JON LEIBOWITZ, Chairman

J. THOMAS ROSCH, Commissioner

EDITH RAMIREZ, Commissioner
Took oath of office April 5, 2010.

JULIE BRILL, Commissioner
Took oath of office April 6, 2010.

MAUREEN K. OHLHAUSEN, Commissioner
Took oath of office April 4, 2012

DONALD S. CLARK, Secretary
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
</table>
| Members of the Commission ..................................................................  
| Table of Cases .................................................................................  
| Findings, Opinions, and Orders .........................................................  
| Interlocutory, Modifying, Vacating, and Miscellaneous Orders ..................  
| Responses to Petitions to Quash ........................................................  
| Table of Commodities ...........................................................................  |

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Members of the Commission ............................................................................ ii</td>
</tr>
<tr>
<td>Table of Cases ............................................................................................... iv</td>
</tr>
<tr>
<td>Findings, Opinions, and Orders ......................................................................... 1</td>
</tr>
<tr>
<td>Interlocutory, Modifying, Vacating, and Miscellaneous Orders ............................. 844</td>
</tr>
<tr>
<td>Responses to Petitions to Quash ....................................................................... 927</td>
</tr>
<tr>
<td>Table of Commodities ..................................................................................... 937</td>
</tr>
</tbody>
</table>
# TABLE OF CASES

## VOLUME 154

<table>
<thead>
<tr>
<th>File or Docket #</th>
<th>Name</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C-4378</td>
<td>ABCSP, Inc.</td>
<td>612</td>
</tr>
<tr>
<td>C-4373</td>
<td>Actavis Inc.</td>
<td>656</td>
</tr>
<tr>
<td>C-4373</td>
<td>Actavis Pharma Holding 4 ehf.</td>
<td>656</td>
</tr>
<tr>
<td>C-4373</td>
<td>Actavis S.á.r.l.</td>
<td>656</td>
</tr>
<tr>
<td></td>
<td>Always Best Care Senior Services, LLC</td>
<td>612</td>
</tr>
<tr>
<td></td>
<td>Ascend Health Corporation</td>
<td>495</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Becton, Dickinson and Company</td>
<td>776</td>
</tr>
<tr>
<td></td>
<td>Biomet, Inc.</td>
<td>104</td>
</tr>
<tr>
<td>C-4375</td>
<td>Brain Pad, Inc.</td>
<td>457</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C-4379</td>
<td>CarePatrol, Inc.</td>
<td>596</td>
</tr>
<tr>
<td></td>
<td>Checknet, Inc.</td>
<td>415</td>
</tr>
<tr>
<td>C-4374</td>
<td>Cooperativa de Farmacias Puertorriqueñas</td>
<td>430</td>
</tr>
<tr>
<td></td>
<td>Coopharma</td>
<td>430</td>
</tr>
<tr>
<td>C-4380</td>
<td>Corning Incorporated</td>
<td>776</td>
</tr>
<tr>
<td>C-4368</td>
<td>CoStar Group, Inc.</td>
<td>213</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Discovery Labware, Inc.</td>
<td>776</td>
</tr>
<tr>
<td></td>
<td>DMG Information, Inc.</td>
<td>213</td>
</tr>
<tr>
<td><strong>E</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C-4370</td>
<td>EPN, Inc.</td>
<td>415</td>
</tr>
<tr>
<td>Case No.</td>
<td>Company/Individual</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------</td>
<td>------</td>
</tr>
<tr>
<td>C-4365</td>
<td>Facebook, Inc.</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Fougera Holdings Inc.</td>
<td>334</td>
</tr>
<tr>
<td></td>
<td>Franklin Toyota/Scion</td>
<td>395</td>
</tr>
<tr>
<td>C-4371</td>
<td>Franklin’s Budget Car Sales, Inc.</td>
<td>395</td>
</tr>
<tr>
<td></td>
<td>Fougera Holdings Inc.</td>
<td>334</td>
</tr>
<tr>
<td></td>
<td>Franklin Toyota/Scion</td>
<td>395</td>
</tr>
<tr>
<td></td>
<td>Google, Inc. (PTQ)</td>
<td>927</td>
</tr>
<tr>
<td></td>
<td>Kinder Morgan, Inc. (Divestiture)</td>
<td>925</td>
</tr>
<tr>
<td>C-4372</td>
<td>Koninklijke Ahold N.V.</td>
<td>183</td>
</tr>
<tr>
<td></td>
<td>Genuardi’s</td>
<td>183</td>
</tr>
<tr>
<td></td>
<td>Giant Carlisle</td>
<td>183</td>
</tr>
<tr>
<td></td>
<td>Google, Inc. (PTQ)</td>
<td>927</td>
</tr>
<tr>
<td>C-4363</td>
<td>Johnson &amp; Johnson</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>McCaffrey’s</td>
<td>183</td>
</tr>
<tr>
<td>C-4369</td>
<td>MySpace, LLC</td>
<td>304</td>
</tr>
<tr>
<td></td>
<td>McWane, Inc. (Interlocutory Order)</td>
<td>867, 869</td>
</tr>
<tr>
<td>C-4372</td>
<td>Miller, Alan B.</td>
<td>495</td>
</tr>
<tr>
<td></td>
<td>Magnesium Elektron North America, Inc.</td>
<td>794</td>
</tr>
<tr>
<td>C-4375</td>
<td>Manzo, Joseph</td>
<td>457</td>
</tr>
<tr>
<td></td>
<td>McCaffrey’s</td>
<td>183</td>
</tr>
<tr>
<td>9351</td>
<td>McWane, Inc. (Interlocutory Order)</td>
<td>867, 869</td>
</tr>
<tr>
<td>C-4368</td>
<td>Lonestar Acquisition Sub, Inc.</td>
<td>213</td>
</tr>
<tr>
<td>C-4381</td>
<td>Magnesium Elektron North America, Inc.</td>
<td>794</td>
</tr>
<tr>
<td>C-4372</td>
<td>Miller, Alan B.</td>
<td>495</td>
</tr>
<tr>
<td></td>
<td>MySpace, LLC</td>
<td>304</td>
</tr>
<tr>
<td>C-4364</td>
<td>Novartis AG</td>
<td>334</td>
</tr>
</tbody>
</table>
P

9344  POM Wonderful LLC (Interlocutory Order) ................................................................. 844, 926

R

9353  Reading Health System ...................................................... 626
Reno Heart Physicians ............................................................... 553
C-4366  Renown Health ................................................................. 553
C-4366  Renown Health (Interlocutory Order) ............. 846
9344  Resnick, Lynda Rae (Interlocutory Order) ................................................................ 844, 926
9344  Resnick, Stewart A. (Interlocutory Order) ................................................................ 844, 926
         Revere Graphics Worldwide, Inc. ..................... 794
9344  Roll International Corp. (Interlocutory Order) ................................................................ 844, 926

S

C-4367  Safeway Inc. ................................................................... 183
Samsung Telecommunications America, LLC ... 927
Sierra Nevada Cardiology Associates ..................... 553
9351  Star Pipe Products, Ltd. (Interlocutory Order) .............................................................. 867, 869
9353  Surgical Institute of Reading ................................... 626
Synthes, Inc. ................................................................. 104

T

Tallgrass Energy Partners LP .................................................. 925
Tolmar, Inc. .............................................................................. 334
9344  Tupper, Matthew (Interlocutory Order) ................................................................. 844, 926

U

Universal Engraving, Inc. ......................................................... 794
C-4372  Universal Health Services, Inc. ........................................ 495

W

C-4373  Watson Pharmaceuticals Inc. ........................................ 656
| Xceligent, Inc. | 213 |

TABLE OF CASES
continued
This consent order addresses Facebook, Inc.’s claims regarding the privacy of users personal information while accessing and using their website. The complaint alleges that Facebook violated Section 5(a) of the Federal Trade Commission Act by allowing Apps and advertisers access to users’ account information without adequately disclosing these policies to consumers. The complaint also alleges that Facebook falsely claimed to comply with the U.S.-EU Safe Harbor Framework. The consent order prohibits Facebook from misrepresenting the privacy or security of “covered information,” as well as the company’s compliance with any privacy, security, or other compliance program, including but not limited to the U.S.-EU Safe Harbor Framework.

Participants

For the Commission: Laura D, Berger, Cora T. Han, David Lincicum, Manas Mohapatra, Kandi Parsons and Laura Riposo VanDruff.

For the Respondent: Ashlie Beringer, Sean Royall, and Eugene Scalia, Gibson, Dunn & Crutcher LLP.

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 Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025.

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 March 2012, Facebook had approximately 900 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:
Complaint

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
Complaint

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
Complaint

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;
Complaint

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 Paragraphs 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
Complaint

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).
Complaint

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.


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
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”).
Complaint

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

   ![Verified App Badge]

   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
Complaint

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.
Complaint

**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.
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 twenty-seventh day of July, 2012, has issued this complaint against Respondent.

By the Commission, Commissioner Rosch dissenting and Commissioner Ohlhausen not participating.
Complaint

Exhibit A
Complaint

Exhibit C
Complaint
Privacy wizard: Step three
Allow Access?

Allowing access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

Allow or cancel

By proceeding, you are allowing to access your information and you are agreeing to the Facebook Terms of Use in your use of the Terms of Service.
Complaint

Exhibit E
This policy is effective as of November 26, 2008.

Facebook Principles:
We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook, that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

1. You should have control over your personal information.
   Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

2. You should have access to the information others want to share.
   There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com.

Safe Use of Facebook
For information for users and parents about staying safe on Facebook, click here.

