Facebook “personally identifying  
2           information?;
- 3           m. Whether, by its misconduct as set forth herein, Facebook and the CLRA  
4           defendants engaged in unfair, deceptive, untrue, or misleading promotion,  
5           implementation, and operation of their websites;
- 6           n. Was Facebook unjustly enriched by its actions in implementing the Beacon  
7           Program?;
- 8           o. Are class members entitled to damages as a result of the implementation of the  
9           Beacon program, and, if so, what is the measure of those damages?  
10

11           99. Defendant engaged in a common course of conduct giving rise to the legal rights  
12           sought to be enforced by the class members. Similar or identical statutory and common law  
13           violations, business practices, and injuries are involved. Individual questions, if any, pale by  
14           comparison to the numerous common questions that dominate.  
15           

16           100. The injuries sustained by the class members flow, in each instance, from a  
17           common nucleus of operative facts. In each case Defendants caused or permitted unauthorized  
18           communications of private and personally identifying information to be delivered to Facebook  
19           and others through the use of the Beacon program without adequate notice, consent, or  
20           opportunity to opt out.  
21           

22           101. **Typicality:** Plaintiffs’ claims are typical of the claims of other members of the  
23           Class, as the Plaintiffs and other Class members were all subjected to Defendant’s identical  
24           wrongful conduct based upon the same transactions which occurred uniformly to the Plaintiffs  
25           and to the public.  
26           

27           102. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the class.  
28

1 Plaintiffs are familiar with the basic facts that form the bases of the proposed class members'  
2 claims. Plaintiffs' interests do not conflict with the interests of the other class members that  
3 they seek to represent. Plaintiffs have retained counsel competent and experienced in class  
4 action litigation and intend to prosecute this action vigorously. Plaintiffs' counsel has  
5 successfully prosecuted complex actions including consumer protection class actions. Plaintiffs  
6 and Plaintiffs' counsel will fairly and adequately protect the interests of the class members.  
7

8       103. **Superiority**: The class action device is superior to other available means for the  
9 fair and efficient adjudication of the claims of Plaintiffs and the proposed class members. The  
10 relief sought per individual member of the class is small given the burden and expense of  
11 individual prosecution of the potentially extensive litigation necessitated by the conduct of  
12 Defendants. Furthermore, it would be virtually impossible for the class members to seek  
13 redress on an individual basis. Even if the class members themselves could afford such  
14 individual litigation, the court system could not.  
15

16       104. Individual litigation of the legal and factual issues raised by the conduct of  
17 Defendants would increase delay and expense to all parties and to the court system. The class  
18 action device presents far fewer management difficulties and provides the benefits of a single,  
19 uniform adjudication, economies of scale and comprehensive supervision by a single court.  
20

21       105. Given the similar nature of the class members' claims and the absence of  
22 material differences in the state statutes and common laws upon which the class members'  
23 claims are based, a nationwide class will be easily managed by the Court and the parties.  
24

25       106. The court may be requested to also incorporate subclasses of Plaintiffs,  
26 defendants, or both, in the interest of justice and judicial economy.  
27

28       107. In the alternative, the class may be certified because:

- 1 a) the prosecution of separate actions by the individual members of the class would  
2 create a risk of inconsistent or varying adjudication with respect to individual  
3 class members which would establish incompatible standards of conduct by  
4 defendant;  
5  
6 b) the prosecution of separate actions by individual class members would create a  
7 risk of adjudications with respect to them which would, as a practical matter, be  
8 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  
11  
12 c) Defendants have acted or refused to act on grounds generally applicable to the  
13 class, thereby making appropriate final and injunctive relief with respect to the  
14 members of the class as a whole.

15 **Count I:**  
16 **VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**  
17 **Against All Defendants**

18 108. Plaintiffs incorporate the above allegations by reference as if set forth herein at  
19 length.

20 109. Plaintiffs assert this claim against each and every Defendant on behalf of  
21 themselves and the Class.

