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

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

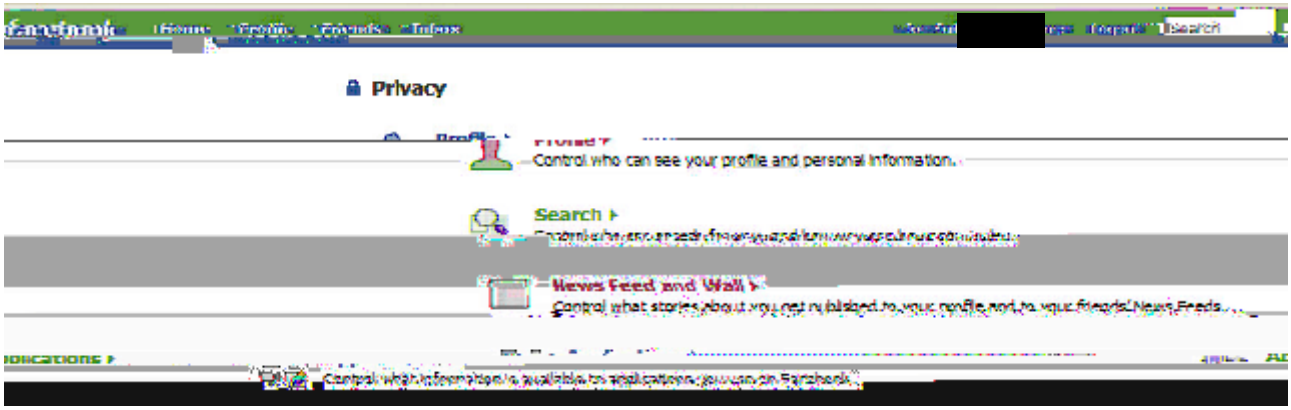
7. Each user's profile information becomes part of the user's online profile and can be accessible to others, as described below.

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.

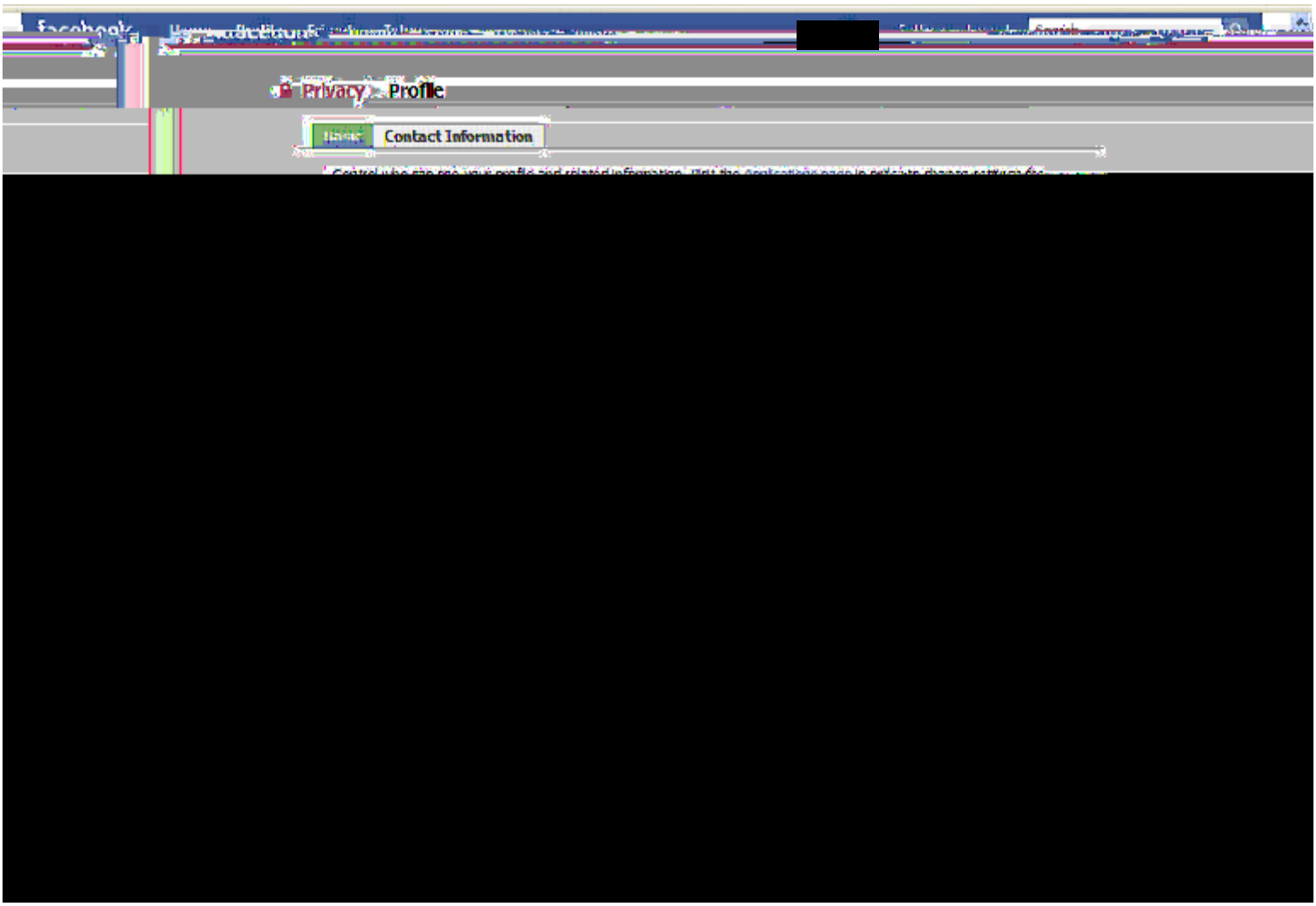
9. Facebook has designed its Platform such that Platform Applications can access user profile information in two main instances. First, Platform Applications that a user authorizes can access the user's profile information. Second, if a user's "Friend" authorizes a Platform Application, that application 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 "

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

FACEBOOK'S

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 37.0.00 0.00 0.00 rg0.00 0.00 0.00 rgBTo4.00b(e)Tj57

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.

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,

0viewtisements. For 1.00000 0.00000 0..000000 1.035ET1.00000 0

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

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 ade

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:

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