Facebook’s Privacy Policy

Facebook’s Privacy Policy is designed to help you understand how we collect and use the personal information you decide to share, and help you make informed decisions when using Facebook, located at www.facebook.com and its directly associated domains (collectively, “Facebook” or “Website”).
Complaint

By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.

Facebook is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. This privacy statement covers the site www.facebook.com and its directly associated domains. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

If you have questions or concerns regarding this statement, you should first contact our privacy staff at privacy@facebook.com. If you do not receive acknowledgment of your inquiry or your inquiry has not been satisfactorily addressed, you should contact TRUSTe's Watchdog at http://www.truste.org/consumer/watchdog_complaint.php. TRUSTe will then serve as a liaison with us to resolve your concerns.

EU Safe Harbor Participation
We participate in the EU Safe Harbor Privacy Framework as set forth by the United States Department of Commerce. As part of our participation in the safe harbor, we have agreed to TRUSTe dispute resolution for disputes relating to our compliance with the Safe Harbor Privacy Framework. If you have any complaints regarding our compliance with the Safe Harbor you should first contact us at privacy@facebook.com. If contacting us does not resolve your complaint, you may raise your complaint with TRUSTe at http://www.truste.org/consumer/whcd_watchdog_intro.html.

The Information We Collect
When you visit Facebook, you provide us with two types of information: personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site.

When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us.

When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain
Complaint

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 user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you 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.

When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you with services and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable recovery to the prior version of that information.

You post User Content [as defined in the Facebook Terms of Use] on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impervious. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.

Any improper collection or misuse of information provided on Facebook is in violation of the Facebook Terms of Service and should be reported to privacy@facebook.com.

If you choose to use our invitation service to tell a friend about our site, we will ask you for information needed to send the invitation, such as your friend's email address. We will send your friend an email or instant message in your name inviting him or her to visit the site, and may send up to two reminders to them. Facebook stores this information to send invitations and reminders, to register a friend connection if your invitation is accepted, to allow you to see invitations
by using Facebook, you are consenting to have your personal data transferred to and processed in the United States.

Children Under Age 13
Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us at privacy@facebook.com.

Children Between the Ages of 13 and 18
We recommend that minors over the age of 13 ask their parents for permission before sending any information about themselves to anyone over the Internet.

Use of Information Obtained by Facebook
When you register with Facebook, you create your own profile and privacy settings. Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook. We may occasionally use your name and email address to send you notifications regarding new services offered by Facebook that we think you may find valuable.

Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings in some cases where:
your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile.

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, network names, and profile picture thumbnail will be available in search results across the Facebook network, and those limited pieces of information may be made available to third-party search engines. This is primarily so your friends can find you and send a friend request. People who see your name in searches, however, will not be able to access your profile information unless they have a relationship to you (friend, friend of friend, member of your networks, etc.) that allows such access based on your privacy settings.

Facebook may send you service-related announcements from time to time through the general operation of the service. For instance, if a friend sends you a new message or pokes, or someone posts on your wall, you may receive an email alerting you to that fact.

Generally, you may opt out of such emails from the Notifications page, though Facebook reserves the right to send you notices about your account even if you opt out of all voluntary email notifications.

Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and 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.

We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile. Where such information is used, we generally allow you to specify in your privacy settings that you do not want this to be done or to
take other actions that limit the connection of this information to your profile (e.g., removing photo tag links).

Sharing Your Information with Third Parties
Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service; 2) legally required or 3) permitted by you. For example:

Your News Feed and Wall may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your News Feed and Wall on your Privacy page.

Unlike most sites on the Web, Facebook limits access to site information by third-party search engines "crawlers" (e.g., Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond your name, profile picture, and limited aggregated data about your profile (e.g., number of wall postings).

We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Facebook-specified purposes.

If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt out of any...
Complaint

sharing of certain or all information through Platform Applications on the Privacy Settings page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data. Before allowing any Platform Developer to make any Platform Application available to you, Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limit their collection, use, and storage of your information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we of course cannot and do not guarantee that all Platform Developers will abide by such agreements. Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you, so please make sure to review those terms and policies carefully before using any Platform Application. You can report any suspected misuse of information through the Facebook Platform and we will investigate any such claim and take appropriate action against the Platform Developer up to and including terminating their participation in the Facebook Platform and/or other formal legal action.

We occasionally provide demonstration accounts that allow new users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.

We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.

We let you choose to share information with marketers or electronic commerce providers through on-site offers."
We may offer services or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service. Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collect certain information from that site and present it to you after you have completed an action on that site. You have the choice to have Facebook disclose that information, or to share it with your friends.

To learn more about the operation of the service, we encourage you to read the tutorial here. To opt out of the service altogether, click here. Like many other websites that interact with third party sites, we may receive some information even if you are logged out from Facebook, or that pertains to non-Facebook users, from those sites in conjunction with the technical operation of the system. In cases where Facebook receives information on users that are not logged in, or on non-Facebook users, we do not attempt to associate it with individual Facebook accounts and will discard it.

If the ownership of all or substantially all of the Facebook business, or individual business units owned by Facebook, Inc., were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in any pre-existing Privacy Policy.

When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos, Marketplace listings or other information, may be shared with other users in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items, this information may become publicly available.

Links
Facebook may contain links to other websites. We are not responsible for the privacy practices of other web sites. We encourage our users to be aware when they leave our site to read the privacy statements of each and every website that collects personally identifiable information. This Privacy Policy applies solely to information collected by Facebook.
Third Party Advertising
Advertisements that appear on Facebook are sometimes delivered (or "served") directly to users by third party advertisers. They automatically receive your IP address when this happens. These third party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer each time they send you an advertisement in order to measure the effectiveness of their ads and to personalize advertising content. In this way, they may compile information about whose individuals using your computer or browser saw their advertisements and determine which advertisements are clicked. Facebook does not have access to or control of the cookies that may be placed by the third party advertisers. Third party advertisers have no access to your contact information stored on Facebook unless you choose to share it with them.

This privacy policy covers the use of cookies by Facebook and does not cover the use of cookies or other tracking technologies by any of its advertisers.

Changing or Removing Information
Access and control over most personal information on Facebook is readily available through the profile editing tools. Facebook users may modify or delete any of their profile information at any time by logging into their account. Information will be updated immediately. Individuals who wish to deactivate their Facebook account may do so on the My Account page. Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g., sending a personal message to another Facebook user) you generally cannot remove such communications.

Security
Facebook takes appropriate precautions to protect our users' information. Your account information is located on a secured server behind a firewall. When you enter sensitive information (such as credit card number or your password), we encrypt that information using secure socket layer technology (SSL). To learn more about SSL, go to http://en.wikipedia.org/wiki/Secure_Sockets_Layer.
Complaint

Because email and instant messaging are not recognized as secure communications, we request that you not send private information to us by email or instant messaging services. If you have any questions about the security of Facebook Web Site, please contact us at privacy@facebook.com.

Terms of Use, Notices and Revisions
Your use of Facebook, and any disputes arising from it, is subject to this Privacy Policy as well as our Terms of Use and all of its dispute resolution provisions, including arbitration, limitation on damages and choice of law. We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy’s new effective date. If we make material changes to this policy, we will notify you here, by email, or through notice on our home page. We encourage you to refer to this policy on an ongoing basis so that you understand our current privacy policy. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account.

Contacting the Web Site
If you have any questions about this privacy policy, please contact us at privacy@facebook.com. You may also contact us by mail at 156 University Avenue, Palo Alto, CA 94301.
Facebook™'s Privacy Policy.

Date of last revision: November 19, 2009.

We want to earn your trust by being transparent about how Facebook works. You should read this policy in its entirety, but should pay particular attention to these three highlights:

- Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings. You should review the default privacy settings and change them if necessary to reflect your preferences. You should also consider your settings whenever you share information.

- Facebook is not just a website. It is also a service for sharing your information on Facebook-connected applications and websites. You can control how you share information with those third-party applications and websites through your application settings and you can learn more about how information is shared with them on our About Platform page. You can also limit how your friends share your information with applications through your privacy settings.

- Facebook is a free service supported primarily by advertising. We will not share your information with advertisers without your consent. We allow advertisers to select characteristics of users they want to show their advertisements to and we use the information we have collected to serve those advertisements.

This policy contains eight sections, and you can jump to each by selecting the links below:

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Share Information
6. How You Can View, Change, or Remove Information
7. How We Protect Information
8. Other Terms

1. Introduction

Questions: If you have any questions or concerns about our privacy policy, contact our privacy team through the help page. You may also contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304.

TRUSTe Program: Facebook is a certified licensee of the TRUSTe Privacy Seal Program. This means that our privacy policy and practices have been reviewed by TRUSTe, an independent organization.
Facebook, Inc.

Complaint

Safe Harbor. Facebook also adheres to the Safe Harbor framework developed by the U.S. Department of Commerce and the European Union. As part of our participation in the Safe Harbor, we agree to resolve all disputes you have with us in connection with our policies and practices through TRUSTe. To view our certification, visit the U.S. Department of Commerce’s Safe Harbor Web site.

Scope. This privacy policy covers all of Facebook. It does not, however, apply to entities that Facebook does not own or control, such as Facebook-enhanced applications and websites. By using or accessing Facebook, you agree to our privacy practices outlined here.

No information from children under age 13. If you are under age 13, please do not attempt to register for Facebook, or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us through this help page.

Parental participation. We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices. Materials to help parents talk to their children about safe internet use can be found on this help page.