22 110. The federal Electronic Communications Privacy Act of 1986 ("ECPA", at 18  
23 U.S.C. § 2511(1) makes it unlawful for a person to "willfully intercept[], endeavor[] to  
24 intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or  
25 electronic communication." 18 USC 2520(a) provides a civil cause of action to "any person  
26  
27  
28



1 whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in  
2 violation of the ECPA.

3 111. The transmission of data by Plaintiffs and the Class between their computers and  
4 the websites of the Facebook Beacon Activated Affiliate Defendants and each of them,  
5 including, but not limited to, communications regarding buy; wish\_list; queue; sign\_up; bid;  
6 review; add; book; comment; create; design; download; find; join; play; post; rate; rent; shop;  
7 subscribe; support; update; view; vote; watch; and/or order, constitute “electronic  
8 communications” within the meaning of 18 U.S.C. §2510.  
9

10 112. Defendants have intentionally obtained and/or intercepted, by device or  
11 otherwise, these electronic communications without Plaintiffs’ or Class members’ knowledge,  
12 consent, or authorization and while the communications were still en route.  
13

14 113. Defendants have intentionally disclosed to another person, and have otherwise  
15 used, such electronic communications, with knowledge, or having reason to know, that the  
16 electronic communications were obtained through interception, for an unlawful purpose.  
17

18 114. Defendants intentional interception of these electronic communications without  
19 Plaintiffs’ or Class members’ knowledge, consent, or authorization was undertaken without a  
20 facially valid court order or certification.

21 115. Defendants exceeded their authorization to access and control private  
22 information concerning Plaintiffs’ electronic communications, in violation of 18 U.S.C. § 2701.  
23

24 116. Defendants unlawfully and knowingly divulged Plaintiffs’ electronic  
25 communication contents and user information, in violation of 18 U.S.C. § 2702.

26 117. Defendants intentionally acquired and/or intercepted the contents of electronic  
27 communications sent by and/or received by Plaintiffs through the use of an electronic device.  
28

1 Defendants intentionally acquired the communications that had been sent from or directed to  
2 Plaintiffs through their use of computers and other electronic devices which were part of, and  
3 utilized in, Defendants’ electronic communications system, in violation of 18 U.S.C. § 2511  
4 and pursuant to 18 U.S.C. § 2520.  
5

6 118. Defendants unlawfully accessed and used, and voluntarily disclosed, the contents  
7 of the intercepted communications to enhance their profitability and revenue through  
8 advertising. This disclosure was not necessary for the operation of Defendants’ system or to  
9 protect Defendants’ rights or property.  
10

11 119. Plaintiffs are “person[s] whose ... electronic communication is intercepted ... or  
12 intentionally used in violation of this chapter” within the meaning of 18 U.S.C. § 2520.  
13

14 120. Defendants are liable directly and/or vicariously for this cause of action.  
15 Plaintiffs therefore seek remedy as provided for by 18 U.S.C. § 2520, including such  
16 preliminary and other equitable or declaratory relief as may be appropriate, damages consistent  
17 with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial,  
18 and a reasonable attorney’s fee and other litigation costs reasonably incurred  
19

20 121. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary,  
21 equitable, and declaratory relief, in addition to statutory damages of the greater of \$10,000 or  
22 \$100 a day for each day of violation, actual and punitive damages, reasonable attorneys’ fees,  
23 and Defendants’ profits obtained from the above-described violations.  
24

25 **Count II:**  
26 **VIOLATIONS OF THE VIDEO PRIVACY PROTECTION ACT**  
27 **- 18 U.S.C. § 2710**  
28 **against Fandango, Blockbuster, Overstock, GameFly, and Doe Defendants 1-20**  
**(hereinafter “VPPA Defendants”)**

122. Plaintiffs incorporate the above allegations by reference as if set forth herein at

1 length.

