0923184

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	
FACEBOOK, INC.,	)	
a corporation.	)	**DOCKET NO. C-**

COMPLAINT

The Federal Trade Commission, having reason to believe that Facebook, Inc., a corporation ("Respondent") has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Facebook, Inc. ("Facebook"), is a privately-owned, Delaware corporation with its principal office or place of business at 1601 S. California Avenue, Palo Alto, California 94304.

2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

FACEBOOK'S BUSINESS PRACTICES

3. Since at least 2004, Facebook has operated www.facebook.com, a social networking website. Users of the site create online profiles, which contain content about them such as their name, interest groups they join, the names of other users who are their "friends" on the site, photos albums and videos they upload, and messages and comments they post or receive from their friends. Users also may add content to other users' profiles by sharing photos, sending messages, or posting comments. As of August 2011, Facebook had approximately 750 million users.

4. Since approximately May 2007, Facebook has operated the Facebook Platform ("Platform"), a set of tools and programming interfaces that enables third parties to

develop, run, and operate software applications, such as games, that users can interact with online ("Platform Applications").

5. Facebook obtains revenue by placing third-party advertisements on its site and by selling Facebook Credits, a virtual currency that it offers on its website and through retail outlets. The company also has obtained revenue from fees paid by applicants for its Verified Apps program, described below in Paragraphs 43-47. In 2009, the company had revenues of approximately $777.2 million.

FACEBOOK'S COLLECTION AND STORAGE OF USER INFORMATION

6. Facebook has collected extensive "profile information" about its users, including, but not limited to:

   a. mandatory information that a user must submit to register with the site, including Name, Gender, Email Address, and Birthday;

   b. optional information that a user may submit, such as:

      i. Profile Picture;
      ii. Hometown;
      iii. Interested in (*i.e.*, whether a user is interested in men or women);
      iv. Looking for (*i.e.*, whether a user is looking for friendship, dating, a relationship, or networking);
      v. Relationships (*e.g.*, marital or other relationship status and the names of family members);
      vi. Political and Religious Views;
      vii. Likes and Interests (*e.g.*, activities, interests, music, books, or movies that a user likes); and
      viii. Education and Work (*e.g.*, the name of a user's high school, college, graduate school, and employer);

      and

   c. other information that is based on a user's activities on the site over time, such as:

      i. a Friend List (*i.e.*, a list of users with whom a user has become "Friends" on the site);
      ii. Pages (*e.g.*, any web page on Facebook's web site, belonging to an organization, brand, interest group, celebrity, or other entity, that a user has clicked an online button to "fan" or "like");
      iii. Photos and Videos, including any that a user has uploaded or been "tagged in" (*i.e.*, identified by a user such that his or her name is displayed when a user "hovers" over the likeness); and

iv. messages that a user posts and comments made in response to other users' content.

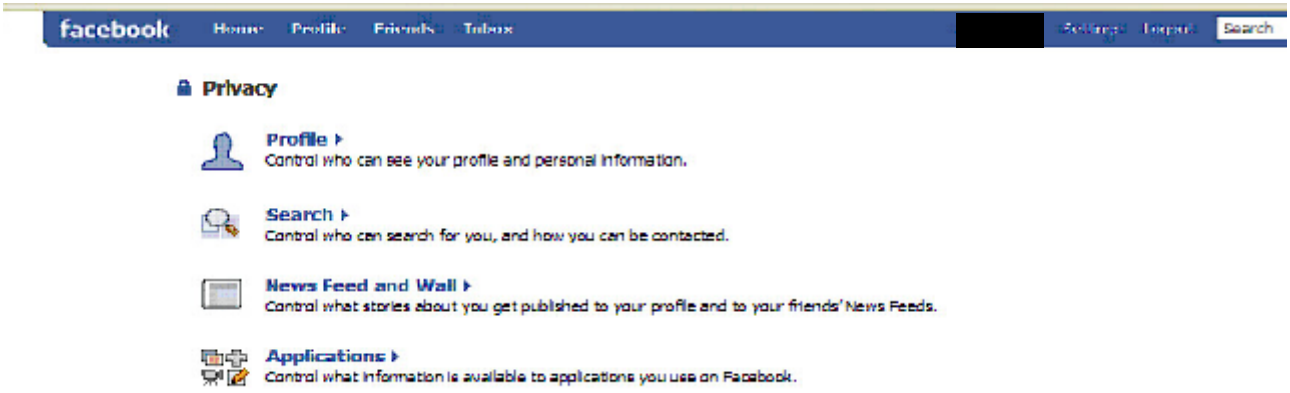
7. Each user's profile information becomes part of the user's online profile and can be accessible to others, as described below.