2. Information We Receive

Information you provide to us:

Personal information. When you sign up for Facebook you provide us with your name, email, gender, and birth date. During the registration process we give you the opportunity to provide additional profile information, such as where you went to school and where you work, and to add a picture of yourself, to help your friends connect with you. In some cases we may ask for additional information for security reasons or to provide specific services to you. Once you register you can visit your profile at any time to add or remove personal information about yourself. You can add basic information about yourself, such
as information about your hometown, family, relationships, and your political and religious views. You can also add other information about yourself including your activities, interests, contact information, as well as more information about your education and job history.

**Content.** One of the primary reasons people use Facebook is to share content with others. Examples include when you update your status, upload or take a photo, upload or record a video, share a link, create an event or a group, make a comment, write something on someone else's Wall, write a note, or send someone a message. If you do not want us to store metadata associated with content you share on Facebook (such as photos), please remove the metadata before uploading the content.

**Transactional Information.** We may retain the details of transactions or payments you make on Facebook. However, we will only keep your payment source account number with your consent.

**Friend Information.** We offer contact importer tools to help you upload your friends' information so that you can find your friends on Facebook, and invite your contacts who do not have Facebook accounts to join. If you do not want us to store this information, visit this help page. If you give us your password to retrieve those contacts, we will not store your password after you have uploaded your contact information.

**Location Information.** When you share your location with others or add a location to something you post, we treat that like any other content you post (for example, it is subject to your privacy settings). If we offer a service that supports this type of location sharing, we will present you with an option about whether you want to participate.

**Information we collect when you interact with Facebook:**

**Site activity information.** We keep track of the actions you take on Facebook, such as adding a friend, becoming a fan of a Facebook Page, joining a group or an event, creating a photo album, sending a gift, poking another user, indicating you like/shared a post, attending an event, or authorizing an application. In some cases, you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content you uploaded, we might log the fact you shared it.

**Access Device and Browser Information.** When you access Facebook from a computer, mobile phone, or other device, we may collect information from that device about your browser type, location, and IP address, as well as the pages you visit.

**Cookie Information.** We use "cookies" (small pieces of data we store for an extended period of time on your computer, mobile phone, or other device) to make Facebook easier to use, to make our advertising better, and to protect both you and Facebook. For example, we use them to store your login ID (but never your password) to make it easier for you to login whenever you come back to Facebook. We also use them to confirm that you are logged into Facebook, and to know when you are interacting with Facebook Platform applications and websites, our widgets and Share buttons, and our advertisers. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use Facebook.

**Information we receive from third parties:**

**Facebook Platform and Facebook Connect.** We do not own or operate the applications that you use
through Facebook Platform (such as games and apps), or the websites that you interact with through Facebook Connect. We refer to them as Facebook-enhanced applications and websites because they use our Platform to provide you with social features. Whenever you authorize a Facebook-enhanced application or website, we will receive information about actions you take. In some cases, in order to personalize the process of connecting, we may receive a limited amount of information even before you authorize the application or website.

Information from other websites. We may instituted programs with advertising partners and other websites in which they share information with us:

- We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who did not see the ads acted on their site). This data sharing, commonly known as ‘conversion tracking,’ helps us measure our advertising effectiveness and improve the quality of the advertisements you see.

- We may receive information about whether or not you’ve seen or interacted with certain ads on other sites in order to achieve the effectiveness of those ads.

In all of these cases, we receive data that we do not already have, we will de-identify it within 180 days, meaning we will stop associating the information with any particular user. If we institute these programs, we will only use the information in the ways we explain in the “How We Use Your Information” section below.

Information from other users. We may collect information about you from other Facebook users, such as when a friend tags you in a photo or video, provides friend details, or indicates a relationship with you. You can limit who can see that you have been tagged in a photo or video which we refer to as your own photos or videos of you in your privacy settings.

3. Information You Share With Third Parties

We take steps to ensure that others use information that you share on Facebook in a manner consistent with your privacy settings, but we cannot guarantee that they will follow our rules. Read the following section to learn more about how you can protect yourself when you share information with third parties.

Sharing information on Facebook. We designed our privacy settings to enable you to control how you share your information on Facebook. You should review the default privacy settings to make sure they reflect your preferences. Here are some specific things to remember:

- You can control the visibility of most of the information you share on Facebook through your privacy settings.

- Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, and some of your interests are considered publicly available, and therefore do not have privacy settings. (We will soon stop using regional networks, but your geographic region will still be considered publicly available). You can limit the ability of others to find this information on third party search engines through your search privacy settings.

- Some of the content you share on Facebook may show up on your friends’ Facebook homepages and other pages they visit.
- Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users.

- You understand that information might be re-shared or copied by other users.

- Certain types of communications that you send to other users cannot be removed, such as messages.

- When you post information on another user’s profile or comment on another user’s post, that information will be subject to the other user’s privacy settings.

- If you use an external source to publish information to Facebook (such as a mobile application or a Content site), you should check the privacy setting for that post, as it is set by that external source.

*Everyone*: Privacy Setting. Information set to *Everyone* is publicly available information. It may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third-party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the Internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of information you post on Facebook is set to *Only Your Friends*. You can review and change the default settings in your privacy settings. If you enter *Everyone* content that you posted on Facebook, we will remove it from your Facebook profile, but we have no control over its use outside of Facebook.

**Facebook Platform.** As mentioned above, we do not own or operate Facebook-enhanced applications or websites. That means that when you visit Facebook-enhanced applications and websites you are making your Facebook information available to someone other than Facebook. To help those applications and sites operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them. You can learn more about which information the operators of those applications and websites can access on our About Platform page. Prior to allowing them to access any information about you, we require them to agree to terms that limit their use of your information (which you can read about in Section 9 of our Statement of Rights and Responsibilities) and we use technical measures to ensure that they only obtain authorized information. We also give you tools to control how your information is shared with them.

- You can choose to opt-out of Facebook Platform and Facebook Connect altogether through your privacy settings.

- You can block specific applications from accessing your information by visiting your application settings or the application’s Opt-Out page.

- You can use your privacy settings to limit which of your information is available to *Everyone* (by default, every application and website, including those you have not connected with, can access *Everyone* and other publicly available content).

- You can use your application settings to limit which of your information your friends can make available to applications and websites.
Complaint

- We may make information about the location of your computer or access device and your age available to Facebook 65+ enhanced applications and websites in order to help them implement appropriate security measures and control the distribution of age-appropriate content.

You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules. If you find an application or website that violates our rules, you should report the violation to us on this help page and we will take action as necessary.

Exporting Information. You (and those you make your information available to) may use tools like RSS feeds, mobile phone address books, or copy and paste functions, to capture and export information from Facebook, including your information and information about you.

Advertisements. Sometimes the advertisers who present ads on Facebook use technological methods to measure the effectiveness of their ads and to personalize advertising content. You may opt-out of the placement of cookies by many of these advertisers here. You may also use your browser's cookie settings to limit or prevent the placement of cookies by advertising networks.

Links. When you click on links on Facebook you may leave our site. We are not responsible for the privacy practices of other sites, and we encourage you to read their privacy statements.

4. How We Use Your Information

We use the information we collect to provide a safe, efficient, and customized experience. Here are some of the details on how we do that:

To manage the service. We use the information we collect to provide our services and features to you, to measure and improve those services and features, and to provide you with customer support. We use the information to prevent potentially illegal activities, and to enforce our Statement of Rights and Responsibilities. For example, we ask for your date of birth to verify that you are over age 13 and so that we can better limit your access to content and advertising that is not age-appropriate. We also use a variety of technological systems to detect and address anomalous activity and screen content to prevent abuse, such as spam. These efforts may on occasion result in a temporary or permanent suspension or termination of some functions for some users.

To contact you. We may contact you with service-related announcements from time to time. You may opt out of all communications except essential updates on your account notification page. We may include content you see on Facebook in the emails we send to you.

To serve personalized advertising to you. We don't share your information with advertisers without your consent. (An example of consent would be if you asked us to provide your shipping address to an advertiser to receive a free sample.) We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable information we have collected (including information you may have decided not to show to others, 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. You can see the criteria advertisers may select by visiting our advertising page. 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.

To serve social ads. We occasionally pair advertisements we serve with relevant information we have about you and your friends to make advertisements more interesting and more tailored to you and your friends. For example, if you become a fan of a Page, we may display your name and profile photo next to an advertisement for that Page that is displayed to your friends. We only share the personally identifiable information visible in the social ad with the friend who can see the ad. You can opt out of having your information used in social ads on this help page.

To supplement your profile. We may use information about you that we collect from other Facebook users to supplement your profile (such as when you are tagged in a photo or mentioned in a status update). In such cases, we generally allow you to direct how that information is shared in your privacy settings or give you the ability to remove the content (such as allowing you to remove a photo tag of you) or limit its visibility on Facebook.

To make Suggestions. We use your profile information, the addresses you import through our contact importers, and other relevant information, to help you connect with your friends, including making suggestions to you and other users that you connect with on Facebook. If you want to limit your visibility in suggestions we make to other people, you can adjust your search visibility privacy setting, as you will only be visible in our suggestions to the extent you choose to be visible in public search listings. You may also block specific individual users from being suggested to you and from being suggested to them.

Downloadable software. Certain downloadable software applications and apps that we offer, such as our browser toolbars and phone uploaders, transmit data to us. We may not make a formal disclosure if we believe our collection of and use of the information is the obvious purpose of the application, such as the fact that we receive photos when you use our photo uploader. If we believe it is not obvious that we are collecting or using such information, we will make a disclosure to you the first time you provide the information to us so that you can decide whether you want to use that feature.