2           123. The Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2002))  
3 (“VPPA”) was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's  
4 video rental records in a newspaper. The bill was drafted by Senator Leahy, who noted during  
5 the floor debate that new privacy protections are necessary in "an era of interactive television  
6 cables, the growth of computer checking and check-out counters, of security systems and  
7 telephones, all lodged together in computers...." S. Rep. No. 100-599, 100th Cong., 2d Sess. at 6  
8 (1988).  
9

10           124. The VPPA defines "personally identifiable information" as that which "identifies  
11 a person as having requested or obtained specific video materials or services from a video tape  
12 service provider." A "video tape service provider" is "any person, engaged in the business, in or  
13 affecting interstate or foreign commerce, of rental, sale or delivery of prerecorded video cassette  
14 tapes or similar audiovisual materials."  
15

16           125. Video tape service providers may disclose personally identifiable information  
17 only:  
18

- 19           ○ to the consumer him- or herself;
- 20           ○ to any other person, with the written consent of the consumer;
- 21           ○ to any other person, if the disclosure is simply of names and addresses, and  
22                 ▪ -the consumer has been provided with an opportunity to opt-out; and  
23                 ▪ -the disclosure does not identify title, description or subject matter  
24                         (though subject matter may be disclosed if "for the exclusive use of  
25                         marketing goods and services to the consumer");  
26           ○ to any other person, if in the ordinary course of business;
- 27
- 28

- 1           ○ to a law enforcement agency, pursuant to a federal or state warrant, a grand jury
- 2           subpoena, or a court order, provided that
- 3           ▪ -the consumer is provided with prior notice, and
- 4           ▪ -there is a showing of probable cause to believe that the records are
- 5           relevant to a legitimate law enforcement enquiry;
- 6
- 7           ○ or
- 8           ○ pursuant to a court order in a civil proceeding, upon showing of a compelling
- 9           need, provided
- 10          ▪ -the consumer is given reasonable notice; and
- 11          ▪ -afforded the opportunity to contest the request.
- 12

13           126. The VPPA permits any person aggrieved by a violation of its disclosure rules to  
14 bring a civil action for damages in a federal court.

15           127. Defendant Blockbuster owns and operates a publicly accessible website for  
16 products and /or services. That website provides consumers with access to prerecorded video  
17 cassette tapes or similar audiovisual materials. During the class period, Facebook members  
18 who visited that website and engaged in one or more of the Beacon Trigger Activities,  
19 including, but not limited to accessing, requesting, purchasing, commenting upon, downloading  
20 and/or viewing specific video materials or services had such activities, along with their  
21 personally identifying information, communicated to Facebook. Even if the Facebook member  
22 was provided with the option to decline the communication through a small, pop-up window  
23 visible for a few seconds (which in most cases he or she was not), the information was  
24 communicated to Facebook even when the Facebook member expressly declined to share such  
25 information.  
26  
27  
28

1           128. Defendant Fandango owns and operates a publicly accessible website for  
2 products and /or services. That website provides consumers with access to prerecorded video  
3 cassette tapes or similar audiovisual materials. During the class period, Facebook members  
4 who visited that website and engaged in one or more of the Beacon Trigger Activities,  
5 including, but not limited to accessing, requesting, purchasing, commenting upon, downloading  
6 and/or viewing specific video materials or services had such activities, along with their  
7 personally identifying information, communicated to Facebook. Even if the Facebook member  
8 was provided with the option to decline the communication through a small, pop-up window  
9 visible for a few seconds (which in most cases he or she was not), the information was  
10 communicated to Facebook even when the Facebook member expressly declined to share such  
11 information.  
12

14           129. Defendant Overstock owns and operates a publicly accessible website for  
15 products and /or services. That website provides consumers with access to prerecorded video  
16 cassette tapes or similar audiovisual materials. During the class period, Facebook members  
17 who visited that website and engaged in one or more of the Beacon Trigger Activities,  
18 including, but not limited to accessing, requesting, purchasing, commenting upon, downloading  
19 and/or viewing specific video materials or services had such activities, along with their  
20 personally identifying information, communicated to Facebook. Even if the Facebook member  
21 was provided with the option to decline the communication through a small, pop-up window  
22 visible for a few seconds (which in most cases he or she was not), the information was  
23 communicated to Facebook even when the Facebook member expressly declined to share such  
24 information.  
25  
26  
27  
28