8. Facebook has stored users' profile information on a computer network that it controls. It has assigned to each user a User Identification Number ("User ID"), a persistent, unique number that Platform Applications and others can use to obtain certain profile information from Facebook.

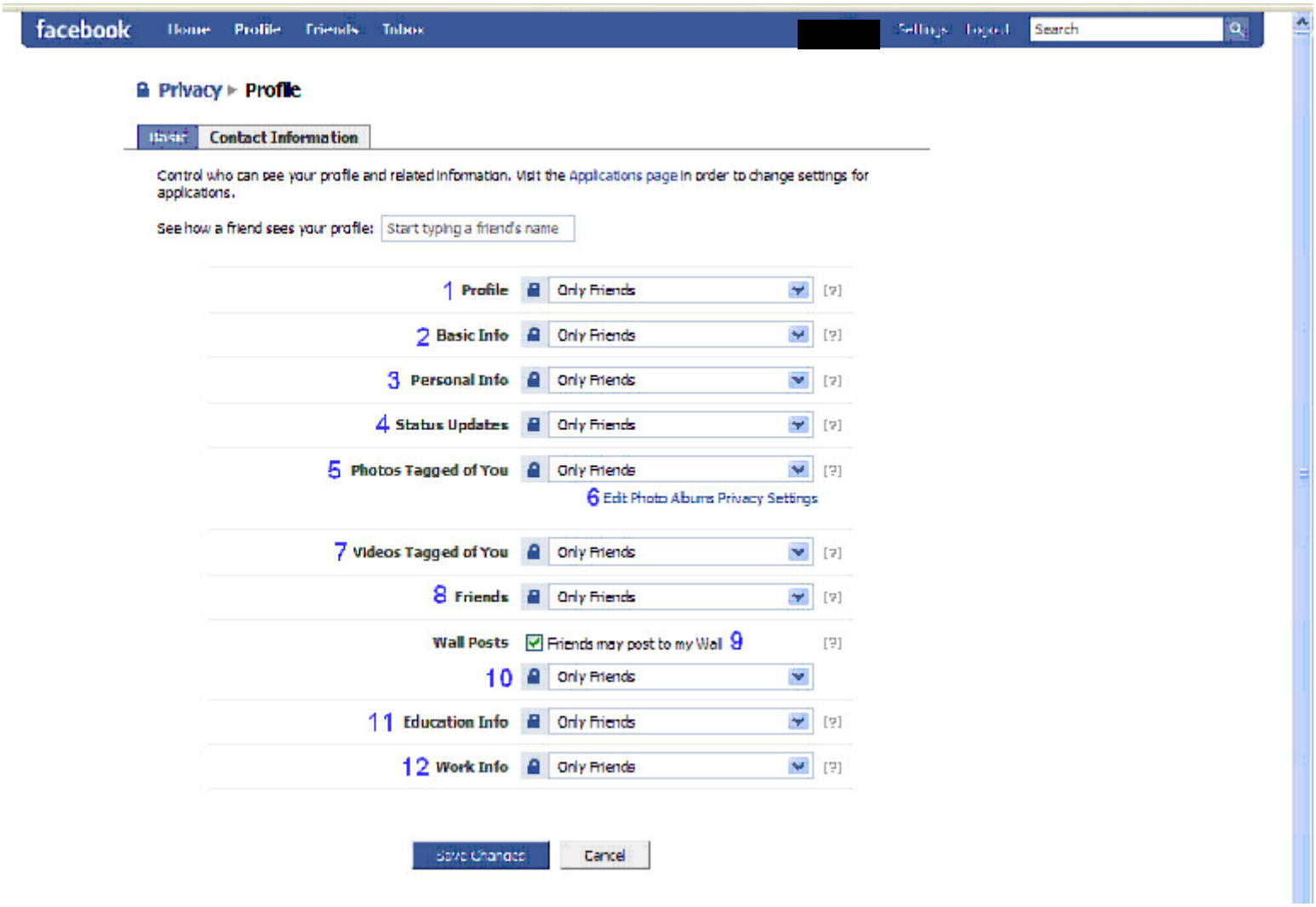
9. Facebook has designed its Platform such that Platform Applications can access user profile information in two main instances. First, Platform Applications that a user authorizes can access the user's profile information. Second, if a user's "Friend" authorizes a Platform Application, that application can access certain of the user's profile information, even if the user has not authorized that Application. For example, if a user authorizes a Platform Application that provides reminders about Friends' birthdays, that application could access, among other things, the birthdays of the user's Friends, even if these Friends never authorized the application.