Memorializing accounts. If we are notified that a user is deceased, we may memorialize the user’s account. In such cases, we restrict profile access to only friends, and allow friends and family to write on the user’s Wall in remembrance. We may close an account if we receive a formal request from the user’s next of kin or other proper legal request to do so.

5. How We Share Information

Facebook is about sharing information with other friends and people in your networks while providing you with privacy settings that you can use to restrict other users from accessing your information. We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so. For example:

When you make a payment. When you enter into transactions with others or make payment on Facebook, we will only share transaction information with those third parties necessary to complete the transaction and will require those third parties to agree to respect the privacy of your information.

When you invite a friend to join. When you ask us to invite a friend to join Facebook, we will send your friend a message on your behalf using your name. We may also send up to two reminders to them.
Complaint

In your name. If your friend does not want us to keep their information, we will remove it at their request on this help page.

When you choose to share your information with marketers. You may choose to share information with marketers or other commerce providers that are not associated with Facebook through on-site offers. This is entirely at your discretion and we will not provide your information to these marketers without your consent.

To help your friends find you. By default, we make certain information you have posted to your profile available in search results on Facebook to help your friends find you. However, you can control who has access to this information, as well as who can find you in searches, through your privacy settings. We also partner with email and instant messaging providers to help their users identify which of their contacts are Facebook users, so that we can promote Facebook to those users.

To give search engines access to publicly available information. We generally limit search engine access to our site. We may allow them to access information set to the "Readers" or "Hidden" setting and your public search listing (but you can turn off your public search listing in your privacy settings).

To help improve or promote our service. Sometimes we share aggregated information with third parties to help improve or promote our service. But we only do so in such a way that no individual user can be identified or linked to any specific action or information.

To provide you with services. We may provide information to service providers that help us bring you the services we offer. For example, we may use third parties to help host our website, send our email updates about Facebook, remove repetitive information from our users' lists, process payments, or provide search results or links (including sponsored links). These service providers may have access to your personal information for use for a limited time, but when this occurs we implement reasonable contractual and technical provisions to limit their use of that information to helping us provide the service.

To advertise our services. We may ask advertisers outside of Facebook to display ads promoting our services. We may ask them to deliver these ads based on the presence of a cookie, but in doing so will not share any other information with the advertiser.

To offer joint services. We may provide services jointly with other companies, such as the classifieds service in the Facebook Marketplace. If you use these services, we may share your information so facilitate that service. However, we will identify the partner and present the joint service provider's privacy policy to you before you use that service.

To respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good-faith belief that the response is required by law. We may also disclose information if we have a good-faith belief that it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.
Facebook Beacon. [We have announced a settlement of a lawsuit related to the Beacon product: the Beacon product will be discontinued and this language removed from the privacy policy upon approval of a settlement by the court.] Facebook Beacon is a feature of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collected certain information from those sites and presented it to you after you had completed an action on that site. You have the choice to have us discard that information, or to share it with your friends. To learn more about the operation of the service, we encourage you to read the material here. To opt out of the service altogether, click here. Like many other websites that interact with third party sites, we may receive some information even if you are logged out from Facebook, or that pertains to non-Facebook users, from those sites in conjunction with the technical operation of the system. In cases where we receive information from Beacon sites on users that are not logged in, or on non-Facebook users, we do not attempt to associate it with individual Facebook accounts and will discard it.

Transfer in the Event of Sale or Change of Control. If the ownership of all or substantially all of our business changes, we may transfer your information to the new owner so that the service can continue to operate. In such a case, your information would remain subject to the premises made in any pre-existing Privacy Policy.

6. How You Can View, Change, or Remove Information

Viewing and editing your profile. You may change or delete your profile information at any time by going to your profile page and clicking “Edit My Profile.” Information will be updated immediately. While you cannot delete your line of birth, you can use the setting on the info tab of your profile information page to hide all or part of it from other users.

Delete uploaded contacts. If you use our contact importer to upload addresses, you can later delete the list on this help page.

Deactivating or deleting your account. If you want us 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. We save your profile information (friends, photos, interests, etc.) in case you later decide to reactivate your account. Many users deactivate their accounts for temporary reasons and in doing so are asking us to maintain their information until they return to Facebook. You will still have the ability to reactivate your account and restore your profile in its entirety. When you delete an account, it is permanently deleted. You should only delete your account if you are certain you never wish to reactivate it. You may deactivate your account on your account settings page or delete your account on this help page.

Limitations on removal. Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users. However, your name will no longer be associated with that information on Facebook. For example, if you post something to another user’s profile, and then you delete your account, that post may remain, but be attributed to an [Anonymous Facebook User]. Additionally, we may retain certain information to prevent identity theft and other misconduct even if deletion has been requested.

Backup copies. Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others.
Non-user contact information. If a user provides your email address to us but you are not a Facebook user but you want us to delete your address, you can do so on this help page. However, that request will only apply to addresses we have at the time of the request and not to any addresses that users provide to us later.

7. How We Protect Information

We do our best to keep your information secure, and we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page.

Steps we take to keep your information secure. We keep your account information on a secured server behind a firewall. When you enter sensitive information (such as credit card numbers and passwords), we encrypt that information using secure socket layer technology (SSL). We also use automated and social measures to enhance security, such as analyzing account behavior for fraudulent or otherwise anomalous behavior, may limit use of site features in response to possible signs of abuse, may remove inappropriate content or links to illegal content, and may suspend or disable accounts for violations of our Statement of Rights and Responsibilities.

Risks inherent in sharing information. Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using stronger, more secure security practices such as choosing a strong password, using different passwords for different services, and using up to date anti-virus software.

Report Violations. You should report any security violations to us on this help page.

8. Other Terms

Changes. We may change this Privacy Policy pursuant to the procedures outlined in the Facebook Statement of Rights and Responsibilities. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account. If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. You can make sure that you receive notices directly by becoming a fan of the Facebook Site Governance Page.

Consent to Collection and Processing in the United States. By using Facebook, you consent to having your personal data transferred to and processed in the United States.

Defined Terms. "Us," "we," "our," "Platform" and "Facebook" mean the same as they do in the Statement of Rights and Responsibilities. All "Information" and "Data" are used more generally and interchangeably here than in the Statement of Rights and Responsibilities unless otherwise limited by the context.

Helpful links

Statement of Rights and Responsibilities
Facebook Site Governance Page
application settings
privacy settings
account notifications page
help page for complaints about our privacy policies or practices
help page to report use by a child under age 13
help page with info to help parents talk to children about safe Internet use
deleting an account
reporting a deceased user
reporting an impostor
reporting abusive content
reporting a compromised account
requesting deletion of data for non-user
removing Friend Finder contacts
reporting and blocking third-party applications
general explanation of third-party applications and how they access data
Complaint

Exhibit I
Complaint

4.7. You will keep your contact information up-to-date and accurate.
4.8. You will not share your password, let anyone else access your account, or do anything else that might jeopardize
    the security of your account.
4.9. You will not transfer your account to someone else or use any name that might confuse
    the identity of your account.

5. Respecting Other People’s Rights

5.1. You will not post content to take action on Facebook that infringes on someone else’s rights or otherwise
    violates the law.
5.2. We don’t remove any content you post on Facebook if we believe that it violates the law.
5.3. We will provide you with tools to help you protect your intellectual property rights. To learn more, visit our 
5.4. If we receive notice from someone that their content is copyright and you believe we removed it by mistake, 
    we will give you an opportunity to appeal.
5.5. If you repeatedly post content that infringes upon intellectual property rights, we will disable your account when
    appropriate.
5.6. We will use your content under the terms of our license agreement.
5.7. If you receive any notice from us, you will obey our request, make sure you (and not Facebook) are the
    one collecting their information, and post a privacy policy explaining what information you collect and how you
    will use it.
5.8. You will not post any personal information or account or service financial information on Facebook.

6. Website

6.1. We constantly provide our website services for free, but you must be aware that your server’s normal fees and taxes,
    such as server or messaging fees, will still apply.
6.2. If the user of the Facebook application chooses to have a Facebook application, you will receive a custom information
    on Facebook where you can choose whether your messages are sent to the person who asked you to add a number.

7. Payments

If you purchase the Facebook Credits, or make direct payments, you agree to the Payment Terms.

8. Special Permissions: Application to Share Links

If you use the Facebook button on your website, the following additional rights apply to it.

8.1. If you give us permission to use Facebook’s Share Button on your website, you agree to host a website on
    Facebook.
8.2. You agree to prevent our users from using links that contain contact information.
8.3. You will not use a Share button on any page containing contact information unless it is labeled as “Share” or
    “Share on Facebook.”

9. Special Permissions: Application to Developers/Operators of Applications or Websites

If you are a developer or operator of a website that is a Facebook application or internet site 
applicable to internet protocol, the following restrictions apply to you.

9.1. You are responsible for your application and its content and all uses you make of Facebook. This includes 
    ensuring that your application or use of Facebook or Facebook’s Guidelines
    7.3. You will not use the Facebook service for personal applications, and will only use it in connection with 
    Facebook.
Complaint

2.2. You will make it clear to users when you use their data you are going to use and how you will use it, display or share that data.
2.3. You will not use, display, or share a user’s data in a manner inconsistent with the user’s privacy settings or your users’ consent.
2.4. You will deliver all data you receive from us to one or more of our customers or providers listed in our Platform Policies.
2.5. You will ensure that all users have received notice of your privacy terms and conditions in a manner that is consistent with the data we have received from us.
2.6. We may request that you provide us with a copy of any data you have received from us.
2.7. We may ask you to update any data you have received from us.
2.8. We may ask you to stop storing any data you have received from us.