1           130. Defendant GameFly owns and operates a publicly accessible website for  
2 products and /or services. That website provides consumers with access to prerecorded video  
3 cassette tapes or similar audiovisual materials. During the class period, Facebook members  
4 who visited that website and engaged in one or more of the Beacon Trigger Activities,  
5 including, but not limited to accessing, requesting, purchasing, commenting upon, downloading  
6 and/or viewing specific video materials or services had such activities, along with their  
7 personally identifying information, communicated to Facebook. Even if the Facebook member  
8 was provided with the option to decline the communication through a small, pop-up window  
9 visible for a few seconds (which in most cases he or she was not), the information was  
10 communicated to Facebook even when the Facebook member expressly declined to share such  
11 information.  
12

14           131. Each of the VPPA Defendants is a “video tape service provider” within the  
15 meaning of 18 U.S.C. § 2710(a)(4) because each VPPA Defendant is a person, engaged in the  
16 business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of  
17 prerecorded video cassette tapes or similar audio visual materials as defined by the Act..  
18

19           132. Each of the VPPA Defendants knowingly disclosed personally identifiable  
20 information concerning each Facebook member -- and the Beacon Trigger Activities the  
21 Facebook member engaged in -- to Facebook without the informed written consent of the  
22 Facebook member. Each of the VPPA Defendants knowingly consented to the operation of the  
23 Beacon program on their website and affirmatively incorporated special Beacon script that  
24 activated the program and its communications to Facebook when the Beacon Trigger Activities  
25 were engaged in by the Facebook member.  
26  
27  
28



1 convinced, or otherwise encouraged each of the VPPA Defendants to place the Beacon script on  
2 their websites, so that when Facebook members engaged in a Beacon Trigger Activity at the  
3 VPPA Defendants' websites, the Beacon script would be triggered to transmit and disclose  
4 information that the VPPA specifically prohibits the disclosure of.

5  
6 138. Defendant Facebook aided and abetted such wrongful conduct, including  
7 providing the means and the tools to violate the VPPA.

8 139. Defendant Facebook also aided and abetted the described wrongful conduct of  
9 the other Defendant Facebook by giving substantial assistance and/or encouragement that,  
10 separately considered, was wrongful in and of itself.

11  
12 140. Defendant Facebook knew, or should have known, that the conduct the VPPA  
13 defendants engaged in by use of the Beacon Program provided by Facebook was unlawful and  
14 that Facebook's provision of the Beacon program was the means by which that unlawful  
15 conduct took place.

16  
17 141. Defendant Facebook knew, or should have known, at all relevant times herein,  
18 its role as part of an overall illegal or tortious activity at the time that Facebook provided its  
19 assistance.

20 142. As a direct and proximate result of the aiding and abetting of these acts,  
21 Plaintiffs have suffered injury and harm and loss, including, but not limited to, loss of the user's  
22 privacy with respect to their actions on the internet (where class members shop, where they  
23 browse, and what goods and services they seek), loss of privacy with respect to their  
24 associational relationships being disclosed to entities that otherwise would not have known or  
25 learned of such associational relationships (disclosure of Facebook membership to each VPPA  
26 defendant who implemented the Beacon program on their site); and loss of privacy with respect  
27  
28



1 to the names, titles, genres and types of audiovisual materials purchased, rented, or even viewed  
2 by the class members (direct violation of the VPPA). The wrongful conduct aided and abetted  
3 by the Defendant Facebook was a substantial factor in causing this harm.  
4

5 **Count IV**  
6 **CIVIL CONSPIRACY ON BEHALF OF THE CLASS**  
7 **Against Defendant Facebook**

8 143. Plaintiffs incorporate by reference each of the allegations in the preceding  
9 paragraphs of this Complaint as though fully set forth here.