FACEBOOK'S DECEPTIVE PRIVACY SETTINGS
(Count 1)

10. Since at least November 2009, Facebook has, in many instances, provided its users with a "Central Privacy Page," the same or similar to the one depicted below. Among other things, this page has contained a "Profile" link, with accompanying text that has stated "[c]ontrol who can see your profile and personal information."



11. When users have clicked on the "Profile" link, Facebook has directed them to a "Profile Privacy Page," the same or similar to the one depicted below, which has stated that users could "[c]ontrol who can see your profile and related information." For each "Profile Privacy Setting," depicted below, users could click on a drop-down menu and restrict access to specified users, *e.g.*, "Only Friends," or "Friends of Friends."



12. Although the precise language has changed over time, Facebook's Central Privacy Page and Profile Privacy Page have, in many instances, stated that the Profile Privacy Settings allow users to "control who can see" their profile information, by specifying who can access it, *e.g.*, "Only Friends" or "Friends of Friends." (*See* Central Privacy Page and Profile Privacy Page screenshots, Exhibit A).

13. Similarly, although the precise interface has changed over time, Facebook's Profile Privacy Settings have continued to specify that users can restrict access to their profile information to the audience the user selects, *e.g.*, "Only Friends," "Friends of Friends." (*See* Profile Privacy Page screenshots, Exhibits A, B). In many instances, a user's Profile Privacy Settings have been accompanied by a lock icon. *Id.*

14. None of the pages described in Paragraphs 10-13 have disclosed that a user's choice to restrict profile information to "Only Friends" or "Friends of Friends" would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to "Only Friends" or "Friends of Friends" accessible to any Platform Applications that the user's Friends have used (hereinafter "Friends' Apps"). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (*e.g.*, schools attended), place of employment, photos, and videos.

15. Facebook's Central Privacy Page and Profile Privacy Page have included links to "Applications," "Apps," or "Applications and Websites" that, when clicked, have taken users to a page containing "Friends' App Settings," which would allow users to restrict the information that their Friends' Apps could access.

16. However, in many instances, the links to "Applications," "Apps," or "Applications and Websites" have failed to disclose that a user's choices made through Profile Privacy Settings have been ineffective against Friends' Apps. For example, the language alongside the Applications link, depicted in Paragraph 10, has stated, "[c]ontrol what information is available to applications **you use** on Facebook." (Emphasis added). Thus, users who did not themselves use applications would have had no reason to click on this link, and would have concluded that their choices to restrict profile information through their Profile Privacy Settings were complete and effective.

Count 1

17. As described in Paragraphs 10-13, Facebook has represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends."

18. In truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends" through their Profile Privacy Settings. Instead, such information could be accessed by Platform

Applications that their Friends used. Therefore, the representation set forth in Paragraph 17 constitutes a false or misleading representation.

FACEBOOK'S UNFAIR AND DECEPTIVE DECEMBER 2009 PRIVACY CHANGES (Count 2 and Count 3)

19. On approximately November 19, 2009, Facebook changed its privacy policy to designate certain user information as "publicly available" ("PAI"). On approximately December 8, 2009, Facebook began implementing the changes referenced in its new policy ("the December Privacy Changes") to make public in new ways certain information that users previously had provided.

20. Before December 8, 2009, users could, and did, use their Friends' App Settings to restrict Platform Applications' access to their PAI. For example, as of November 2009, approximately 586,241 users had used these settings to "block" Platform Applications that their Friends used from accessing any of their profile information, including their Name, Profile Picture, Gender, Friend List, Pages, and Networks. Following the December Privacy Changes, Facebook users no longer could restrict access to their PAI through these Friends' App Settings, and all prior user choices to do so were overridden.

21. Before December 8, 2009, users could, and did, use their Profile Privacy Settings to limit access to their Friend List. Following the December Privacy Changes, Facebook users could no longer restrict access to their Friend List through their Profile Privacy Settings, and all prior user choices to do so were overridden, making a user's Friend List accessible to other users. Although Facebook reinstated these settings shortly thereafter, they were not restored to the Profile Privacy Settings and instead were effectively hidden.