3.1. You will not transfer the data you receive from us without our prior consent.
3.2. You will not give or otherwise make available to any third party any data you have received from us.
3.3. You will not modify or otherwise affect the data we have received from us.
3.4. You will not use the data we have received from us to create any derivative works.
3.5. You will not use the data we have received from us for any purpose other than the purpose for which we provided it.
3.6. You will not use the data we have received from us in any manner that violates our Platform Policies.

4.1. You will not use the data we have received from us to create any derivative works.
4.2. You will not use the data we have received from us to create any derivative works.
4.3. You will not use the data we have received from us to create any derivative works.
4.4. You will not use the data we have received from us to create any derivative works.
4.5. You will not use the data we have received from us to create any derivative works.
4.6. You will not use the data we have received from us to create any derivative works.
4.7. You will not use the data we have received from us to create any derivative works.
4.8. You will not use the data we have received from us to create any derivative works.
4.9. You will not use the data we have received from us to create any derivative works.
4.10. You will not use the data we have received from us to create any derivative works.

5.1. You will not use the data we have received from us to create any derivative works.
5.2. You will not use the data we have received from us to create any derivative works.
5.3. You will not use the data we have received from us to create any derivative works.
5.4. You will not use the data we have received from us to create any derivative works.
5.5. You will not use the data we have received from us to create any derivative works.
5.6. You will not use the data we have received from us to create any derivative works.
5.7. You will not use the data we have received from us to create any derivative works.
5.8. You will not use the data we have received from us to create any derivative works.
5.9. You will not use the data we have received from us to create any derivative works.
5.10. You will not use the data we have received from us to create any derivative works.

6.1. You will not use the data we have received from us to create any derivative works.
6.2. You will not use the data we have received from us to create any derivative works.
6.3. You will not use the data we have received from us to create any derivative works.
6.4. You will not use the data we have received from us to create any derivative works.
6.5. You will not use the data we have received from us to create any derivative works.
6.6. You will not use the data we have received from us to create any derivative works.
6.7. You will not use the data we have received from us to create any derivative works.
6.8. You will not use the data we have received from us to create any derivative works.
6.9. You will not use the data we have received from us to create any derivative works.
6.10. You will not use the data we have received from us to create any derivative works.

7.1. You will not use the data we have received from us to create any derivative works.
7.2. You will not use the data we have received from us to create any derivative works.
7.3. You will not use the data we have received from us to create any derivative works.
7.4. You will not use the data we have received from us to create any derivative works.
7.5. You will not use the data we have received from us to create any derivative works.
7.6. You will not use the data we have received from us to create any derivative works.
7.7. You will not use the data we have received from us to create any derivative works.
7.8. You will not use the data we have received from us to create any derivative works.
7.9. You will not use the data we have received from us to create any derivative works.
7.10. You will not use the data we have received from us to create any derivative works.

8.1. You will not use the data we have received from us to create any derivative works.
8.2. You will not use the data we have received from us to create any derivative works.
8.3. You will not use the data we have received from us to create any derivative works.
8.4. You will not use the data we have received from us to create any derivative works.
8.5. You will not use the data we have received from us to create any derivative works.
8.6. You will not use the data we have received from us to create any derivative works.
8.7. You will not use the data we have received from us to create any derivative works.
8.8. You will not use the data we have received from us to create any derivative works.
8.9. You will not use the data we have received from us to create any derivative works.
8.10. You will not use the data we have received from us to create any derivative works.

9.1. You will not use the data we have received from us to create any derivative works.
9.2. You will not use the data we have received from us to create any derivative works.
9.3. You will not use the data we have received from us to create any derivative works.
9.4. You will not use the data we have received from us to create any derivative works.
9.5. You will not use the data we have received from us to create any derivative works.
9.6. You will not use the data we have received from us to create any derivative works.
9.7. You will not use the data we have received from us to create any derivative works.
9.8. You will not use the data we have received from us to create any derivative works.
9.9. You will not use the data we have received from us to create any derivative works.
9.10. You will not use the data we have received from us to create any derivative works.

10.1. [AdHERE] Advertising Agreements
10.2. [AdHERE] Advertising Agreements
10.3. [AdHERE] Advertising Agreements
10.4. [AdHERE] Advertising Agreements
10.5. [AdHERE] Advertising Agreements
10.6. [AdHERE] Advertising Agreements
10.7. [AdHERE] Advertising Agreements
10.8. [AdHERE] Advertising Agreements
10.9. [AdHERE] Advertising Agreements
10.10. [AdHERE] Advertising Agreements
Complaint
Complaint

11. Definitions

11.1 "Facebook" means the features and services we make available, including through (a) our websites at www.facebook.com and any other Facebook-branded or -endorsed websites including subdomains, (b) our Facebook, and (c) other mobile, desktop or network applications, existing or later developed.

11.2 By "we", "our" and "us" we mean Facebook, Inc. and its affiliates.

11.3 "Facebook" means a set of APIs and services that enable applications, developers, operators or service providers to retrieve data from Facebook and provide data to us regarding to Facebook users.

11.4 "Subscription" means the current information you post on Facebook, including information about you and the world you see.

11.5 "You" means the person who has posted data on Facebook or otherwise is making any data to us.

11.6 "Data" means any text, copy, photos, performances or displays, distribute and copy, transmute, and create derivative works of it.

11.7 "other"

11.7.1 This Statement makes up the online agreement between you and Facebook, and supersedes any prior agreements.

11.7.2 You agree that any update of this Statement is effective as soon as it is published, and the revision takes effect in full force and effect.

11.7.3 We will not sell or distribute any of this Statement, which you must be under your control and signed by us.

11.7.4 You acknowledge that you have read and understand the terms and conditions under which Facebook and provide data to us.

11.7.5 We will not sell, rent, lease or license information about you to anyone who does not do so.

11.7.6 You acknowledge that you have read and understand the terms and conditions under which Facebook and provide data to us.

11.7.7 Nothing in these agreements shall preclude us from exercising the law.

11.7.8 You agree that we may enter into separate agreements that you choose to make available on Facebook as long as the agreement is consistent with your intellectual property rights under this Statement and you have permission of your owner to make that content available to the public in the way you choose.

11.7.9 This Statement does not affect any third party trademark rights.
Complaint

Exhibit J
Complaint
Exhibit K

The Role of Advertising on Facebook

By David Southorn (on Facebook, Thursday, July 4, 2011, 9:15am)

In recent years, Facebook users have been increasingly exposed to targeted advertising. It is likely that if you are a Facebook user, you have been exposed to targeted advertising. It is likely that if you are a Facebook user, you have been exposed to targeted advertising.

Facebook Help Center

Exhibit K


2/4/2011
Facebook has used its dominant market position to harm small businesses, innovation, and users across the United States by requiring that all Facebook applications ("Apps") comply with Facebook’s "developers agreement," which Facebook uses to impose on App developers restrictive and anticompetitive terms and conditions. Many small businesses and developers have been unable to continue providing their services and products to Facebook users, and the App developers who have been able to continue providing them have been at a competitive disadvantage. Facebook’s conduct has been illegal and anticompetitive under sections 2 and 1 of the Clayton Act, 15 U.S.C. §§ 15, 12.

This Conduct

Facebook has used its dominant market position to harm small businesses, innovation, and users across the United States by requiring that all Facebook applications ("Apps") comply with Facebook’s "developers agreement," which Facebook uses to impose on App developers restrictive and anticompetitive terms and conditions. Many small businesses and developers have been unable to continue providing their services and products to Facebook users, and the App developers who have been able to continue providing them have been at a competitive disadvantage. Facebook’s conduct has been illegal and anticompetitive under sections 2 and 1 of the Clayton Act, 15 U.S.C. §§ 15, 12.
Complaint
Complaint

Exhibit M

* What are Verified applications?
Verified applications have passed a rigorous 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.

Because these applications have passed a review by Facebook, they are
prioritized higher in the application directory and are highlighted by a green
checkmark. A "Verified Apps" badge will appear on their Profile page as well.

* 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's 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.
Complaint

Exhibit N
Complaint

Exhibit P
Complaint

Exhibit Q

[Image of Facebook's Privacy Policy]

We urge you to review this page before you use Facebook. You should read the entire page before using Facebook, and you should not use Facebook if you disagree with its terms.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]

If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. How We Use Your Information
5. How We Use Your Information
6. How You Can View, Change, or Remove Information
7. How Your Personal Information Is Used
8. Other Terms

Questions? If you have any questions or concerns about our privacy policy, contact us at privacy@facebook.com. You can also contact us at 732-101 S California Ave, Los Altos, CA 94024.

If you have any complaints about our policy or if you think a page is in use, please contact us through the help page. If you are not satisfied with our response, you can contact TRUSTe.

[Image of TRUSTe seal]
Complaint
Complaint

To Facebook, Inc.

We are filing this complaint because Facebook, Inc. ("Facebook") has repeatedly violated the California Consumer Privacy Act ("CCPA") by collecting and utilizing personal information about our members without proper notice and consent. As a result, we believe Facebook has also violated the California Constitution and the California Business and Professions Code. Facebook has failed to comply with the requirements of the CCPA and has caused us substantial harm.

Facebook collects, utilizes, and sells the personal information of its members, including sensitive personal information such as names, addresses, phone numbers, email addresses, and financial information. This information is collected through various means, including but not limited to, Facebook’s advertising, marketing, and data mining activities.

Despite the fact that Facebook has a ripe and technologically feasible mechanism to gather and utilize the personal information of its users, it has failed to provide adequate notice and obtain the necessary consent from its members.