10 144. Defendant Facebook willfully, intentionally, and knowingly agreed and  
11 conspired with the VPPA Defendants to engage in the alleged wrongful conduct, including the  
12 VPPA Defendants violation of the VPPA.

13 145. Defendant Facebook did the acts alleged pursuant to, and in furtherance of, that  
14 agreement and/or furthered the conspiracy by cooperating, encouraging, ratifying, or adopting  
15 the acts of the others.

16 146. As a direct and proximate result of the acts in furtherance of the conspiracy,  
17 Plaintiffs have suffered injury, damage, loss, and harm, including, but not limited to, loss of the  
18 user's privacy with respect to their actions on the internet (where class members shop, where  
19 they browse, and what goods and services they seek), loss of privacy with respect to their  
20 associational relationships being disclosed to entities that otherwise would not have known or  
21 learned of such associational relationships (disclosure of Facebook membership to each VPPA  
22 defendant who implemented the Beacon program on their site); and loss of privacy with respect  
23 to the names, titles, genres and types of audiovisual materials purchased, rented, or even viewed  
24 by the class members (direct violation of the VPPA).  
25  
26

27 147. The wrongful conduct committed pursuant to the conspiracy was a substantial  
28

1 factor in causing this harm.

2 148. Defendant Facebook’s intentional agreement to commit, and commission of,  
3 these wrongful acts was willful, malicious, oppressive, and in conscious disregard of Plaintiffs’  
4 rights, and Plaintiffs are therefore entitled to an award of punitive damages to punish their  
5 wrongful conduct and deter future wrongful conduct.  
6

7 **Count V**  
8 **VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT**  
9 **against Facebook, Fandango, Hotwire, STA, and GameFly**  
10 **(Hereinafter “CLRA California Defendants”)**

11 149. Plaintiffs incorporate the above allegations by reference as if set forth herein at  
12 length.

13 150. Defendant Fandango owns and operates a publicly accessible website for  
14 products and/or services that it makes available to consumers throughout California and the  
15 United States. Consumer services are available through its website, and consumers can use the  
16 service its website makes available to purchase tickets to films. The website advises consumers  
17 that the use of the website is subject to certain terms and conditions and/or a privacy policy that  
18 governs the relationship between consumers and that website, and in particular, how the website  
19 will use and/or disclose or not disclose information that the consumer provides to the website in  
20 the context of the consumer’s use of the website to third parties. Nowhere in any of the terms  
21 and conditions and/or in the privacy policy that governed the use of the website did the website  
22 advise that Facebook members would have their information treated differently from other  
23 consumers using the website. Nowhere in any of the terms and conditions and/or in the privacy  
24 policy that governed the use of the website did the website advise Facebook members that their  
25 transactions on the website were, in real time, being communicated to the Facebook website, or  
26  
27  
28

1 that those transactions included personally identifying information and specific product or  
2 service information in conjunction with the disclosure of their identity.

3           151. Defendant Hotwire owns and operates a publicly accessible website for products  
4 and/or services that it makes available to consumers throughout California and the United  
5 States. Consumer services are available through its website, and consumers can use the service  
6 its website makes available to purchase discount travel airline tickets, hotel reservations, car  
7 rentals vacations packages and cruises. The website advises consumers that the use of the  
8 website is subject to certain terms and conditions and/or a privacy policy that governs the  
9 relationship between consumers and that website, and in particular, how the website will use  
10 and/or disclose or not disclose information that the consumer provides to the website in the  
11 context of the consumer's use of the website to third parties. Nowhere in any of the terms and  
12 conditions and/or in the privacy policy that governed the use of the website did the website  
13 advise that Facebook members would have their information treated differently from other  
14 consumers using the website. Nowhere in any of the terms and conditions and/or in the privacy  
15 policy that governed the use of the website did the website advise Facebook members that their  
16 transactions on the website were, in real time, being communicated to the Facebook website, or  
17 that those transactions included personally identifying information and specific product or  
18 service information in conjunction with the disclosure of their identity.