22. Before December 8, 2009, users could, and did, use their Search Privacy Settings (available through the "Search" link on the Privacy Settings Page depicted in Paragraph 11) to restrict access to their Profile Picture and Pages from other Facebook users who found them by searching for them on Facebook. For example, as of June 2009, approximately 2.5 million users who had set their Search Privacy Settings to "Everyone," still hid their Profile Picture. Following the December Privacy Changes, Facebook users could no longer restrict the visibility of their Profile Picture and Pages through these settings, and all prior user choices to do so were overridden.

23. To implement the December Privacy Changes, Facebook required each user to click through a multi-page notice, known as the Privacy Wizard, which was composed of:

    a. an introductory page, which announced:

> We're making some changes to give you more control of your information and help you stay connected. We've simplified the Privacy page and added the ability to set privacy on everything you share, from status updates to photos.

> At the same time, we're helping everyone find and connect with each other by keeping some information – like your name and current city – publicly available. The next step will guide you through choosing your privacy settings.

b. privacy update pages, which required each users to choose, via a series of radio buttons, between new privacy settings that Facebook "recommended" and the user's "Old Settings," for ten types of profile information (*e.g.*, Photos and Videos of Me, Birthday, Family and Relationships, etc.), and which stated:

> Facebook's new, simplified privacy settings give you more control over the information you share. We've recommended settings below, but you can choose to apply your old settings to any of the fields.

and

c. a confirmation page, which summarized the user's updated Privacy Settings.

(*See* Privacy Wizard screenshots, Exhibit C).

24. The Privacy Wizard did not disclose adequately that users no longer could restrict access to their newly-designated PAI via their Profile Privacy Settings, Friends' App Settings, or Search Privacy Settings, or that their existing choices to restrict access to such information via these settings would be overridden. For example, the Wizard did not disclose that a user's existing choice to share his or her Friend List with "Only Friends" would be overridden, and that this information would be made accessible to the public.

25. The information that Facebook failed to disclose as described in Paragraph 24 was material to Facebook users.

26. Facebook's designation of PAI caused harm to users, including, but not limited to, threats to their health and safety, and unauthorized revelation of their affiliations. Among other things:

a. certain users were subject to the risk of unwelcome contacts from persons who may have been able to infer their locale, based on the locales of their Friends (*e.g.*, their Friends' Current City information) and of the organizations reflected in their Pages;

b. each user's Pages became visible to anyone who viewed the user's profile, thereby exposing potentially controversial political views or other sensitive information to third parties – such as prospective employers, government organizations, or business competitors – who sought to obtain personal information about the user;

c. each user's Friend List became visible to anyone who viewed the user's profile, thereby exposing potentially sensitive affiliations, that could, in turn, reveal a user's political views, sexual orientation, or business relationships, to third parties – such as prospective employers, government organizations, or business competitors – who sought to obtain personal information about the user; and

d. each user's Profile Photo became visible to anyone who viewed the user's profile, thereby revealing potentially embarrassing or political images to third parties whose access users previously had restricted.

Count 2

27. As described in Paragraph 23, Facebook has represented, expressly, or by implication, that its December Privacy Changes provided users with "more control" over their information, including by allowing them to preserve their "Old Settings," to protect the privacy of their profile information.

28. As described in Paragraph 24-26, Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them. Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks. These facts would be material to consumers. Therefore, Facebook's failure to adequately disclose these facts, in light of the representation made, constitutes a deceptive act or practice.

Count 3

29. As described in Paragraphs 19-26, by designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice constitutes an unfair act or practice.

SCOPE OF PLATFORM APPLICATIONS' ACCESS TO FACEBOOK USERS' INFORMATION
(Count 4)

30. Facebook has disseminated or caused to be disseminated numerous statements to users stating that Platform Applications they use will access only the profile information these applications need to operate, including, but not limited to:

a. the following statement, which appeared within a dialog box that each user must click through before using a Platform Application for the first time:

> Allowing [name of Application] access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

(Authorization Dialog box, Exhibit D); and

b. the following additional statements on www.facebook.com:

i. Applications you use will access your Facebook information in order for them to work.

(Facebook Privacy Settings: What You Share, Exhibit E); and

ii. When you authorize an application, it will be able to access any information associated with your account that it requires to work.