We believe Facebook should be held accountable for its failure to comply with the CCPA and the California Constitution. Therefore, we request the following relief:

1. A permanent injunction prohibiting Facebook from collecting, utilizing, and selling the personal information of its members without proper notice and consent.
2. Compensatory damages for the harm caused by Facebook’s violation of the CCPA.
3. A civil penalty of $100 for each violation of the CCPA.

We believe that Facebook’s violation of the CCPA has caused substantial harm to us and our members. We request that Facebook be held accountable for its actions.

Respectfully submitted,

[Your Name]
[Your Contact Information]

[Date]

facebook.com/terms/compliance
FACEBOOK, INC. 73

Complaint

Exhibit R

Introduction

Facebook, Inc. (“Facebook”) is a social networking platform that serves as a means for users to communicate with each other. Facebook has established a network of servers to facilitate this communication and has developed a set of terms of service (“TOS”) that govern the use of the platform. The TOS is designed to protect the rights of Facebook and its users, and to ensure a safe and secure environment for all users.

1. Information

2. Information the FCA has

3. Information the FCA does not have

4. The FCA has other information

5. The FCA does not have other information

6. The FCA has no other information

7. The FCA does not have any other information

8. The FCA does not have any other information

9. The FCA does not have any other information

10. The FCA does not have any other information

11. The FCA does not have any other information

12. The FCA does not have any other information

13. The FCA does not have any other information

14. The FCA does not have any other information

15. The FCA does not have any other information

16. The FCA does not have any other information

17. The FCA does not have any other information

18. The FCA does not have any other information

19. The FCA does not have any other information

20. The FCA does not have any other information

21. The FCA does not have any other information

22. The FCA does not have any other information

23. The FCA does not have any other information

24. The FCA does not have any other information

25. The FCA does not have any other information

26. The FCA does not have any other information

27. The FCA does not have any other information

28. The FCA does not have any other information

29. The FCA does not have any other information

30. The FCA does not have any other information

31. The FCA does not have any other information

32. The FCA does not have any other information

33. The FCA does not have any other information

34. The FCA does not have any other information

35. The FCA does not have any other information

36. The FCA does not have any other information

37. The FCA does not have any other information

38. The FCA does not have any other information

39. The FCA does not have any other information

40. The FCA does not have any other information

41. The FCA does not have any other information

42. The FCA does not have any other information

43. The FCA does not have any other information

44. The FCA does not have any other information

45. The FCA does not have any other information

46. The FCA does not have any other information

47. The FCA does not have any other information

48. The FCA does not have any other information

49. The FCA does not have any other information

50. The FCA does not have any other information

51. The FCA does not have any other information

52. The FCA does not have any other information

53. The FCA does not have any other information

54. The FCA does not have any other information

55. The FCA does not have any other information

56. The FCA does not have any other information

57. The FCA does not have any other information

58. The FCA does not have any other information

59. The FCA does not have any other information

60. The FCA does not have any other information

61. The FCA does not have any other information

62. The FCA does not have any other information

63. The FCA does not have any other information

64. The FCA does not have any other information

65. The FCA does not have any other information

66. The FCA does not have any other information

67. The FCA does not have any other information

68. The FCA does not have any other information

69. The FCA does not have any other information

70. The FCA does not have any other information

71. The FCA does not have any other information

72. The FCA does not have any other information

73. The FCA does not have any other information

74. The FCA does not have any other information

75. The FCA does not have any other information

76. The FCA does not have any other information

77. The FCA does not have any other information

78. The FCA does not have any other information

79. The FCA does not have any other information

80. The FCA does not have any other information

81. The FCA does not have any other information

82. The FCA does not have any other information

83. The FCA does not have any other information

84. The FCA does not have any other information

85. The FCA does not have any other information

86. The FCA does not have any other information

87. The FCA does not have any other information

88. The FCA does not have any other information

89. The FCA does not have any other information

90. The FCA does not have any other information

91. The FCA does not have any other information

92. The FCA does not have any other information

93. The FCA does not have any other information

94. The FCA does not have any other information

95. The FCA does not have any other information

96. The FCA does not have any other information

97. The FCA does not have any other information

98. The FCA does not have any other information

99. The FCA does not have any other information

100. The FCA does not have any other information
Complaint

FACEBOOK, INC.

1. How the Use Your Information

No one is informed about it except in its own use. It is not shared or sold in any condition for any condition for any condition.

2. What We Do When We Use Your Information

We have used your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

3. The People Who Have Access to Your Information

We have access to your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

4. How to Share Your Information

Your information will not be shared or sold unless it has been shared or sold by you. It will be used only with your approval. You can withdraw your approval at any time.

5. How to Use Your Information

We will use your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

6. How to Optimize Your Information

We will optimize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

7. How to Personalize Your Information

We will personalize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

8. How to Improve Your Information

We will improve your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

9. How to Optimize Your Information

We will optimize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

10. How to Personalize Your Information

We will personalize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

11. How to Improve Your Information

We will improve your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

12. How to Optimize Your Information

We will optimize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

13. How to Personalize Your Information

We will personalize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

14. How to Improve Your Information

We will improve your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

15. How to Optimize Your Information

We will optimize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

16. How to Personalize Your Information

We will personalize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

17. How to Improve Your Information

We will improve your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

18. How to Optimize Your Information

We will optimize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

19. How to Personalize Your Information

We will personalize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

20. How to Improve Your Information

We will improve your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

21. How to Optimize Your Information

We will optimize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

22. How to Personalize Your Information

We will personalize your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.

23. How to Improve Your Information

We will improve your Information for the following purposes: to analyze, to advertise, to market, to research, to develop, to improve, to optimize, and to personalize.
Complaint

goes都不能说漆面的条件是因由再生的，予以多夜推进，要求对蒂戈艾尔或蒂戈会定的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序的程序
Complaint

Exhibit S

Facebook:

http://www.facebook.com/policy.php

8/31/2011
Facebook:

78 FEDERAL TRADE COMMISSION DECISIONS
VOLUME 154

Complaint

http://www.facebook.com/policy.php
8/31/2011
We give you this notice even though we are not required to do so by law. We have implemented this notice to help you understand the purposes for which we use information about you when you use our services, and to enhance your experience with Facebook. As you use Facebook, we receive and/or collect information about you, and we use that information in a variety of ways, including to personalize the Facebook experience for you, to help you find other people you may know, to help you communicate with them, and to improve Facebook. We also use this information to provide you updates and other communications, to send you ads or other marketing communications, and to otherwise improve your use of the Facebook services. We also use this information to develop new products and services, to improve existing products and services, to conduct research and analysis, and to otherwise improve our business. We may also use this information to provide you with personalized suggestions, to improve our advertising and other marketing communications, and to otherwise improve your use of the Facebook services. We also use this information to provide you with personalized suggestions, to improve our advertising and other marketing communications, and to otherwise improve your use of the Facebook services.

We use personal identifiers, such as your name, email address, phone number, and Facebook login information, to identify you and to provide you with personalized experiences, including ads and other content, and to facilitate your use of Facebook. We also use personal identifiers to verify your identity and to ensure that you are the person you claim to be. We may also use your personal identifiers to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use personal identifiers to provide you with personalized content, including ads, and to facilitate your use of Facebook. We also use personal identifiers to verify your identity and to ensure that you are the person you claim to be. We may also use your personal identifiers to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We use anonymous identifiers, such as your IP address and other information, to enable us to provide you with a more personalized experience, including ads and other content, and to facilitate your use of Facebook. We also use anonymous identifiers to verify your identity and to ensure that you are the person you claim to be. We may also use your anonymous identifiers to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We use cookies and other technologies to improve your use of Facebook and to deliver ads and other content more relevant to you. We may also use cookies and other technologies to verify your identity and to ensure that you are the person you claim to be. We may also use your cookies and other technologies to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use cookies and other technologies to provide you with a more personalized experience, including ads and other content, and to facilitate your use of Facebook. We also use cookies and other technologies to verify your identity and to ensure that you are the person you claim to be. We may also use your cookies and other technologies to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use cookies and other technologies to provide you with a more personalized experience, including ads and other content, and to facilitate your use of Facebook. We also use cookies and other technologies to verify your identity and to ensure that you are the person you claim to be. We may also use your cookies and other technologies to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use cookies and other technologies to provide you with a more personalized experience, including ads and other content, and to facilitate your use of Facebook. We also use cookies and other technologies to verify your identity and to ensure that you are the person you claim to be. We may also use your cookies and other technologies to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use cookies and other technologies to provide you with a more personalized experience, including ads and other content, and to facilitate your use of Facebook. We also use cookies and other technologies to verify your identity and to ensure that you are the person you claim to be. We may also use your cookies and other technologies to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We use this information to improve the content and functionality of Facebook, to develop new products and services, to improve our existing products and services, to conduct research and analysis, and to otherwise improve our business. We may also use this information to develop new products and services, to improve our existing products and services, to conduct research and analysis, and to otherwise improve our business.

We also use this information to provide you with personalized content, including ads and other content, and to facilitate your use of Facebook. We also use this information to verify your identity and to ensure that you are the person you claim to be. We may also use your personal information to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use this information to provide you with personalized content, including ads and other content, and to facilitate your use of Facebook. We also use this information to verify your identity and to ensure that you are the person you claim to be. We may also use your personal information to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use this information to provide you with personalized content, including ads and other content, and to facilitate your use of Facebook. We also use this information to verify your identity and to ensure that you are the person you claim to be. We may also use your personal information to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use this information to provide you with personalized content, including ads and other content, and to facilitate your use of Facebook. We also use this information to verify your identity and to ensure that you are the person you claim to be. We may also use your personal information to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.