19           152. Defendant STA owns and operates a publicly accessible website for products  
20 and/or services that it makes available to consumers throughout California and the United  
21 States. Consumer services are available through its website, and consumers can use the service  
22 its website makes available to purchase air transportation, lodging, tours, and ground  
23 transportation. The website advises consumers that the use of the website is subject to certain  
24  
25  
26  
27  
28

1 terms and conditions and/or a privacy policy that governs the relationship between consumers  
2 and that website, and in particular, how the website will use and/or disclose or not disclose  
3 information that the consumer provides to the website in the context of the consumer's use of  
4 the website to third parties. Nowhere in any of the terms and conditions and/or in the privacy  
5 policy that governed the use of the website did the website advise that Facebook members  
6 would have their information treated differently from other consumers using the website.  
7  
8 Nowhere in any of the terms and conditions and/or in the privacy policy that governed the use  
9 of the website did the website advise Facebook members that their transactions on the website  
10 were, in real time, being communicated to the Facebook website, or that those transactions  
11 included personally identifying information and specific product or service information in  
12 conjunction with the disclosure of their identity.  
13

14           153. Defendant GameFly owns and operates a publicly accessible website for  
15 products and/or services that it makes available to consumers throughout California and the  
16 United States. Consumer services are available through its website, and consumers can use the  
17 service its website makes available for video game rentals. The website advises consumers that  
18 the use of the website is subject to certain terms and conditions and/or a privacy policy that  
19 governs the relationship between consumers and that website, and in particular, how the website  
20 will use and/or disclose or not disclose information that the consumer provides to the website in  
21 the context of the consumer's use of the website to third parties. Nowhere in any of the terms  
22 and conditions and/or in the privacy policy that governed the use of the website did the website  
23 advise that Facebook members would have their information treated differently from other  
24 consumers using the website. Nowhere in any of the terms and conditions and/or in the privacy  
25 policy that governed the use of the website did the website advise Facebook members that their  
26  
27  
28

1 transactions on the website were, in real time, being communicated to the Facebook website, or  
2 that those transactions included personally identifying information and specific product or  
3 service information in conjunction with the disclosure of their identity.

4  
5 154. The Consumer Legal Remedies Act (“CLRA”) applies to the CLRA Defendant’s  
6 actions and the conduct described herein because it extends to transactions that are intended to  
7 result, or which have resulted, in the sale of goods or services to consumers.

8  
9 155. Plaintiffs and each member of the Class are “consumers” within the meaning of  
10 Civil Code Section 1761 (d).

11  
12 156. The goods and services that are the subject of this litigation are “goods” and/or  
13 “services” within the meaning of Civil Code Section 1761 (a).

14  
15 157. The CLRA Defendants have violated the CLRA in at least the following  
16 respects:

- 17  
18 ■ In violation of Section 1770 (a)(5) he CLRA Defendants have represented that  
19 the use of their websites have characteristics, uses, benefits, or quantities which  
20 they do not have;
- 21  
22 ■ In violation of Section 1770 (a)(14), the CLRA Defendants have represented that  
23 the use of their websites confers or involves rights, remedies, or obligations  
24 which it does not have or involve, or which are prohibited by law.

25  
26 158. The CLRA Defendants concealed material facts regarding the use and  
27 implementation of their websites from Plaintiffs and other Class members, including the  
28 existence of the Beacon Program which automatically communicated real-time information  
regarding transactions of the consumer on the website to the Facebook website, including

1 personally identifying information and specific product or service information in conjunction  
2 with the disclosure of their identity.

3 159. This type of information is relied upon by consumers in making purchase  
4 decisions, and is fundamental to the decision to purchase goods or services from one seller or  
5 another.  
6

7 160. Had the CLRA Defendants disclosed this material information regarding the  
8 presence, existence, and function of the Beacon program to Plaintiffs and the other Class  
9 members, they would not have purchased the goods and /or services from their website.  
10

11 161. Plaintiffs and other Class members relied upon the CLRA Defendant's  
12 misrepresentations to their detriment.