(Facebook Privacy Settings: How Applications Interact With Your Information, Exhibit F).

31. Contrary to the statements set forth in Paragraph 30, in many instances, a Platform Application could access profile information that was unrelated to the Application's purpose or unnecessary to its operation. For example, a Platform Application with a narrow purpose, such as a quiz regarding a television show, in many instances could access a user's Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook's web site, despite the lack of relevance of this information to the Application.

Count 4

32. As set forth in Paragraph 30, Facebook has represented, expressly or by implication, that it has provided each Platform Application access only to such user profile information as the Application has needed to operate.

33. In truth and in fact, as described in Paragraph 31, from approximately May 2007 until July 2010, in many instances, Facebook has provided Platform Applications unrestricted access to user profile information that such Applications have not needed to operate. Therefore, the representation set forth in Paragraph 32 constitutes a false or misleading representation.

FACEBOOK'S DISCLOSURE OF USER INFORMATION TO ADVERTISERS (Count 5)

34. Facebook has displayed advertisements ("ads") from third-parties ("Platform Advertisers") on its web site.

35. Facebook has allowed Platform Advertisers to target their ads ("Platform Ads") by requesting that Facebook display them to users whose profile information reflects certain "targeted traits," including, but not limited to:

    a. location (*e.g.*, city or state),

    b. age,

    c. sex,

    d. birthday,

    e. "Interested in" responses (*i.e.*, as described in Paragraph 6(b), whether a user is interested in men or women),

    f. Relationship Status,

    g. Likes and Interests,

    h. Education (*e.g.*, level of education, current enrollment in high school or college, affiliation with a particular college, and choice of major in college), and

    i. name of employer.

36. Facebook has disseminated or caused to be disseminated numerous statements that it does not share information about its users with advertisers, including:

    a. Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as . . . personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an

advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

(Facebook Privacy Policy, November 26, 2008, Exhibit G).

b. We don't share information with advertisers without your consent . . . We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are . . . Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement, there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.

(Facebook Privacy Policy, November 19, 2009, Exhibit H).

c. We do not give your content to advertisers. (Facebook Statement of Rights and Responsibilities, May 1, 2009, Exhibit I).

d. Still others asked to be opted-out of having their information shared with advertisers. This reflects a common misconception about advertising on Facebook. We don't share your information with advertisers unless you tell us to ([*e.g.,*] to get a sample, hear more, or enter a contest). Any assertion to the contrary is false. Period . . . we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads.

(Facebook Blog, http://blog.facebook.com/blog.php, "Responding to Your Feedback," Barry Schnitt, April 5, 2010, Exhibit J).

e. We never share your personal information with advertisers. We never sell your personal information to anyone. These protections are yours no matter what privacy settings you use; they apply equally to people who share openly with everyone and to people who share with only select friends.

The only information we provide to advertisers is aggregate and anonymous data, so they can know how many people viewed their ad and general categories of information about them. Ultimately, this helps advertisers better understand how well their ads work so they can show better ads.

(Facebook Blog, http://blog.facebook.com/blog.php, "The Role of Advertising on Facebook," Sheryl Sandberg, July 6, 2010, Exhibit K).

37. Contrary to the statements set forth in Paragraph 36(a)-(d), in many instances, Facebook has shared information about users with Platform Advertisers by identifying to them the users who clicked on their ads and to whom those ads were targeted. Specifically, from at least September 2008 until May 26, 2010, Facebook designed and operated its web site such that, in many instances, the User ID for a user who clicked on a Platform Ad was shared with the Platform Advertiser.

38. As a result of the conduct described in Paragraph 37, Platform Advertisers potentially could take steps to get detailed information about individual users. For example, a Platform Advertiser could use the User ID to:

a. access the user's profile page on www.facebook.com, to obtain his or her real name, and, after December 8, 2009, other PAI which has included a user's Profile Picture, Gender, Current City, Friend List, Pages, and Networks;

b. combine the user's real name with:

i. any targeted traits used for the ad the user clicked (*e.g.*, if the ad targeted 23-year-old men who were "Interested In" men and "liked" a prescription drug, the advertiser could ascribe these traits to a specific user); and

ii. information about the user's visit to the advertiser's website, including: the time and date of the visit, the pages viewed, and time spent viewing the ad (collectively, "browsing information"); and

c. over time, combine the information described in subparts (a) - (b) with targeting traits related to additional ads or other information about the user's browsing activities across the web.