We may also use this information to provide you with personalized content, including ads and other content, and to facilitate your use of Facebook. We also use this information to verify your identity and to ensure that you are the person you claim to be. We may also use your personal information to protect the security of your Facebook account and to prevent unauthorized access to your Facebook account.
Facebook:  

Page 4 of 5

Parties

Facebook.com and Facebook, Inc. (collectively, "Facebook") and Lulu.com ("Lulu"), are seeking to resolve certain policing issues between Facebook and Lulu.

Facebook is a social networking website that allows users to create a personal profile, add friends, and interact with them via various means such as sending messages, posting updates, and sharing photos and videos. Lulu is a platform for authors to publish and sell their books directly to readers.

The issue between Facebook and Lulu concerns the policy enforcement and moderation of content on Facebook. Lulu claims that Facebook's policies are inconsistent and unfair, resulting in the removal of content that Lulu believes is protected under the First Amendment.

Facebook argues that its policies are necessary to maintain a safe and pleasant environment on its platform. Lulu argues that its content is protected under the First Amendment and that Facebook's removal of its content is a violation of its rights.

The parties are seeking to resolve these issues through mediation, and they have agreed to abide by the mediation process described in the mediation agreement.

Complaint
Complaint
DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq.;

The Respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having carefully considered the comments filed by interested persons, now in further conformity with the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Facebook, Inc. (“Facebook”) is a Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

A. Unless otherwise specified, “Respondent” shall mean Facebook, its successors and assigns. For purposes of Parts I, II, and III of this order, “Respondent” shall also mean Facebook acting directly, or through any corporation, subsidiary, division, website, or other device.

B. “Commerce” shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

C. “Clear(ly) and prominent(ly)” shall mean:

1. in textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

2. in communications disseminated orally or through audible means (e.g., radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;

3. in communications disseminated through video means (e.g., television or streaming video), the required disclosures are in writing in a form
consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and

4. in all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

D. “Covered information” shall mean information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol (“IP”) address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above.

E. “Nonpublic user information” shall mean covered information that is restricted by one or more privacy setting(s).

F. “Privacy setting” shall include any control or setting provided by Respondent that allows a user to restrict which individuals or entities can access or view covered information.

G. “Representatives” shall mean Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

H. “Third party” shall mean any individual or entity that uses or receives covered information obtained by or on
Decision and Order

behalf of Respondent, other than: (1) a service provider of Respondent that (i) uses the covered information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the covered information, or any individually identifiable information derived from such covered information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a user and for no other purpose; or (2) any entity that uses the covered information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Respondent’s terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

I. “User” shall mean an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent’s products and services.

I.

IT IS ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

A. its collection or disclosure of any covered information;

B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;

C. the extent to which Respondent makes or has made covered information accessible to third parties;

D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;
E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user’s account with Respondent or during such time as a user’s account is deactivated or suspended; and

F. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user’s nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user’s privacy setting(s), shall:

A. clearly and prominently disclose to the user, separate and apart from any “privacy policy,” “data use policy,” “statement of rights and responsibilities” page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and

B. obtain the user’s affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user’s nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user’s privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. §45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect
compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III.

**IT IS FURTHER ORDERED** that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent’s control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user’s covered information that has been posted to Respondent’s websites or services by a user other than the user who deleted such information or deleted or terminated such account.

IV.

**IT IS FURTHER ORDERED** that Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in
Decision and Order

Respondent’s unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

E. the evaluation and adjustment of Respondent’s privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent’s operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

V. IT IS FURTHER ORDERED that, in connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of
privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the covered information;

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.
VI.

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;

B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

C. for a period of five (5) years from the date received, any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent’s compliance with this order;

D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent’s attempt to obtain the consent of users referred to in Part II above, along with documents and information sufficient to show each user’s consent; and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Respondent has attempted to
obtain and/or been required to obtain such consent; and

E. for a period of three (3) years after the date of preparation of each Assessment required under Part V of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VII.

IT IS FURTHER ORDERED that Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

VIII.

IT IS FURTHER ORDERED that Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement,
Decision and Order

Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the Matter of Facebook, Inc., FTC File No.[   ]. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IX.

IT IS FURTHER ORDERED that Respondent, within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, Respondent shall submit additional true and accurate written reports.

X.

This order will terminate on July 27, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part of this order that terminates in fewer than twenty (20) years; and

B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that this order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.
STATEMENT OF THE COMMISSION

The final consent order in In re Facebook, Inc. that we approve today advances the privacy interests of the nearly one billion Facebook users around the world by requiring the company to live up to its promises and submit to privacy audits. Notably, Facebook will be subject to civil penalties of up to $16,000 for each violation of the order. We intend to monitor closely Facebook’s compliance with the order and will not hesitate to seek civil penalties for any violations.

We write to address the arguments raised by our colleague, Commissioner Rosch, who opposes final approval of the order. One of his objections relates to the extent to which the order would reach the activities of third-party “apps” downloaded by consumers while using the Facebook platform. The Order broadly prohibits Facebook from misrepresenting in any manner, expressly or by implication, the extent to which it maintains the privacy or security of any information it collects from or about consumers. For a company whose entire business model rests on collecting, maintaining, and sharing people’s information, this prohibition touches on virtually every aspect of Facebook’s operations. Further, the Order sets forth clear examples of how this broad prohibition would apply in connection with apps, by prohibiting Facebook from misrepresenting (1) the extent to which it makes its users’ information accessible to apps; or (2) the steps it takes to verify the privacy or security protections that apps provide.\footnote{Agreement Containing Consent Order, § I.C-D.} A statement from Facebook about an app’s conduct may well amount to a promise that Facebook is taking steps to assure the level of privacy or security that the app provides for
consumers’ information.2 These provisions make clear that Facebook will be liable for conduct by apps that contradicts Facebook’s promises about the privacy or security practices of these apps.

Commissioner Rosch also opposes the consent order because it includes a denial by Facebook of the substantive allegations in the Commission’s complaint.3 Based on this denial, Commissioner Rosch asserts that the Commission lacks the requisite “reason to believe” that Facebook violated Section 5 of the Federal Trade Commission Act and a basis to conclude that the settlement is in “the interest of the public.”

We strongly disagree with Commissioner Rosch’s view that if the Commission allows a respondent to deny the complaint’s substantive allegations, or use language that is tantamount to a denial, there is no basis for the Commission to conclude that the respondent engaged in unlawful conduct or that the consent is in the public interest. As Commissioner Rosch is aware, an extensive investigation and detailed staff recommendation has given the Commission a strong—not just a reasonable—basis to issue its complaint in this case and to conclude that both the complaint and the resulting settlement are in the public interest. Here, as in all enforcement cases, it is the evidentiary record developed by FTC staff during the course of its investigation, not any ensuing settlement agreement, that forms the basis for action by the Commission. A respondent’s denial of liability in a consent agreement does not diminish staff’s extensive investigation or the ability of the Commission to find a reasonable basis to finalize a settlement or to enforce an order that results from settlement negotiations. Moreover, express denials of

---

2 Indeed, in light of Facebook’s representations to users about apps when offering them the ability to install and use apps, the prohibition covers privacy disclosures by Facebook of the very sort that gave rise to Commissioner Rosch’s concern.

3 The order states that Facebook “expressly denies the allegations set forth in the complaint, except for the jurisdictional facts.” Agreement Containing Consent Order, ¶ 5.

4 Dissenting Statement of Commissioner Rosch at 1 (quoting 15 U.S.C. § 45(b)).
liability are consistent with the Commission’s current Rules of Practice.5

We view the final consent order in this matter to be a major step forward for consumer privacy and hereby approve it.

While we do not believe that a respondent’s denial of liability is reason to reject a settlement that is in the public interest, we share Commissioner Rosch’s desire to avoid any possible public misimpression that the Commission obtains settlements when it lacks reason to believe that the alleged conduct occurred. We commend Commissioner Rosch for focusing our attention on the issue; going forward, express denials will be strongly disfavored. We also appreciate Commissioner Rosch’s suggestion that consent order language that the respondent “neither admits nor denies” a complaint’s allegations may very well be a more effective way to ensure that there are no misimpressions about the Commission’s process. Accordingly, we will consider in the coming months whether a modification to the Commission Rules of Practice is warranted.

---

5 Rule 2.32 of the FTC Rules of Practice, which governs administrative settlements, provides that “[t]he agreement may state that the signing thereof is for settlement purposes only and does not constitute an admission by any party that the law has been violated as alleged in the complaint.” 16 C.F.R. § 2.32.
Dissenting Statement of Commissioner J. Thomas Rosch

I dissent from acceptance of this final consent order for two reasons. First, in the Agreement Containing Consent Order, respondent Facebook “expressly denies the allegations set forth in the complaint, except for the jurisdictional facts.” Our Federal Trade Commission Rules of Practice do not provide for such a denial. Beyond that, as I read Section 5, Commissioners are authorized to accept a consent agreement only if there is reason to believe that a respondent is engaging in an unfair or deceptive act or practice and that acceptance of the consent agreement is in the interest of the public. I respectfully suggest that the whole reason for requiring the Commission to conclude that there is “reason to believe” is to force the Commission to come to grips with the probability that the respondent did engage in conduct creating liability. I would further argue that in the real world, if the Commission allows the respondent to expressly deny that it did engage in that conduct (or to use language that is tantamount to an express denial), there is a questionable basis for us to conclude that that probability exists (or that the consent is in the public interest either.). Accordingly, I cannot find that either the “reason to believe” or the “in the interest of the public” requirement is satisfied when, as here, there is an express denial of the allegations set forth in the complaint.

---

1 Agreement Containing Consent Order, ¶ 5.

2 See Rule 2.32, 16 C.F.R. § 2.32 (“The agreement may state that the signing thereof is for settlement purposes only and does not constitute an admission by any party that the law has been violated as alleged in the complaint.”) (emphasis added).

3 15 U.S.C. § 45(b). See Johnson Prods. Co. v. FTC, 549 F.2d 35, 38 (7th Cir. 1977) (“The Commission, unlike a private litigant, must act in furtherance of the public interest.”) (explaining that the public interest mandate entitles the Commission to reserve to itself the option of withdrawing its acceptance of a consent decree after the public comment period).

4 See FTC v. Circa Direct LLC, 2012 U.S. Dist. LEXIS 81878, *3-*6 (D.N.J. June 13, 2012) (expressing the concern that when being faced with a settlement without an admission of liability, it is difficult to determine whether or not the public interest is being served).
Dissenting Statement

I should add that I am also in favor of reconsidering Rule 2.32’s authorization of the inclusion of language in a consent agreement that it “is for settlement purposes only and does not constitute an admission by any party that the law has been violated as alleged in the complaint.” In comparison, the Securities and Exchange Commission’s informal procedures provide that, “it is important to avoid creating, or permitting to be created, an impression that a decree is being entered or a sanction imposed, when the conduct alleged did not, in fact, occur.”

Accordingly, the SEC has adopted a policy not to permit a defendant or respondent to consent to a judgment or order that imposes a sanction while denying the allegations in the complaint or order for proceedings. Importantly, the SEC also has concluded that “a refusal to admit the allegations is equivalent to a denial, unless the defendant or respondent states that he neither admits nor denies the allegations.” I would encourage consideration of whether our authorization of language that a consent agreement “is for settlement purposes only and does not constitute an admission that the law has been violated” is tantamount to a denial and if so, whether the Commission should similarly embrace the “neither admits nor denies” model language.

Second, while I hope that the majority is correct in their assertion that the consent order covers the deceptive practices of Facebook as well as the applications (“apps”) that run on the Facebook platform, it is not clear to me that it does. In particular, I am concerned that the order may not unequivocally cover all representations made in the Facebook environment (while a user is “on Facebook”) relating to the deceptive information sharing practices of apps about which Facebook knows or should know. For example, a reporter from Forbes recently disclosed that while downloading an app on Facebook, a pop up screen informed users that “This app shares articles you read and more on Facebook with:” and then allowed users to choose between “public,”

---

5 17 C.F.R. § 202.5(e).

6 Id.

7 Id.
Dissenting Statement

“friends,” or “only me.” The reporter assumed – as most users would – that choosing “only me” meant that no one else would be able to see what one was reading when using that app. However, to the contrary, according to this report, choosing “only me” merely meant that your reading habits didn’t show up in your friends’ news feed or tickers on Facebook. Users reading articles within the app would still see articles read by other users, even those users that had chosen the “only me” option. Apparently there is no way to turn off sharing within the app, except on an article-by-article basis. I consider such inadequate disclosure to be deceptive when it occurs in the Facebook environment, irrespective of whether that failure to fully disclose stems from the conduct of the app or Facebook itself. I would include language in the order to make that clear, lest Facebook argue subsequently that the Commission order only covers deceptive conduct engaged in by Facebook itself.

---


9 Subsequently, some changes have been made to the Washington Post Social Reader application download page. There is now a small question mark icon located next to the “who can see activity from this app on Facebook” language. When a user scrolls over the question mark icon, it says “This does not control who can see your activity within the app itself.”

10 Users can learn about the app on the Washington Post website or on the Facebook website. The app is downloaded from the Facebook website itself and users access the application while on Facebook.
ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Facebook, Inc. (“Facebook”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

Since at least 2004, Facebook has operated www.facebook.com, a social networking website that enables a consumer who uses the site (“user”) to create an online profile and communicate with other users. Among other things, a user’s online profile can include information such as the user’s name, a “profile picture,” interest groups they join, a “Friend List” of other users who are the user’s “Friends” on the site, photo albums and videos they upload, and messages and comments posted by them or by other users. Users can also use third-party applications through the site (“Apps”) to, for example, play games, take quizzes, track their physical fitness routines for comparison to their friends’ routines, or receive discount offers or calendar reminders. As of August 2011, Facebook had more than 750 million users.

The Commission’s complaint alleges eight violations of Section 5(a) of the FTC Act, which prohibits deceptive and unfair acts or practices in or affecting commerce, by Facebook:

- **Facebook’s Deceptive Privacy Settings:** Facebook communicated to users that they could restrict certain information they provided on the site to a limited audience, such as “Friends Only.” In fact, selecting these categories did not prevent users’ information from being shared with Apps that their Friends used.

- **Facebook’s Deceptive and Unfair December 2009 Privacy Changes:** In December 2009, Facebook changed
its site so that certain information that users may have designated as private – such as a user’s Friend List – was made public, without adequate disclosure to users. This conduct was also unfair to users.

- **Facebook’s Deception Regarding App Access:** Facebook represented to users that whenever they authorized an App, the App would only access the information of the user that it needed to operate. In fact, the App could access nearly all of the user’s information, even if unrelated to the App’s operations. For example, an App that provided horoscopes for users could access the user’s photos or employment information, even though there is no need for a horoscope App to access such information.

- **Facebook’s Deception Regarding Sharing with Advertisers:** Facebook promised users that it would not share their personal information with advertisers; in fact, Facebook did share this information with advertisers when a user clicked on a Facebook ad.

- **Facebook’s Deception Regarding its Verified Apps Program:** Facebook had a “Verified Apps” program through which it represented that it had certified the security of certain Apps when, in fact, it had not.

- **Facebook’s Deception Regarding Photo and Video Deletion:** Facebook stated to users that, when they deactivate or delete their accounts, their photos and videos would be inaccessible. In fact, Facebook continued to allow access to this content even after a user deactivated or deleted his or her account.

- **Safe Harbor:** Facebook deceptively stated that it complied with the U.S.-EU Safe Harbor Framework, a mechanism by which U.S. companies may transfer data from the European Union to the United States consistent with European law.
The proposed order contains provisions designed to prevent Facebook from engaging in practices in the future that are the same or similar to those alleged in the complaint.

Part I of the proposed order prohibits Facebook from misrepresenting the privacy or security of “covered information,” as well as the company’s compliance with any privacy, security, or other compliance program, including but not limited to the U.S.-EU Safe Harbor Framework. “Covered information” is defined broadly as “information from or about an individual consumer, including but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol (“IP”) address, User ID, or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above.”

Part II of the proposed order requires Facebook to give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings. A “material . . . practice is one which is likely to affect a consumer’s choice of or conduct regarding a product.” FTC Policy Statement on Deception, Appended to Clifdale Associates, Inc., 103 F.T.C. 110, 174 (1984).

Part III of the proposed order requires Facebook to implement procedures reasonably designed to ensure that a user’s covered information cannot be accessed from Facebook’s servers after a reasonable period of time, not to exceed thirty (30) days, following a user’s deletion of his or her account.

Part IV of the proposed order requires Facebook to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook’s size.
Analysis to Aid Public Comment

and complexity, the nature and scope of its activities, and the sensitivity of covered information. Specifically, the order requires Facebook to:

- designate an employee or employees to coordinate and be responsible for the privacy program;

- identify reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of covered information and assess the sufficiency of any safeguards in place to control these risks;

- design and implement reasonable controls and procedures to address the risks identified through the privacy risk assessment and regularly test or monitor the effectiveness of these controls and procedures;

- develop and use reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and require service providers by contract to implement and maintain appropriate privacy protections; and

- evaluate and adjust its privacy program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its privacy program.

Part V of the proposed order requires that Facebook obtain within 180 days, and every other year thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that it has in place a privacy program that provides protections that meet or exceed the protections required by Part IV of the proposed order; and its privacy controls are operating with sufficient effectiveness to provide reasonable assurance that the privacy of covered information is protected.
Parts VI through X of the proposed order are reporting and compliance provisions. Part VI requires that Facebook retain all “widely disseminated statements” that describe the extent to which respondent maintains and protects the privacy, security, and confidentiality of any covered information, along with all materials relied upon in making such statements, for a period of three (3) years. Part VI further requires Facebook to retain, for a period of six (6) months from the date received, all consumer complaints directed at Facebook, or forwarded to Facebook by a third party, that relate to the conduct prohibited by the proposed order, and any responses to such complaints. Part VI also requires Facebook to retain for a period of five (5) years from the date received, documents, prepared by or on behalf of Facebook, that contradict, qualify, or call into question its compliance with the proposed order. Part VI additionally requires Facebook to retain for a period of three (3) years, each materially different document relating to its attempt to obtain the affirmative express consent of users referred to in Part II, along with documents and information sufficient to show each user’s consent and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Facebook has attempted to obtain such consent. Finally, Part VI requires that Facebook retain all materials relied upon to prepare the third-party assessments for a period of three (3) years after the date that each assessment is prepared.

Part VII requires dissemination of the order now and in the future to principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of the order. Part VIII ensures notification to the FTC of changes in corporate status. Part IX mandates that Facebook submit an initial compliance report to the FTC and make available to the FTC subsequent reports. Part X is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify the proposed order’s terms in any way.