13 162. The CLRA Defendants failure to disclose the presence, existence, and function  
14 of the Beacon program to Plaintiffs and the other Class members are omissions and  
15 concealments of material fact that constitute unfair, deceptive, and misleading business  
16 practices in violation of Civil Code Section 1770 (a).  
17

18 163. The CLRA Defendants deceptive acts and omissions occurred in the course of  
19 selling a consumer product or service and have occurred continuously through the filing of this  
20 Complaint.  
21

22 164. As a direct and proximate result of The CLRA Defendant's violation of Civil  
23 Code Section 1770, et seq., Plaintiffs and other Class members have suffered irreparable harm.  
24 Plaintiffs, on behalf of themselves and on behalf of a similarly situated Class of consumers,  
25 seek injunctive relief.

26 **Count VI**  
27 **VIOLATION OF CALIFORNIA'S COMPUTER CRIME LAW ("CCCL")**  
28 **CAL. PENAL CODE § 502**  
**against Facebook, Fandango, Hotwire, STA, and GameFly**

**(Hereinafter "CCCL California Defendants")**

1  
2 165. Plaintiffs incorporate the above allegations by reference as if set forth herein at  
3 length.

4  
5 166. The CCCL Defendants have violated California Penal Code § 502(c)(1) by  
6 knowingly and without permission, accessing, taking, copying, and making use of data from  
7 Plaintiffs' computers in order to wrongfully obtain valuable private data from Plaintiffs.

8  
9 167. The CCCL Defendants have violated California Penal Code § 502(c)(2) by  
10 knowingly and without permission, accessing and taking data from Plaintiffs computers.

11  
12 168. The CCCL Defendants have violated California Penal Code § 502(c)(6) by  
13 knowingly and without permission providing, or assisting in providing, a means of accessing  
14 Plaintiff's computers, computer system, and/or computer network.

15  
16 169. The CCCL Defendants have violated California Penal Code § 502(c)(7) by  
17 knowingly and without permission accessing, or causing to be accessed, Plaintiffs' computer  
18 system, and/or computer network.

19  
20 170. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant"  
21 means any set of computer instructions that are designed to . . . record, or transmit information  
22 within a computer, computer system, or computer network without the intent or permission of  
23 the owner of the information. The CCCL Defendants have violated California Penal Code §  
24 502(c)(8) by knowingly and without permission introducing a computer contaminant into the  
25 transactions between Plaintiffs and the CCCL defendants.

26  
27 171. As a direct and proximate result of CCCL Defendants' unlawful conduct within  
28 the meaning of California Penal Code § 502, CCCL Defendants have caused loss to Plaintiffs in

1 an amount to be proven at trial. Plaintiffs are also entitled to recover their reasonable attorneys'  
2 fees pursuant to California Penal Code § 502(e).

3 172. Plaintiffs have also suffered irreparable injury from these unauthorized acts of  
4 disclosure, and due to the continuing threat of such injury, have no adequate remedy at law,  
5 entitling Plaintiffs to injunctive relief.  
6

7 **Count VII**  
8 **VIOLATION OF FEDERAL COMPUTER FRAUD AND ABUSE ACT**  
9 **18 U.S.C. §§ 1030(a)(2)(C) & (a)(5)**  
10 **Against All Defendants**

11 173. Plaintiffs incorporate the above allegations by reference as if set forth herein at  
12 length.

13 174. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. §  
14 1030(a)(2)(C), by intentionally accessing a computer used for interstate commerce or  
15 communication, without authorization or by exceeding authorized access to such a computer,  
16 and by obtaining information from such a protected computer.