39. In addition, contrary to the statements set forth in Paragraph 36, Facebook has shared information about users with third parties that advertise on certain Platform Application web sites ("Application Advertisers"), by identifying to them the specific users who visited these applications. Specifically, at various times relevant to this Complaint, when a user visited certain Platform Applications, Facebook disclosed the user's User ID, in plain text, to any Application Advertiser that displayed an ad on the application's web page.

40. As a result of the conduct described in Paragraph 39, Application Advertisers potentially could take steps to get detailed information, similar to those steps described in Paragraph 38(a), (b)(ii), and (c), regarding the user and his or her activities on any Platform Application web site where the advertiser displayed an ad.

Count 5

41. As set forth in Paragraph 36, Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users.

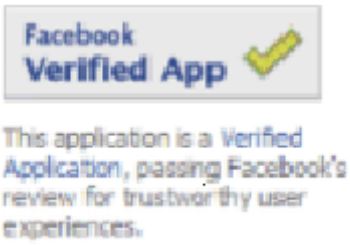
42. In truth and in fact, as described in Paragraphs 37-40, Facebook has provided advertisers with information about its users. Therefore, the representation set forth in Paragraph 41 constitutes a false or misleading representation.

FACEBOOK'S DECEPTIVE VERIFIED APPS PROGRAM (Count 6)

43. From approximately May 2009 until December 2009, Facebook operated a Verified Apps program, through which it designated certain Platform Applications as "Facebook Verified Apps" ("Verified Apps").

44. Facebook provided each Verified App with preferential treatment compared to other Platform Applications, including, but not limited to:

a. a Verified Apps badge, the same or similar to the badge depicted below, for display on the application's profile page on www.facebook.com; and



b. a green check mark alongside the Platform Application's name, and higher ranking among search results, on www.facebook.com and within Facebook's Application Directory.

45. To apply for the Verified Apps badge, a Platform Application developer paid Facebook a fee of $375, or $175 for a student or nonprofit organization. Facebook awarded the badge to approximately 254 Platform Applications.

46. Facebook has disseminated or caused to be disseminated statements to consumers conveying that it has taken steps to verify the security of Verified Apps, compared to the security of other Platform Applications, including:

a. the Verified Apps badge, described in Paragraph 44(a);

b. the Verified Apps green check mark, described in Paragraph 44(b); and

c. the following statements on its website:

i. **Application Verification** Facebook is introducing the Application Verification program **which is designed to offer extra assurances to help users identify applications they can trust -- applications that are secure, respectful and transparent, and have demonstrated commitment to compliance with Platform policies**.

(Press Release, "Facebook Expands Power of Platform Across the Web and Around the World," July 23, 2008, Exhibit L (latter emphasis added)); and

ii. What are Verified Applications?

Verified applications have passed a detailed Facebook review to confirm that the user experience they provide complies with Facebook policies. Verified Applications have committed to be transparent about how they work and will respect you and your friends when they send communication on your behalf.

What is the green check mark next to some applications?

Applications that choose to participate in Facebook's Application Verification Program receive a green check mark when they pass Facebook's detailed review process. The review process is designed to ensure that the application complies with Facebook policies. In addition, Verified applications have committed to be transparent about how they work and will respect you and your friends when they send communication on your behalf.

(Facebook Help Center FAQ, Exhibit M (emphases added)).

47. Contrary to the statements set forth in Paragraph 46, before it awarded the Verified Apps badge, Facebook took no steps to verify either the security of a Verified Application's website or the security the Application provided for the user information it collected, beyond such steps as it may have taken regarding any other Platform Application.

Count 6

48. As set forth in Paragraph 46, Facebook has represented, expressly or by implication, that Facebook has permitted a Platform Application to display its Verified Apps badge when Facebook's review of the security of such Applications has exceeded its review of the security of other Platform Applications.

49. In truth and in fact, as described in Paragraph 47, in many instances Facebook has permitted a Platform Application to display its Verified Apps badge when its review of the application's security has not exceeded its review of other Platform Applications. Therefore, the representation set forth in Paragraph 48 constitutes a false or misleading representation.

FACEBOOK'S DISCLOSURE OF USER PHOTOS AND VIDEOS (Count 7)

50. As described above, Facebook has collected and stored vast quantities of photos and videos that its users upload, including, but not limited to: at least one such photo from approximately ninety-nine percent of its users, and more than 100 million photos and 415,000 videos from its users, collectively, every day.