17 175. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. §  
18 1030(a)(5)(A)(i) by knowingly causing the transmission of a program, information, code, or  
19 command and as a result causing a loss to one or more persons during any one-year period  
20 aggregating at least \$5,000 in value.  
21

22 176. Plaintiffs have suffered loss by reason of these violations, including, without  
23 limitation, violation of the right of privacy, disclosure of affiliation and business relationships  
24 between Plaintiffs and internet product and service providers, and disclosure of specific  
25 purchase and transactional information that otherwise is private, confidential, and not of public  
26 record.  
27  
28





1 b) As applicable to the Class *mutatis mutandis*, awarding injunctive and equitable  
2 relief including, *inter alia*: (i) prohibiting Defendants from engaging in the acts  
3 alleged above; (ii) requiring Defendants to disgorge all of their ill-gotten gains to  
4 Plaintiffs and the other Class members, or to whomever the Court deems  
5 appropriate; (iii) requiring Defendants to delete all data surreptitiously or  
6 otherwise collected through the acts alleged above; (iv) requiring Defendants to  
7 provide Plaintiffs and the other class members a means to easily and permanently  
8 decline any participation in the Beacon program and an opportunity to decline  
9 any future iteration of the Beacon program; (v) awarding Plaintiffs and class  
10 members full restitution of all benefits wrongfully acquired by Defendant by  
11 means of the wrongful conduct alleged herein; and (vi) ordering an accounting  
12 and constructive trust imposed on the data, funds, or other assets obtained by  
13 unlawful means as alleged above, to avoid dissipation, fraudulent transfers,  
14 and/or concealment of such assets by Defendants;

15  
16  
17  
18 c) For a preliminary and permanent injunction restraining Defendants, their  
19 officers, agents, servants, employees, and attorneys, and those in active concert  
20 or participation with any of them from:

21 (1) transmitting any information about Plaintiffs or class member's  
22 activities on any of the Facebook Beacon Activated Affiliates' websites  
23 to any other websites, including Facebook;

24  
25 (2) transmitting any information about Plaintiffs or class member's  
26 activities on any of the Facebook Beacon Activated Affiliates' websites  
27 to any other websites, including Facebook without fair, clear and  
28

1 conspicuous notice of the intent to transmit information, including a  
2 full description of all information for transmission;

3 (3) transmitting any information about Plaintiffs or class member's  
4 activities on any of the Facebook Beacon Activated Affiliates' websites  
5 to any other websites, including Facebook without fair, clear and  
6 conspicuous opportunity to decline the transmittal prior to any  
7 transmission of data or information;

8  
9 d) Awarding damages, including statutory damages where applicable, to the Class  
10 in an amount to be determined at trial (for purposes of clarity, no damages are  
11 sought at present with respect to Plaintiffs' claims brought pursuant to the  
12 CLRA);

13  
14 e) Awarding Plaintiffs reasonable attorney's fees and costs;

15 f) Awarding pre- and post-judgment interest; and

16 g) Granting such other and further relief as the Court may deem just and proper.  
17

18 **JURY TRIAL DEMAND**

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

20 Respectfully submitted,

21 DATED this 12th day of August, 2008.

22   
23 By: Alan Himmelfarb

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

Alan Himmelfarb  
KamberEdelson, LLC  
2757 Leonis Blvd  
Vernon, California 90058-2304  
Telephone: (323) 585-8696  
[ahimmelfarb@kamberedelson.com](mailto:ahimmelfarb@kamberedelson.com)

Scott A. Kamber  
KamberEdelson, LLC  
11 Broadway, 22nd Floor.  
New York, NY. 10004  
Telephone: (212) 920-3072  
Fax: (212) 202-6364  
[skamber@kamberedelson.com](mailto:skamber@kamberedelson.com)

Joseph H. Malley  
Law Office of Joseph H. Malley  
1045 North Zang Boulevard  
Dallas, Texas 75208  
Ph. (214) 943-6100  
Fax (214) 943-6170  
[malleylaw@gmail.com](mailto:malleylaw@gmail.com)  
*(Pro Hac Vice Pending)*

*Counsel for Plaintiffs*