51. Facebook has stored users' photos and videos such that each one is assigned a Content URL – a uniform resource locator that specifies its location on Facebook's servers. Facebook users and Platform Applications can obtain the Content URL for any photo or video that they view on Facebook's web site by, for example, right-clicking on it. If a user or Application further disseminates this URL, Facebook will "serve" the user's photo or video to anyone who clicks on the URL.

52. Facebook has disseminated or caused to be disseminated statements communicating that a user can restrict access to his or her profile information – including, but not limited to, photos and videos that a user uploads – by deleting or deactivating his or her user account. Such statements include:

a. **Deactivating or deleting your account.** If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted . . . When you delete an account, it is permanently deleted from Facebook.

* * *

Backup copies. Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others;

(Facebook Privacy Policy, November 19, 2009, Exhibit H);

b. To deactivate your account, navigate to the "Settings" tab on the Account Settings page. Deactivation will remove your profile and content associated with your account from Facebook. In addition, users will not be able to search for you or view any of your information.

(Facebook Help Center FAQ, Exhibit N);

> If you deactivate your account, your profile and all information associated with it are immediately made inaccessible to other Facebook users.

(Facebook Help Center FAQ, Exhibit O); and

> If you deactivate your account from the "Deactivate Account" section on the Account page, your profile and all information associated with it are immediately made inaccessible to other Facebook users.

(Facebook Help Center FAQ, Exhibit P).

53. Contrary to the statements set forth in Paragraph 52, Facebook has continued to display users' photos and videos to anyone who accesses Facebook's Content URLs for them, even after such users have deleted or deactivated their accounts.

Count 7

54. As set forth in Paragraph 52, Facebook has represented, expressly or by implication, that after a user has deleted or deactivated his or her account, Facebook does not provide third parties with access to his or her profile information, including any photos or videos that the user has uploaded.

55. In truth and in fact, as described in Paragraph 53, in many instances, Facebook has provided third parties with access to a user's profile information – specifically photos or videos that a user has uploaded – even after the user has deleted or deactivated his or her account. Therefore, the representation set forth in Paragraph 54 constitutes a false or misleading representation.

U.S.-EU SAFE HARBOR FRAMEWORK
(Count 8)

56. The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of the European Union ("EU") that is consistent with the requirements of the European Union Data Protection Directive ("Directive"). The Directive sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission ("EC") has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is commonly referred to as meeting the EU's "adequacy" standard.

57. To satisfy the EU's adequacy standard for certain commercial transfers, the U.S. Department of Commerce ("Commerce") and the EC negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The Safe Harbor is a voluntary

framework that allows U.S. companies to transfer personal data lawfully from the EU to the U.S. To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.

58. The Safe Harbor privacy principles, issued by Commerce on July 21, 2000, include the following:

> **NOTICE:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.
>
> **CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

59. From at least May 10, 2007, until the present, Facebook has maintained a current self-certification to Commerce and has appeared on the list of Safe Harbor companies on the Commerce website. Pursuant to its self-certification, Facebook has transferred data collected from its users in the EU to the U.S. for processing.

60. From approximately May 2007 until the present, Facebook has stated in its Privacy Policy that it participates in, adheres to, and/or complies with "the EU Safe Harbor Privacy Framework as set forth by the United States Department of Commerce." (*See* Facebook Privacy Policy, November 26, 2008, Exhibit G; Facebook Privacy Policy, November 19, 2009, Exhibit H; Facebook Privacy Policy, December 9, 2009, Exhibit Q; Facebook Privacy Policy, April 22, 2010, Exhibit R; Facebook Privacy Policy, December 22, 2010, Exhibit S). Similarly, from approximately November 19, 2009 until the present, Facebook has stated on the Commerce website that it "adheres to the U.S. Safe Harbor Framework developed by the U.S. Department of Commerce and the European Union."

Count 8

61. As described in Paragraphs 59-60, Facebook has represented, expressly or by implication, that it has complied with the U.S. Safe Harbor Privacy Principles, including the principles of Notice and Choice.

62. In truth and in fact, as described in Paragraphs 10-42 and 50-55, in many instances, Facebook has not adhered to the U.S. Safe Harbor Privacy Principles of Notice and Choice. Therefore, the representation set forth in Paragraph 61 constitutes a deceptive act or practice.

63. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ___ day of _____, ____, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary