

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA,

Plaintiff

v.

FACEBOOK, Inc.,  
a corporation,

Defendant.

Case No. 19-cv-2184

**COMPLAINT FOR CIVIL  
PENALTIES, INJUNCTION, AND  
OTHER RELIEF**

Plaintiff, the United States of America, acting by and through the Consumer Protection Branch of the U.S. Department of Justice, alleges that:

1. Plaintiff brings this action against Defendant Facebook, Inc. (“Facebook”) under Sections 5(a) and (l) and 16(a)(1) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a) and (l) and 56(a)(1), to obtain civil penalties, an injunction, and other equitable relief for violations of a 2012 order previously issued by the Federal Trade Commission (“FTC” or “Commission”) for violations of Section 5(a) of the FTC Act. *See* Exhibit A, *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012) (Decision and Order) (“Commission Order” or “2012 Order”). This action seeks to hold Facebook accountable for its failure to protect consumers’ privacy as required by the 2012 Order and the FTC Act.

### **NATURE OF THE CASE**

2. Facebook operates a social-networking service through its website—[www.facebook.com](http://www.facebook.com)—and mobile applications. Those applications connect consumer users of Facebook’s service, who each create a Facebook “profile” showing personal information, with “Friends” who also have Facebook accounts and profiles (“Friends” or “Facebook Friends”). Through its service, Facebook collects and maintains vast amounts of consumer information. As of 2018, Facebook had more than 2.2 billion monthly active users worldwide. Over one hundred million Americans use Facebook every day to share personal information, such as their real name, date of birth, hometown, current city, employer, relationship status, and spouse’s name, as well as sensitive personal information, such as political views, sexual orientation, photos of minor children, and membership in health-related and other support groups. Users can also provide information about themselves by indicating that they “like” public Facebook pages. Research suggests that a user’s “likes” of public Facebook pages can be used to accurately predict that user’s personality traits, sometimes better than the user’s own friends and family. In addition, Facebook users may install and use applications (“apps”) developed by third-parties (“third-party developers”) that allow the users to share information with their Facebook Friends.

3. Facebook’s core business model monetizes user information by using it for advertising. Substantially all of Facebook’s \$55.8 billion in 2018 revenues came from advertising.

4. To encourage users to share information, Facebook promises users that they can control the privacy of their information through Facebook’s privacy settings. However, through at least June 2018, Facebook subverted users’ privacy choices to serve its own business interests.

5. Beginning at least as early as 2010, every Facebook user who installed an app (“App User”) agreed to Facebook sharing with the third-party developer of the installed app both information about the App User and the App User’s Facebook Friends. Facebook’s default settings were set so that Facebook would share with the third-party developer of an App User’s app not only the App User’s data, but also data of the App User’s Facebook Friends (“Affected Friends”), even if those Affected Friends had not themselves installed the app. Affected Friends could only avoid this sharing by finding and opting out of it via settings on Facebook’s Applications page, which was located on Facebook’s website and mobile applications, separate and apart from Facebook’s Privacy Settings page. Third-party developers that received user and Affected Friend information could use that information to enhance the in-app experience or target advertising to App Users and their Affected Friends. In the wrong hands, user and Affected Friend data could be used for identity theft, phishing, fraud, and other harmful purposes.

6. In 2012, after an FTC investigation, Facebook settled allegations that its practice of sharing Affected Friends’ data with third-party developers of apps was deceptive. The resulting Commission Order, among other things, prohibits Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information accessible to third parties. *See* Commission Order, Parts I.B. & C.

7. In the wake of the FTC’s initial investigation, Facebook retained the separate opt-out sharing setting on its Applications page, but it added a disclaimer to its Privacy Settings page, warning users that information shared with Facebook Friends could also be shared with the

apps those Friends used. However, four months after the 2012 Order was finalized, Facebook removed this disclaimer—even though it was still sharing Affected Friends data with third-party developers and still using the same separate opt-out setting that undermined users’ privacy choices before entry of the Commission Order.

8. At its F8 conference in April 2014—one theme of which was user trust—Facebook announced that it would stop allowing third-party developers to collect data about Affected Friends. Facebook also told third-party developers that existing apps could only continue to collect Affected Friend data for one year, or until April 2015. But, after April 2015, Facebook had private arrangements with dozens of developers, referred to as “Whitelisted Developers,” that allowed those developers to continue to collect the data of Affected Friends, with some of those arrangements lasting until June 2018.

9. At least tens of millions of American users relied on Facebook’s deceptive privacy settings and statements to restrict the sharing of their information to their Facebook Friends, when, in fact, third-party developers could access and collect their data through their Friends’ use of third-party developers’ apps. Facebook knew or should have known that its conduct violated the 2012 Order because it was engaging in the very same conduct that the Commission alleged was deceptive in Count One of the original Complaint that led to the 2012 Order. *See* Exhibit B, *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 136 (F.T.C. July 27, 2012) (“Original Complaint”).

10. Facebook also failed to maintain a reasonable privacy program that safeguarded the privacy, confidentiality, and integrity of user information, as required by Part IV of the 2012 Order. The requirement in the 2012 Order that Facebook maintain a reasonable privacy program

was vitally important because Facebook had allowed millions of third-party developers to access and collect massive troves of consumer data about both App Users and their Facebook Friends, and Facebook failed to track that data in an organized, systematic way.

11. As a general practice, Facebook did not vet third-party developers before granting them access to consumer data; instead, developers simply had to check a box agreeing to comply with Facebook's policies and terms and conditions, including those designed to protect consumer information. This made Facebook's enforcement of its policies, terms, and conditions acutely important.

12. Facebook's enforcement of its policies, terms, and conditions, however, was inadequate and was influenced by the financial benefit that violator third-party app developers provided to Facebook. This conduct was unreasonable. Facebook never disclosed this disparate enforcement practice to the third-party assessor charged by the 2012 Order with assessing the implementation and effectiveness of Facebook's privacy program, nor did Facebook disclose its enforcement practices to the Commission in its biennial assessment reports mandated by the 2012 Order. *See* Commission Order, Part V.

13. In addition to its violations of the 2012 Order, Facebook also engaged in deceptive practices in violation of Section 5(a) of the FTC Act. Between November 2015 and March 2018, Facebook asked its users to provide personal information to take advantage of security measures on the Facebook website or mobile application, including a two-factor authentication measure that encouraged provision of users' phone numbers. Facebook did not effectively disclose that such information would also be used for advertising.

14. Finally, in April 2018, Facebook updated its data policy to explain that Facebook would use an updated facial-recognition technology to identify people in user-uploaded pictures and videos “[i]f it is turned on,” implying that users must opt in to use facial recognition. Contrary to the implication of this updated data policy, however, tens of millions of users who still had an older version of Facebook’s facial-recognition technology had to opt out to disable facial recognition. This violated the 2012 Order by misrepresenting the extent to which consumers could control the privacy of their information used for facial recognition.

### **JURISDICTION AND VENUE**

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355; and 15 U.S.C. §§ 45(a) and (l), and 56(a)(1).

16. Venue in this District is proper under 28 U.S.C. §§ 1391(b)(2), (c)(2), and 1395(a); and 15 U.S.C. § 53(b).

### **DEFENDANT**

17. Facebook, Inc. is a Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025. At all times relevant to this Complaint, Facebook has operated its social-networking service through its website, www.facebook.com, and mobile applications that connect users with Friends on Facebook.

### **COMMERCE**

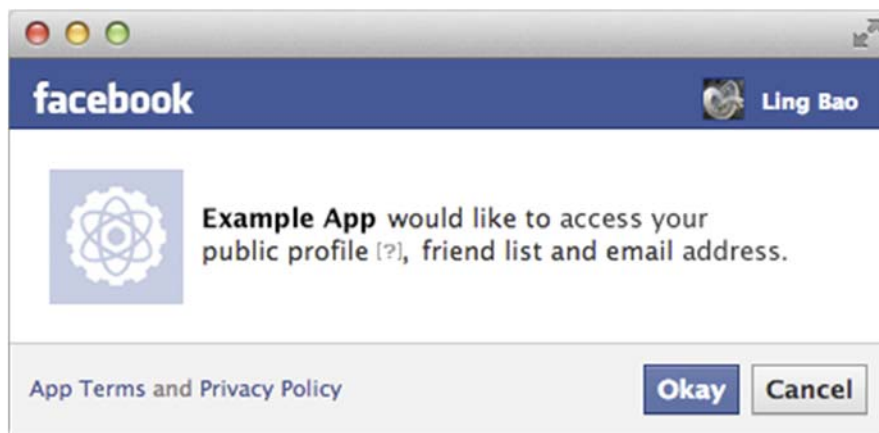
18. At all times material to this Complaint, Facebook maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

### **THE COMMISSION ORDER**

19. As part of Facebook’s operation of its social-networking service, it has for years offered the Facebook Platform (“Platform”), a set of tools and application programming interfaces (“APIs”) that enable third-party developers to access user data and develop software applications, such as games, with which Facebook users can interact; it also allows users to use apps or log into websites using their Facebook credentials.

20. In April 2010, Facebook launched an initial version of the Graph API (“Graph API V1”), which allowed third-party developers to access and collect data about Facebook App Users. Graph API V1 also allowed third-party developers to access and collect data about Affected Friends.

21. At that time, Facebook’s settings presented an App User with a screen whereby the app requested permission from the App User before initial installation to permit it to access certain fields of data, as shown in the example below:<sup>1</sup>



---

<sup>1</sup> <https://newsroom.fb.com/news/2012/12/better-controls-for-managing-your-content/>

22. Facebook did not require third-party developers to request permission directly from Affected Friends of App Users to access those Affected Friends' data from Facebook. Instead, Facebook automatically sent Affected Friend data based solely on App Users' granted permission.

23. Using this process, third-party developers could collect dozens of pieces of data from Facebook about Affected Friends, including information related to each Affected Friend's:

- birthday
- bio
- activities
- news article activity
- books activity
- check-ins
- current city
- education history
- events
- fitness activity
- games activity
- groups
- hometown
- interests
- likes
- music activity
- notes
- online presence
- Open Graph activity
- photos
- questions
- relationships
- relationship details
- religion/political views
- status
- subscriptions
- videos
- video-watch activity
- website URL
- work history



24. In its 2012 Original Complaint in the proceeding bearing Docket No. C-4365, the Commission charged Facebook with engaging in unfair and deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), for, among other things, its practices associated with giving third-party developers access to Affected Friends' data.

25. Specifically, Count One of the Original Complaint alleged that Facebook was engaging in deceptive acts and practices by representing to users that Facebook's privacy settings allowed them to restrict to limited audiences (*e.g.*, "Only Friends") the sharing of non-public personal information that they added to their Facebook profiles and their non-public Facebook posts (collectively, "Profile Information"), when, in fact, those settings did not prevent Facebook from sharing that information with third-party developers of apps installed by the users' Friends. *See* Exhibit B at ¶¶ 10-18.

26. The Original Complaint also asserted that Facebook misled users by placing the option to block third-party developers from accessing their information through Friends not prominently on Facebook's Privacy Settings page, but rather, on a page called, at various times, "Applications," "Apps," or "Applications and Websites." This Applications page allowed users, among other things, to restrict the information that third-party developers of Friends' apps could access. But no Facebook page other than the Applications page disclosed to users that, unless they adjusted the setting on the Applications page, their other privacy choices were ineffective to prevent the sharing of their data with third-party developers of their Friends' apps.

27. The Original Complaint also noted that users who did not themselves use apps would have no reason to click on the Applications page, and thus would have concluded that

their choices to restrict Facebook's sharing of their Profile Information through the Privacy Settings page were complete and effective.

28. Facebook settled the Commission's Original Complaint with the Commission Order. The Commission Order became final in August 2012 and remains in effect.

29. Part I of the Commission Order, in relevant part, states:

**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:

...

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;

...

*See Commission Order, Part I.*

30. The Commission Order defines "Covered Information" 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.

*See Commission Order, Definition 4.*

31. Part IV of the Commission Order, in relevant part, states that Facebook shall:

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 [Facebook]’s size and complexity, the nature and scope of [Facebook]’s activities, and the sensitivity of covered information, including:

...

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in [Facebook]’s unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. . . .

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.

...

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

*See* Commission Order, Part IV.

32. Part V of the Commission Order states that Facebook 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.”

33. The Commission Order requires, among other things, that each such Assessment shall:

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

B. explain how such privacy controls are appropriate to [Facebook]’s size and complexity, the nature and scope of [Facebook]’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 [the Commission] 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 operating period.

*See* Commission Order, Part V.

#### **DEFENDANT'S NOTICE OF THE COMMISSION ORDER**

34. Facebook's General Counsel signed the Commission Order on behalf of Facebook. The Commission served the Commission Order in August 2012.

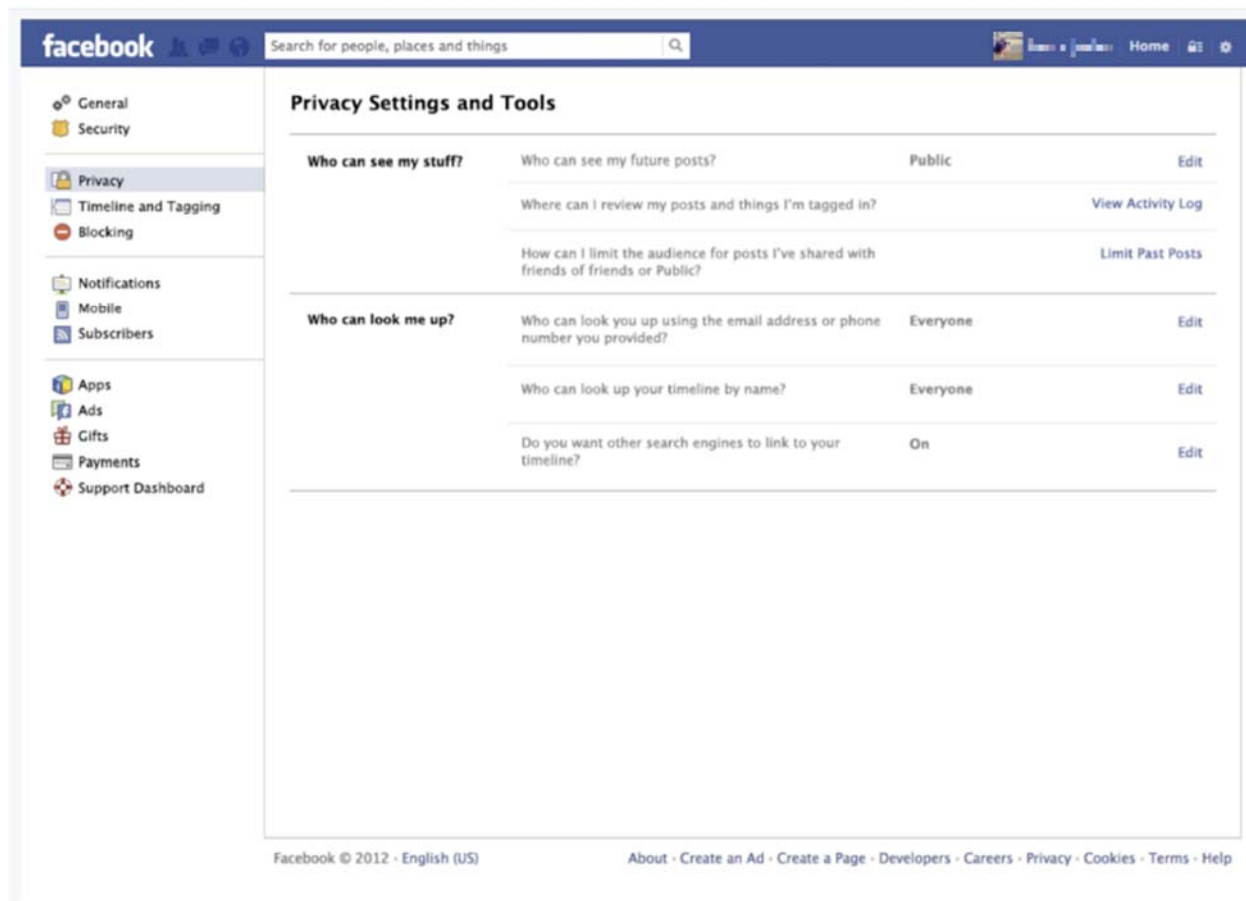
#### **DEFENDANT'S CONDUCT**

##### **Facebook's Desktop Privacy Settings Failed to Disclose That Users' Privacy Choices Would Be Undermined by Default Settings That Allowed Facebook to Share Users' Data with Third-Party Developers of Their Friends' Apps**

35. Around the time that it resolved the Original Complaint through the Commission Order in 2012, Facebook added a disclaimer to the top of its desktop Privacy Settings page stating, "You can manage the privacy of your status updates, photos, and information using the inline audience selector—when you share or afterwards. *Remember: the people you share with can always share your information with others, including apps.*" (emphasis added), as shown in the figure below:



36. Approximately four months after the Commission Order became effective, however, Facebook removed the disclaimer from the Privacy Settings page, as shown in the below example:



37. Facebook’s new “Privacy Settings” page purported to allow users to restrict who could see their past and future posts.

38. Posts could include, among other things, status updates, photos, videos, check-ins, and notes.<sup>2</sup>

39. A user wishing to restrict future posts on the Privacy Settings page would click “edit” and select from non-public categories, such as “Friends,” “Only me,” and “Custom.”

---

<sup>2</sup> <https://developers.facebook.com/docs/graph-api/reference/v2.8/post>

40. Facebook did not disclose anywhere on this page, or anywhere along the path that users would have had to take to reach the Privacy Settings page, that users who shared their posts with “Friends” or a “Custom” audience<sup>3</sup> could still have those posts shared with any of the millions of third-party developers whose apps were used by their Friends.

41. As was the case before the Commission Order, Affected Friends who sought to opt out of such sharing—and to have their privacy choices honored—needed to locate and adjust settings located under the separate “Apps” tab.

42. The Apps tab did not alert users that it linked to a page containing settings that users had to disable in order to have their privacy choices fully honored.

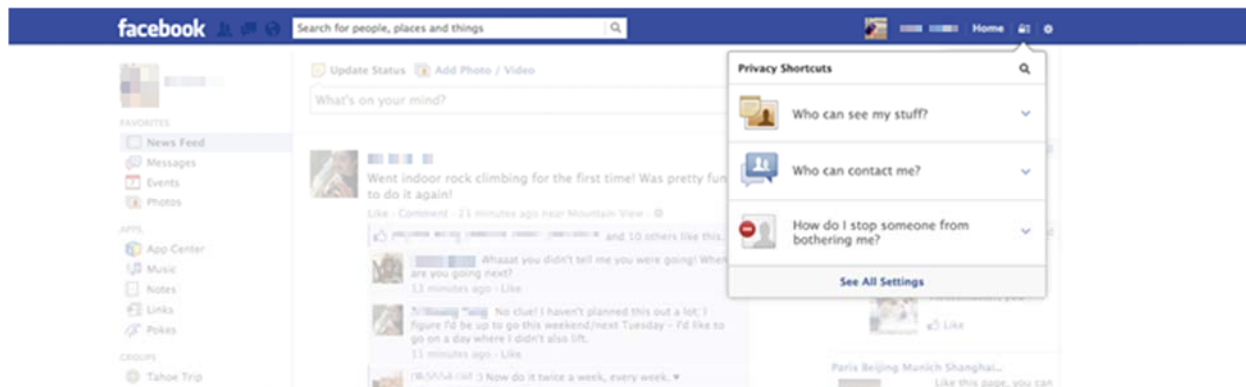
43. In December 2012, Facebook introduced “Privacy Shortcuts,” which it touted as a privacy tool that helps users navigate “key settings.” *See* Exhibit C (Dec. 21, 2012 Press Release); *see also* Exhibit D (May 22, 2014 Press Release) (describing Privacy Shortcuts as a “tool designed to help people make sure they are sharing with just the audience they want”).

44. The Privacy Shortcuts tool also had privacy settings for posts that purported to allow users to restrict their posts to Friends, as shown in the example below:<sup>4</sup>

---

<sup>3</sup> “Custom” audiences are typically a subset of Friends and are thus a more restrictive privacy setting than “Friends.” For simplicity, this Complaint refers to both “Friends” and “Custom” audience selections as “Friends.”

<sup>4</sup> <https://newsroom.fb.com/news/2012/12/better-controls-for-managing-your-content/>



45. However, Facebook did not disclose on the Privacy Shortcuts tool, or anywhere along the path that users took to reach this tool, that their non-public posts could be shared with third-party developers of Friends' apps.

46. At all times relevant to this Complaint, Facebook also provided users with inline controls that purported to allow users to restrict who could see their posts.

47. Specifically, when users posted a status update, photo, or video, Facebook gave users a drop-down menu that allowed them to restrict the audience for that post to, for example, "Friends," as shown below:<sup>5</sup>

---

<sup>5</sup> <https://www.facebook.com/notes/facebook/making-it-easier-to-share-with-who-you-want/10150251867797131/>





48. However, Facebook did not disclose to users that sharing their non-public posts with Friends would allow Facebook to share those posts with third-party developers of Friends’ apps.

49. In addition, Facebook’s settings conveyed that users could restrict on their Facebook “About” page who could see personal information that users added to their profile, such as hometown, birthday, relationship, current city, education history, and work history.

50. But Facebook did not disclose to users on their About page that sharing their personal information with Friends would allow Facebook to share that information with third-party developers of Friends’ apps.

#### **Facebook’s Desktop “Apps others use” and “Platform” Settings Also Undermined Users’ Privacy Choices**

51. Facebook also misled users by having default settings that shared Affected Friends’ Profile Information with third-party developers of Friends’ apps unless the Affected Friend found and opted out of settings found on the Apps Settings page.

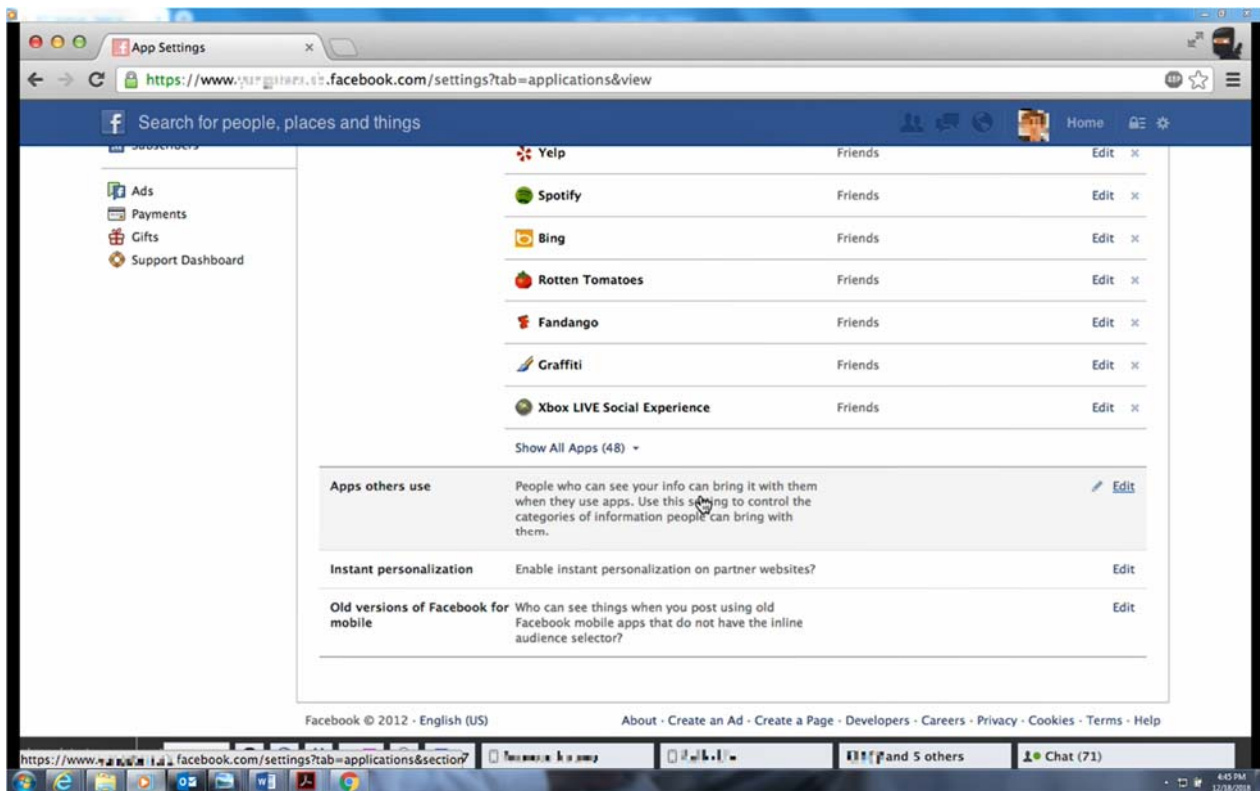
52. The Apps Settings page contained two opt-out settings—the “Apps others use” setting and the “Platform” setting.

53. To access the “Apps others use” setting, Affected Friends first had to realize that Facebook shared their Profile Information with third-party developers of Friends’ apps, and then successfully had to navigate a series of steps to find and opt-out of that setting.

54. A user first had to click on the “Apps” tab in the settings menu. This tab did not include any disclosure that the “Apps” tab linked to any privacy settings for apps not installed by the user.

55. After clicking the “Apps” tab, users were directed to the Apps Settings page, where they had to locate the “Apps others use” setting.

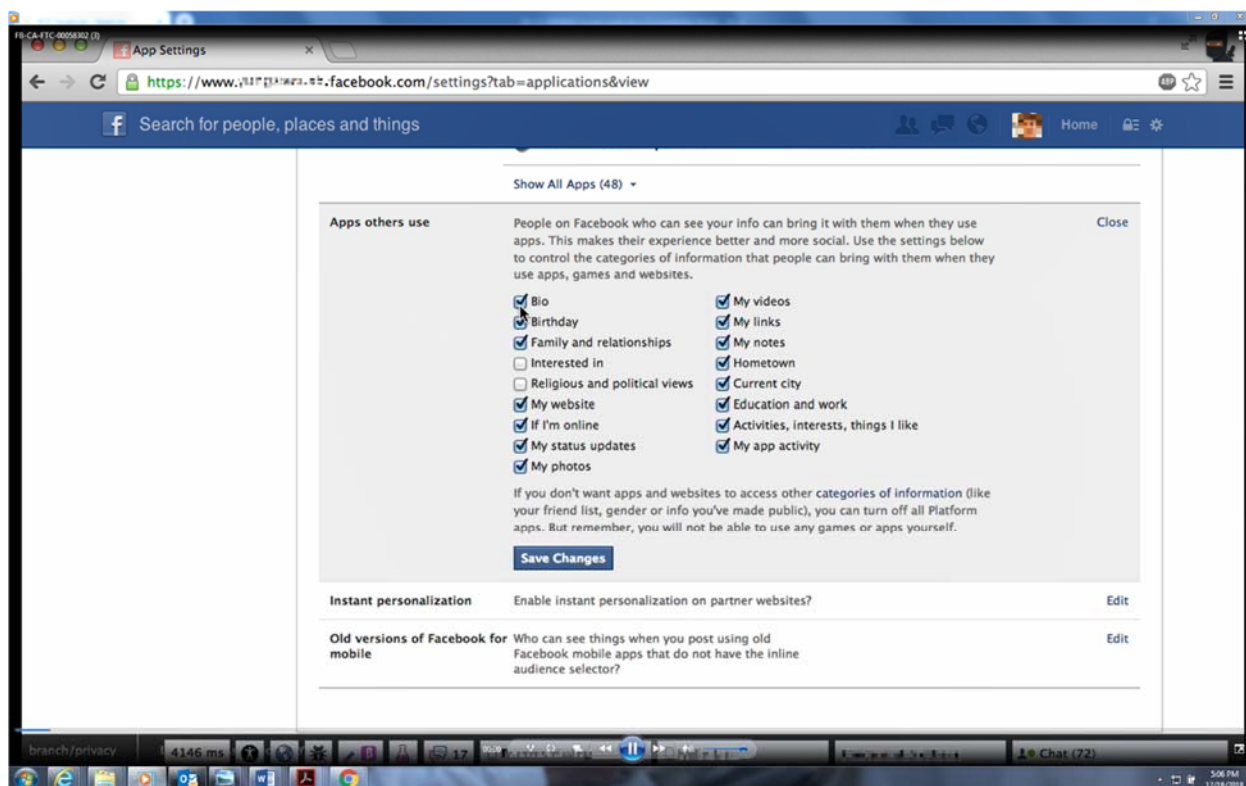
56. The format of the Apps Settings page varied over time. However, at all times relevant to this Complaint, the “Apps others use” setting at the bottom of the page, separate and apart from the privacy settings for the apps the user installed, as shown in the below example:



57. On the “Apps others use” setting, Facebook stated, “People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.”

58. This was Facebook’s only representation on any of the settings pages informing users that third-party developers of Friends’ apps could access and collect their Profile Information.

59. Facebook presented users who clicked on “edit” within the “Apps others use” setting with options that allowed them to opt out of Facebook sharing their data, as shown in the below example:



60. By default, all categories of Affected Friend data, except “Religious and political views” and “Interested in,” were set to be shared with third-party developers who requested them.

61. During all times relevant to this Complaint, only a very low percentage of users opted out of this default setting.

62. Alternatively, users could prevent Facebook from sharing their Profile Information with third-party developers of Friends’ apps by opting out of Facebook’s “Platform” setting within the Apps Setting page. But, in so doing, users could not use any Facebook apps themselves. By default, this setting was turned “on” and allowed Facebook to share users’ data with third-party developers of Friends’ apps.

63. To access the Platform setting, a user had to: (1) click on the “Apps” tab in the settings menu; (2) find the Platform opt-out setting, which was located in a section of the page devoted to the user’s apps and labeled at various times “Apps you use” or “Apps, Websites, and Plugins”; and (3) click on the “edit” button to disable the default setting that shared the user’s data with third-party developers of Friends’ apps.

64. Although the precise language varied over time, disclaimers on the Platform setting warned that turning it off would prevent users from using any Facebook apps themselves and prevent their Friends from being able to “interact and share *with you* using apps and websites” (emphasis added).

## App Settings

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps ([Learn Why](#)). Remember: When you let an app access your **public profile**, it may also access other information you choose to make public.

### Apps you use

#### Platform is on.

[Close](#)

If you turn Platform off you can't use the Facebook integrations on third party apps or websites. If you want to use these apps and websites with Facebook, turn Platform back on. Using Platform allows you to bring your Facebook experience to the other apps and websites you use on the web and to your mobile device and apps. It allows Facebook to receive information about your use of third party apps and websites to provide you with better and more customized experiences. [Learn More](#)

If you turn off Platform apps:

- You will not be able to log into websites or applications using Facebook.
- Your friends won't be able to interact and share with you using apps and websites.
- Instant personalization will also be turned off.
- Apps you've previously installed may still have info you shared. Please contact these apps for details on removing this data.

[Turn Off Platform](#)

 Sösh

Not yet sharing · [Add to timeline](#)

[Edit](#) ×

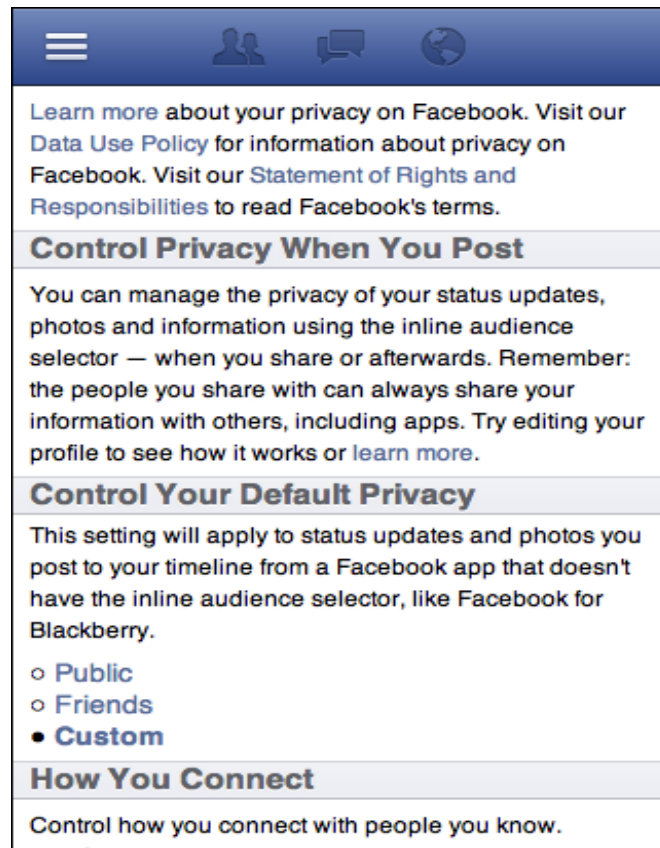
65. This language—which focused on information that would be shared with the user, rather than information Facebook would share about the user—did not inform users that: (a) by default, Facebook shared their Profile Information with third-party developers of Friends' apps; or (b) this setting allowed them to opt out of such sharing.

66. A very low percentage of Facebook users disabled the Platform setting between August 2012 and April 2015.

### Facebook's Mobile Privacy Settings Also Deceived Users

67. As early as March 2012, and until March 2013, as shown in the example below, Facebook's mobile interface contained a disclaimer near the top of the Privacy Settings page stating, "You can manage the privacy of your status updates, photos and information using the

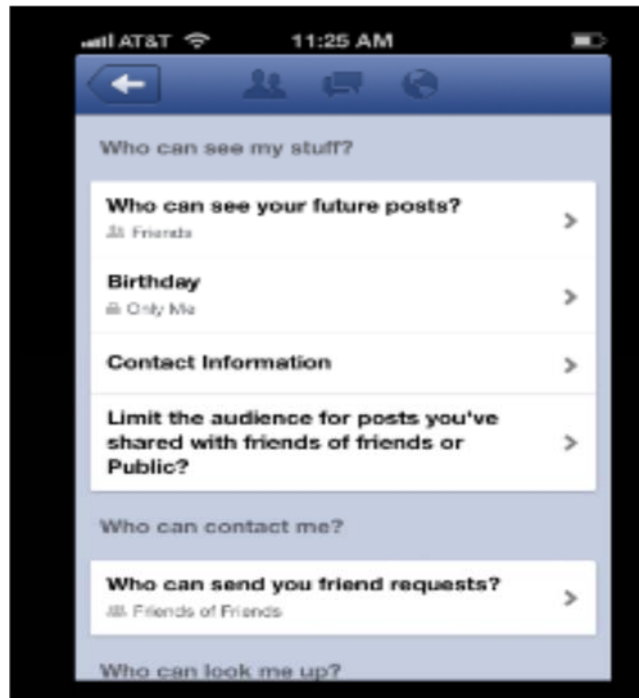
inline audience selector—when you share or afterwards. *Remember: the people you share with can always share your information with others, including apps. . .*” (emphasis added).



68. The mobile Privacy Settings page purported to allow users to restrict who could see their past and future posts, as well as, for approximately six months, users' birthday and contact information.

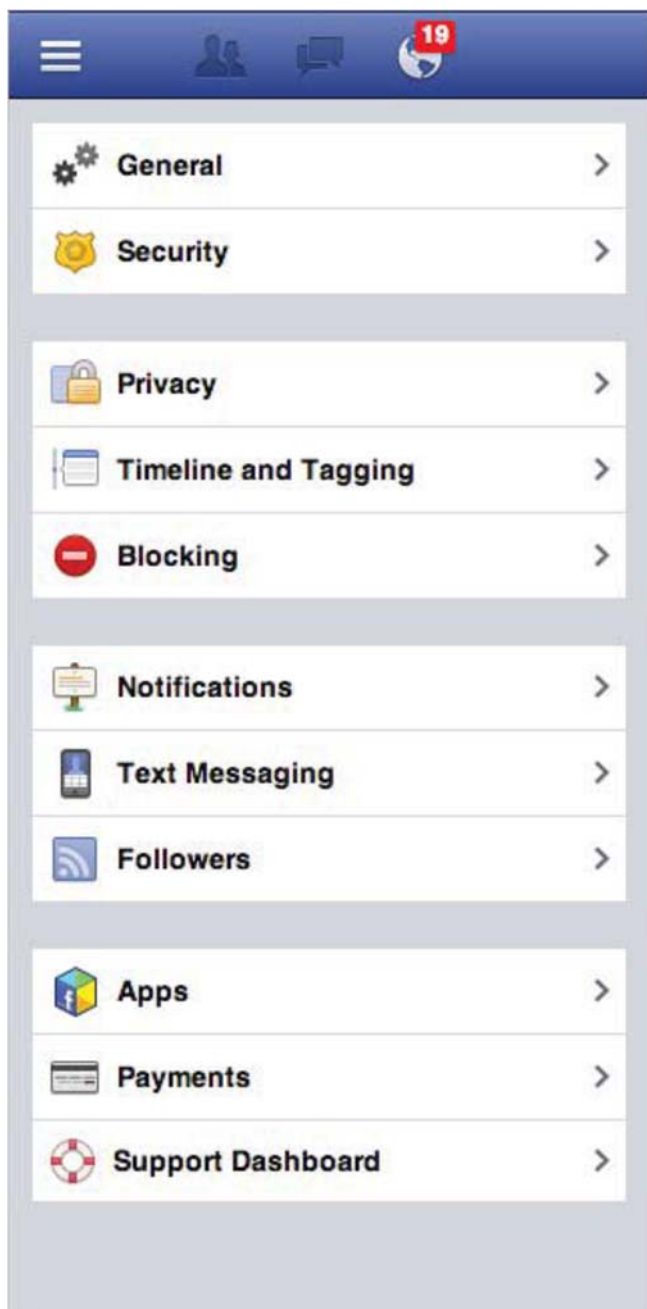
69. During this time, Facebook's Privacy Settings page further featured a link to the Apps Settings page.

70. In or around March 2013, Facebook removed the disclaimer about the sharing of data with apps, as shown in the below figure:



71. Facebook also removed from the mobile Privacy Settings page the link to the Apps Settings page.

72. After Facebook made these changes, to find the Apps Setting page, a user on the mobile interface had to go to the main settings menu and click on the heading labeled “Apps” or “Apps and Websites,” as shown in the below example:



73. The headings did not disclose that the “Apps” or “Apps and Websites” tabs included privacy settings for apps that the user did not install.



74. Once on the Apps Settings page, users had to locate the “Apps others use” setting and click on “edit” before gaining access to options that allowed them to opt out of Facebook sharing their data with third-party developers of Friends’ apps.

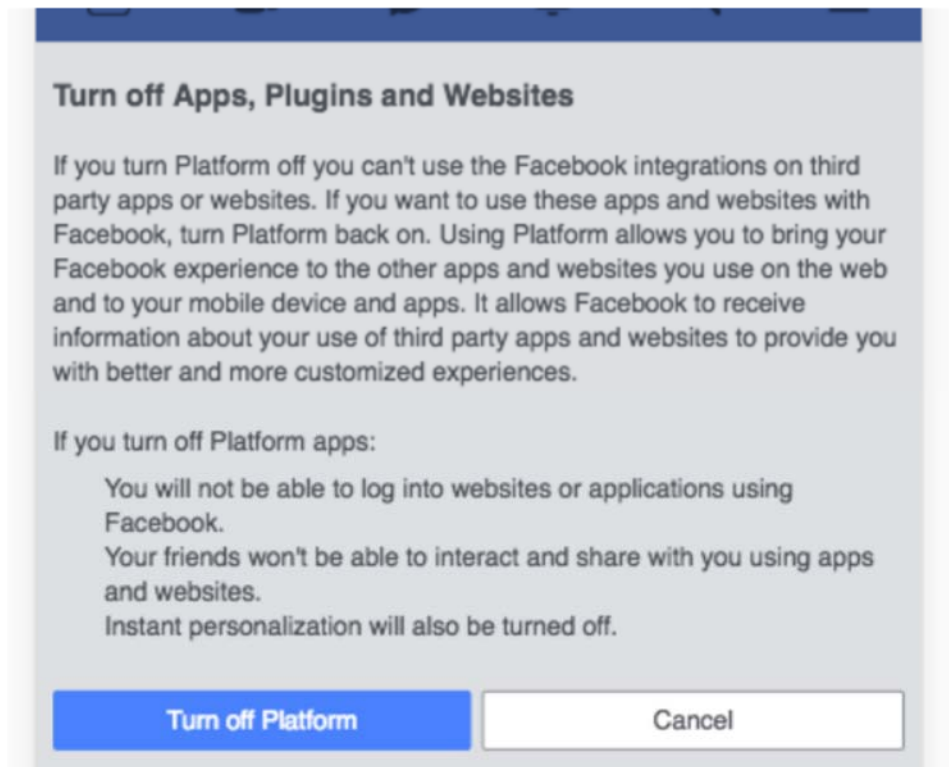
75. The “Apps others use” setting was located separate and apart from the privacy settings for the apps the user installed.

76. Users’ bios, birthdays, family and relationships, websites, status updates, photos, videos, links, notes, hometowns, current cities, education histories, work histories, activities, interests, “likes,” app activity, and status of being online, were set to be shared with third-party developers by default.

77. Similarly, to access the Platform setting in the mobile interface, users had to click on the “Apps” heading in the settings menu and then click on the “Platform” opt-out setting link.

78. The Platform setting link referenced apps the *user* authorized rather than apps authorized by the user’s Friends.

79. Moreover, although the precise language varied over time, disclaimers on the Platform setting explained that turning off the Platform setting would prevent users from using any Facebook apps themselves and prevent their Friends from being able to “interact and share *with you* using apps and websites” (emphasis added).



80. This language—which focused on information that would be shared with the user rather than information Facebook would share about the user—did not alert users to the fact that: (a) Facebook shared their Profile Information with third-party developers of Friends’ apps by default; or (b) the Platform setting allowed them to opt out of such sharing.

**Facebook Was Aware That Giving Millions of Third-Party Developers Access to Affected Friend Data Posed Privacy Risks**

81. Facebook was aware of the privacy risks posed by allowing millions of third-party developers to access and collect Affected Friend data for nearly two years before it changed the Graph API to remove third-party developers’ access to that data. By August 2013, Facebook had decided to remove third-party developers’ access to Affected Friend data. As an internal document explained:

We are removing the ability for users to share data that belongs to their friends who have not installed the app. Users should not be able to act as a proxy to access personal information about friends that have not expressed any intent in using the app.

82. In September 2013, Facebook audited a set of apps to determine whether to revoke their data permissions. That audit revealed that over a 30-day period, the audited apps were making hundreds of millions of requests to the Graph API for a variety of data, including Affected Friends' work histories, photos, videos, statuses, "likes," interests, events, education histories, hometowns, locations, relationships, and birthdays.

83. In some instances, the apps called for data about Affected Friends in numbers that greatly exceeded the number of the apps' monthly active users. For example, one app highlighted in the audit made more than 450 million requests for data—roughly 33 times its monthly active users.

84. Indeed, the volume of data acquired by the audited apps led one Facebook employee to comment, "I must admit, I was surprised to find out that we are giving out a lot here for no obvious reason."

85. This was not the only instance in which an examination of apps showed massive amounts of Affected Friends' data being accessed. A mere month after the September 2013 audit, while discussing upcoming Platform changes, senior Facebook management employees observed that third-party developers were making more than *800 billion* calls to the API per month and noted that permissions for Affected Friends' data were being widely misused.

86. Likewise, in 2014, when discussing changes that would be made to the Platform, Facebook senior management employees considered reports showing that, every day, more than 13,000 apps were requesting Affected Friends' data.

87. Facebook made several changes to the Privacy Settings and Apps Settings pages throughout 2013 and 2014. However, none of the changes sought to inform users that sharing data with their Friends also allowed Facebook to share that data with any of the more than one million third-party developers whose apps could be used by their Friends.

**Financial Considerations Influenced Facebook’s Decisions Regarding Whether to Restrict Third-Party Developers’ Access to User Data**

88. Even though Facebook acknowledged the data-privacy risks associated with the data access it gave to third-party developers, on numerous occasions, while determining whether to continue granting a particular developer access to user data, it considered how large a financial benefit the developer would provide to Facebook, such as through spending money on advertisements or offering reciprocal data-sharing arrangements.

89. At one point in 2013, for instance, Facebook considered whether to maintain or remove data permissions for third-party developers based on whether the developer spent at least \$250,000 in mobile advertising with Facebook.

90. As internal Facebook documents explained, Facebook would contact apps spending more than \$250,000 on advertising and ask them to confirm the need for the data they were accessing, while Facebook would terminate access for apps spending less than \$250,000.

91. Similarly, during the transition to the second version of Graph API (“Graph API V2”), when preparing to implement changes to the Platform to remove third-party developers’ access to Affected Friend data, Facebook explicitly evaluated whether apps affected by the changes spent money on advertising with Facebook, generated revenue for the company, or otherwise offered something of value such as reciprocal access to user data.

**Facebook Falsely Announced That Third-Party Developers Would No Longer Be Able to Access Affected Friend Data**

92. In 2013, Facebook conducted a survey that showed that its users were concerned about sharing their data with apps, believed apps asked for unnecessary information or permissions, and were concerned about the information apps used for marketing.

93. Similarly, based on research Facebook conducted, Facebook employees discussed that certain categories of data requests—the user’s activities, birthday, education history, list of interests, religious and political affiliation, page “likes,” photos, videos, hometown, relationship preferences, work history, current city, status messages, and check-ins—were sensitive and, accordingly, should require review after Graph API V2 was introduced.

94. As one employee explained, “Perm[ission]s like user relationships, work history, and relationship details (which indicates the user’s gender preferences) can be perceived as really sensitive. It’s really bad for user trust whenever these perm[ission]s are asked for. . . .”

95. Facebook communicates with its users through various means, including keynote addresses during F8 conferences, videos on Facebook’s YouTube channel, and Facebook Newsroom.

96. In April 2014, Facebook announced that it was deprecating (*i.e.*, discontinuing) Graph API V1 and replacing it with Graph API V2.

97. At Facebook’s April 30, 2014 F8 Conference, Facebook announced that it would no longer allow third-party developers to collect Affected Friend data. In the keynote address, Facebook explained:

[W]e’ve also heard that sometimes you can be surprised when one of your friends shares some of your data with an app. . . . So now we’re going to change this, and *we’re going to make it so that now, everyone has to choose to share their own data with an app*

*themselves*. . . . [W]e think this is a really important step for giving people power and control over how they share their data with apps.

(emphasis added). Facebook posted a video of this keynote address on its YouTube channel in May 2014.

98. On April 30, 2014, Facebook also issued a press release in which it stated:

**Putting people first:** We've heard from people that they are worried about sharing information with apps, and they want more control over their data. We are giving people more control over these experiences so they can be confident pressing the blue button.

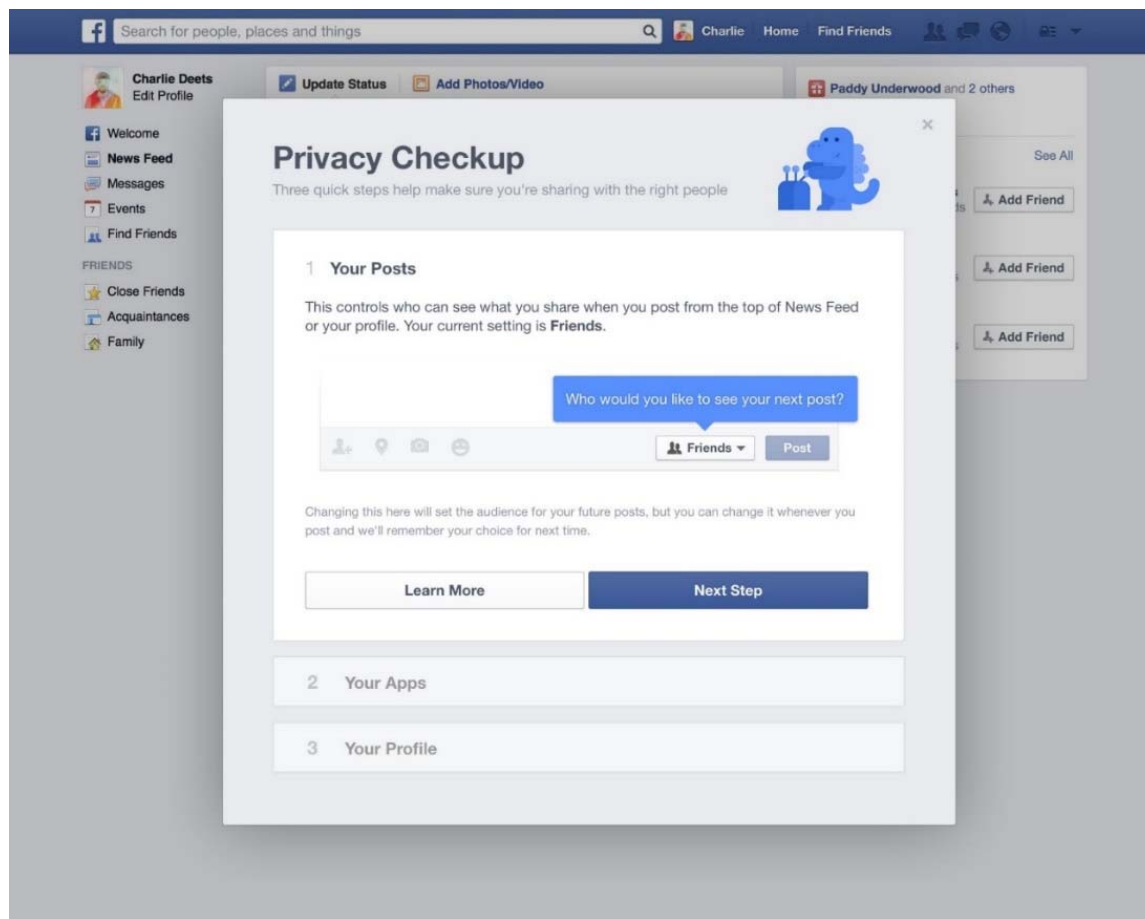
99. These communications with users addressed, among other things, the privacy controls that Facebook made available on its Platform.

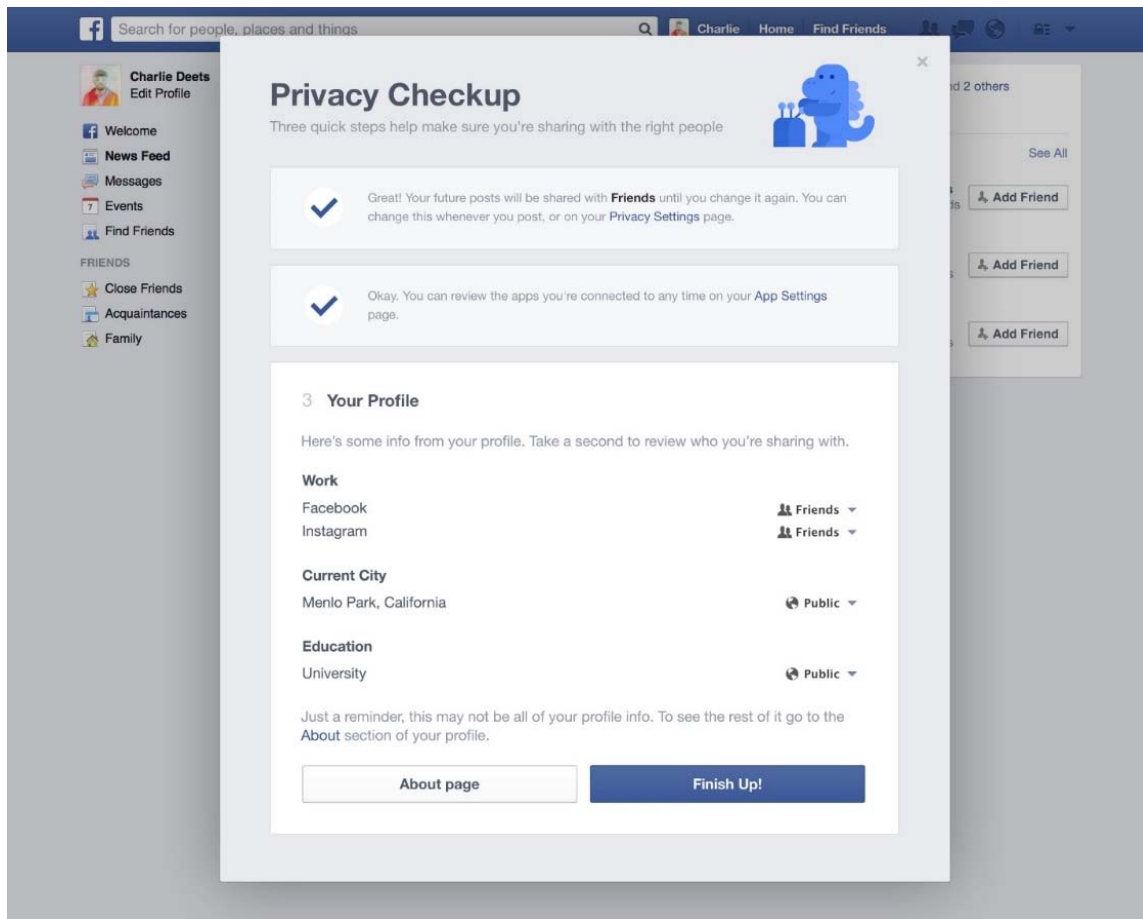
100. Despite these clear statements, Facebook gave third-party developers with a pre-existing, approved app at least one year of continued access to Affected Friends' data. In other words, third-party developers that had a preexisting app on the Facebook Platform as of April 2014 could still access and collect Affected Friend data until April 2015. Facebook did not disclose this fact to its users.

**Facebook's Privacy Checkup Did Not Tell Users That Sharing with Their Friends Allowed Third-Party Developers to Access Their Profile Information**

101. In September 2014, Facebook launched "Privacy Checkup." Facebook publicized Privacy Checkup as a means to help users "be in control" of what they shared and with whom they shared it. *See* Exhibit E (Press release).

102. Privacy Checkup purported to allow users to restrict who could see their posts and “review and edit the privacy of key pieces of information,” Exhibit E, on the user’s profile, as shown in the below figures:





103. The Privacy Checkup tool highlighted the apps that users installed, but it did not list the apps that had access to users' Profile Information based on their Friends' consent.

104. The Privacy Checkup tool also included a link to the Facebook user's About page, where Profile Information such as birthdate, hometown, religious views, political views, interests (e.g., sports teams, music, movies), public page "likes," relationships, and relationship details were displayed. These settings also purported to allow users to restrict who could see their data.

105. Facebook did not disclose anywhere on these pages that, when users shared their Profile Information with Friends, Facebook could continue to share that information with millions of third-party developers of their Friends' installed apps.



**Facebook Finally Removed General Access to Affected Friend Data but Granted Special Access to Affected Friend Data to Certain Developers Without Telling Users**

106. On April 30, 2015, Facebook deprecated Graph API V1. As a result, this generally required third-party developers that had not already migrated to Graph API V2 to do so. Graph API V2 did not allow third-party developers to access or collect Affected Friend data.

107. In or around April 2015, Facebook gathered journalists in San Francisco and discussed the deprecation of Graph API V1 and the removal of access to Affected Friend data.

108. However, going forward, Facebook privately granted continued access to Graph API V1 to more than two dozen developers—the Whitelisted Developers—which included gaming, retail, and technology companies, as well as third-party developers of dating apps and other social-media services. Those Whitelisted Developers thus still had access to the same Affected Friend data that Facebook had publicly announced was no longer available.

109. Some of the Whitelisted Developers retained access for months, while others retained access for years.

110. Facebook granted access to Affected Friend data to a few Whitelisted Developers as a beta test, with that access left active until June 2018.

111. Facebook granted other Whitelisted Developers specific permissions to Affected Friend data, including data on public page “likes,” location, education, work status, relationship status, notes, groups, events, photos, religion, “looking for,” significant other, websites, activities, and interests—much of which Facebook knew consumers might be sensitive to sharing.

112. Facebook did not tell its users that it was still granting these Whitelisted Developers access to their data.

113. When users chose to share their data with Friends, they had no way of knowing that Facebook would still share it with these Whitelisted Developers.

**Facebook Failed to Implement and Maintain Appropriate Safeguards and Controls Over Third-Party Developers' Access to User Data**

114. To address concerns associated with Facebook's sharing of user and Affected Friend data with the more than 36 million third-party apps on the Facebook Platform in 2012, Part IV of the Commission Order required Facebook to implement and maintain a comprehensive privacy program reasonably designed to address privacy risks and protect the privacy and confidentiality of covered information.

115. Part V of the Commission Order required Facebook to obtain initial and biennial assessments from an independent third-party professional that, among other things, set forth Facebook's specific privacy controls and explained how those controls met or exceeded Part IV's requirements.

116. In the initial and biennial assessment reports required by the Commission Order, Facebook claimed that it had implemented certain controls and procedures to address the privacy risks created by the extensive access to user data it provided to third-party developers.

117. Facebook's assessment reports also claimed that it had monitoring controls in place to detect material misuse of the Platform by third-party developers.

118. Other than requiring third-party developers to agree to Facebook's policies and terms when they registered their app with the Platform ("Platform Policies"), however, Facebook generally did not screen the third-party developers or their apps before granting them access to vast amounts of user data through Graph API V1.

119. For example, while Facebook used an automated tool to check that apps had an active link to a privacy policy, it did not actually review the app's privacy policy to confirm that it, in fact, complied with Facebook's policies.

120. Similarly, Facebook routinely granted third-party developers broad permissions to access user and Affected Friend data without first performing any checks on whether such permissions were consistent with a Facebook Platform policy requiring that apps request only data necessary to run the app or to enhance the user's app experience.

121. The Platform Policies outlined a number of privacy obligations and restrictions, such as limits on an app's use of data received through Facebook, requirements that an app obtain consent for certain data uses, and restrictions on selling or transferring user data. For example, third-party developers were specifically prohibited from transferring, directly or indirectly, any data—including aggregate, anonymous, or derivative data—to any ad network or data broker.

122. According to Facebook, these policies ensured that users' personal information was disclosed only to third-party developers who agreed to protect the information in a manner consistent with Facebook's privacy program.

123. To enforce its Platform Policies, Facebook relied on administering consequences for policy violations that came to its attention after third-party developers had already received the data. But Facebook did not consistently enforce its Platform Policies. Rather, the severity of consequences that Facebook administered to third-party developers for violating the company's Platform Policies, and the speed with which such measures were effectuated, took into account

the financial benefit that Facebook considered the developer to offer to Facebook, such as through a commercial partnership.

124. Facebook did not inform its third-party assessor that it was engaging in this practice, and the differential enforcement model was not noted in any of the company's Part V assessments.

125. As reported in the *Wall Street Journal*, Facebook's Vice President of Product Partnerships acknowledged that, for many years, the company's emphasis was on growth. It was only after March 2018, after Facebook had been giving third-party developers access to user data through the Graph API for years, that Facebook began a "massive cultural shift" to focus more on "enforcement as a key component" of its system.

126. The full scale of unauthorized collection, use, and disclosure of consumer information resulting from Facebook's conduct is unknown due, at least in part, to the company's lack of recordkeeping.

127. In March 2018, Facebook announced it had launched an internal investigation into the potential misuse of user data by third-party developers. But, due to various issues, including the company's own lack of an organized system or technical means for tracking all the massive troves of user data it released to third-party developers, Facebook could neither ascertain where most of the data went after it was pulled from the Platform, nor determine how the data had been used.

**Facebook Deceptively Used Covered Information Provided  
for Security Purposes for Advertisements**

128. Since May 2011, Facebook has allowed users to log into Facebook using two-factor authentication, originally called Login Approvals. When they logged in from a new or

unrecognized device, users of Login Approvals accessed their Facebook accounts with their username, password, and a code texted to their phone.

129. Until May 2018, to take advantage of this security feature, Facebook users had to add or confirm their phone numbers during the Login Approvals signup process. After May 2018, users could log in with two-factor authentication either by adding a phone number or by using a third-party authentication app, which generated a security code that Facebook could use to authenticate the user.

130. Facebook encouraged users to employ this security feature as an “industry best practice” for providing additional account security, and specifically touted Login Approvals as helping users take “more control over protecting their account from unauthorized access.”<sup>6</sup>

131. Facebook did not disclose, or did not disclose adequately, that the phone numbers Login Approvals users provided for two-factor authentication would also be used by Facebook to target advertisements to those users.

132. For example, from at least November 20, 2015, to March 25, 2018, during the signup process for Login Approvals, Facebook presented mobile App Users with a dialog box called “Set Up Login Code Delivery.”

133. At that dialog box, Facebook asked for users’ mobile phone numbers and told them, “For us to text you security codes, you need to add your mobile phone to your Timeline.”<sup>7</sup>

---

<sup>6</sup> <https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920/>; <https://www.facebook.com/notes/facebook-security/two-factor-authentication-for-facebook-now-easier-to-set-up/10155341377090766/>

<sup>7</sup> From April 25, 2017 until March 15, 2018, the text of the Set Up Login Code Delivery Box read, “For us to text you login codes, you need to add your mobile phone to your Timeline.”

Facebook then provided a space for users to add their phone numbers and prompted them to click the “Continue” button.

134. Facebook did not tell users anywhere in that dialog box, or anywhere on the path to that dialog box, that Facebook would also use phone numbers provided for two-factor authentication for advertising.

135. Similarly, from at least November 15, 2015, to February 23, 2018, during the Login Approval signup process on its mobile interface, Facebook asked for a user’s mobile phone number on a screen titled “Set Up Login Code Delivery.”

136. At that screen, Facebook told users, “For us to text you login codes, you need to add your mobile phone to your timeline.” Facebook then provided a space for users to add their phone numbers and click the “Continue” button.

137. There was no disclosure on the “Set Up Login Code Delivery” screen, or anywhere on the path to that screen, that Facebook would also use phone numbers provided for two-factor authentication for advertising.

138. Additionally, during the signup process for two-factor authentication on Facebook’s desktop website from April 26, 2018, to November 20, 2018, Facebook presented users with a dialog box titled “Add A New Phone Number.”

139. In that dialog box, Facebook asked for users’ mobile phone numbers and told them, “Add your mobile number to your account so you can reset your password if you ever need to, find friends, and more. You can later choose to turn SMS updates on for this number.”

140. There was no disclosure in that dialog box, or anywhere on the path to that dialog box, that Facebook would also use phone numbers provided for two-factor authentication for advertising.

141. When users were led to, or looked for, more information about adding a phone number for two-factor authentication, they were brought to a webpage that asked, “Why am I being asked to add my mobile phone number to my account?” This webpage stated:

Adding a mobile phone number to your account:

- Helps keep your account secure
- Makes it easier to connect with friends and family on Facebook
- Makes it easier to regain access to your account if you have trouble logging in

142. Facebook did not inform users that it would also use mobile phone numbers for advertising.

143. The fact that Facebook would use mobile phone numbers provided for two-factor authentication for advertising would be material to users when deciding whether to use two-factor authentication at all, and, after May 2018, whether to use a third-party authentication app to log in with two-factor authentication instead of giving Facebook their mobile phone numbers.

**Facebook’s April 2018 Data Policy Was Deceptive to Users Who Did Not Have Its New “Face Recognition” Setting**

144. In 2010, Facebook began offering users a “Tag Suggestions” feature that used facial-recognition technology to assist them in “tagging” Friends in photos or videos, or associating a photo or video to a particular Friend’s Facebook account.

145. Specifically, Facebook’s facial-recognition technology used, and still uses, an algorithm that analyzes pixels in a user’s profile picture and photos in which the user is tagged to create a unique facial-recognition template that Facebook employs to identify that user in photos

and videos uploaded by the user's Friends. Facebook then suggests the user's name rather than requiring the Friend to manually type the user's name.

146. Users could control this feature through a Tag Suggestions privacy setting ("Tag Suggestions Setting"). All users who signed up for a Facebook account originally had the Tag Suggestions Setting following the launch of the Tag Suggestions feature. The Tag Suggestions Setting default was set to "Friends," which enabled facial recognition. Users could opt out of facial recognition by changing the Tag Suggestions Setting to "No One." For any user who opted out of facial recognition, Facebook would not create a facial-recognition template, or it would delete an existing facial-recognition template, for that user.

147. In December 2017, Facebook introduced a new "Face Recognition" setting ("Face Recognition Setting") to replace the existing Tag Suggestions Setting. Like the Tag Suggestions Setting, the Face Recognition Setting controlled whether Facebook created and stored a facial-recognition template for a user. Thus, if a user turned off the Face Recognition Setting, Facebook would not create a facial-recognition template for the user, and it would delete any existing facial-recognition template.

148. When it introduced the Face Recognition Setting, Facebook began using its facial-recognition technology for three new features, in addition to tag suggestions: Photo Review, which notifies users that they may be in certain photos or videos that have been uploaded onto Facebook even if the user is not tagged in the photo or video; Automatic Alt Text, which helps screen readers with visual impairments identify who is in the photo or video; and Profile Photo Review, which helps Facebook identify potential account impersonation. These new features



were available only to users who had migrated to the Face Recognition Setting and whose setting was “On.”

149. Between January and April 2018, Facebook provided a notice to individual users before migrating them to the Face Recognition Setting (the “Facial Recognition Notice”). This notice appeared at the top of a user’s News Feed and informed users of the three new uses for facial recognition and whether the Face Recognition Setting for that user was “On” or “Off.” The initial setting for the new Face Recognition Setting was based on whether the user had facial recognition enabled under their most recent Tag Suggestions Setting. Facebook thereby imported the user’s previous privacy choice on facial recognition to the new Face Recognition Setting.

150. The Facial Recognition Notice contained a link for users to “Learn More” about Facebook’s facial-recognition technology and a link to the Settings page where users could turn the Face Recognition Setting on or off. If a user did not click either link, Facebook provided the Facial Recognition Notice to that user three separate times and then migrated the user to the new Face Recognition Setting and its new features.

151. This migration experience occurred only for users who had Facebook accounts as of April 2018 and who had received Facebook’s Facial Recognition Notice three times. Approximately 30 million Facebook users in the United States who had not received the Facial Recognition Notice three separate times were not migrated to the Face Recognition Setting. The migration also did not occur for approximately 30 million new users who signed up for Facebook after April 2018.

152. Accordingly, Facebook did not migrate these approximately 60 million users to the new Face Recognition Setting, and their accounts still featured only the Tag Suggestions Setting.

153. In April 2018, Facebook deleted from its Platform all prior references to “Tag Suggestions” and updated its Data Policy to reference only its new Face Recognition Setting. In relevant part, Facebook stated:

**Face recognition:** *If you have it turned on*, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create may constitute data with special protections under the laws of your country. Learn more about how we use face recognition technology, or control our use of this technology in Facebook Settings. If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.

(emphasis added).

154. Users who still had the Tag Suggestions Setting after April 2018, however, did not have to “turn[ ] on” facial recognition, because—unless the user had previously opted out—facial recognition was turned on by default. Thus, the updated Data Policy, which emphasized the need for users to “turn[ ] on” facial recognition, was not accurate for the approximately 60 million users who were not migrated to the Face Recognition Setting, as facial-recognition technology was turned on by default for those users. If those users did not want the technology, they—contrary to the updated Data Policy—had to turn it off.

## **VIOLATIONS OF THE COMMISSION ORDER**

### **Count 1—Misrepresenting the Extent to Which Users Could Control the Privacy of Their Data and the Extent to Which Facebook Made User Data Accessible to Third Parties**

155. Part I.B. of the Commission Order prohibits Facebook from misrepresenting “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.”

156. Part I.C. of the Commission Order prohibits Facebook from misrepresenting “the extent to which Respondent makes or has made covered information accessible to third parties.”

157. During the period from December 2012 through April 2014, Facebook represented to consumers that they could control the privacy of their data by using desktop and mobile privacy settings to limit the information Facebook could share with their Facebook Friends, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, and profile settings.

158. In fact, Facebook did not limit its sharing of consumer information with third-party developers based on those privacy settings.

159. Therefore, the representations described in Paragraph 157 violated Parts I.B. and I.C. of the Commission Order.

### **Count 2—Misrepresenting the Extent to Which Users Could Control the Privacy of Their Data and the Extent to Which Facebook Made User Data Accessible to Third Parties**

160. Part I.B. of the Commission Order prohibits Facebook from misrepresenting “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.”

161. Part I.C. of the Commission Order prohibits Facebook from misrepresenting “the extent to which Respondent makes or has made covered information accessible to third parties.”

162. At the April 30, 2014, F8 Conference, Facebook publicly announced that it would no longer allow third-party developers to access Affected Friend data.

163. In addition, Facebook continued to represent to consumers that they could control the privacy of their data by using Facebook’s desktop and mobile privacy settings to limit to their Facebook Friends the information Facebook could share, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, profile settings, and Privacy Checkup.

164. In fact, Facebook continued to allow millions of third-party developers access to Affected Friend data for at least another year.

165. Additionally, Facebook did not limit its sharing of consumer information with third-party developers based on Facebook’s desktop and mobile privacy settings, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, profile settings, and Privacy Checkup.

Therefore, the representations described in Paragraphs 162 and 163 violated Parts I.B. and I.C. of the Commission Order.

**Count 3—Misrepresenting the Extent to Which Facebook Made User Data Accessible to Third Parties**

166. Part I.B. of the Commission Order prohibits Facebook from misrepresenting “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.”

167. Part I.C. of the Commission Order prohibits Facebook from misrepresenting “the extent to which Respondent makes or has made covered information accessible to third parties.”

168. At the April 30, 2014, F8 Conference, Facebook announced that it would no longer allow third-party developers to access Affected Friend data.

169. On April 30, 2015, Facebook generally deprecated Graph API V1 so that it was no longer publicly available to third-party developers.

170. However, Facebook privately granted the Whitelisted Developers continued access to the capabilities of Graph API V1.

171. As a result, even after April 30, 2015, the Whitelisted Developers maintained access to the same Affected Friend data that Facebook had publicly announced in April 2014 was no longer available to third-party developers.

172. Some of the Whitelisted Developers retained access to Affected Friend data for months, while others retained access for years, with some retaining active access in 2018.

173. Additionally, from April 30, 2015, to at least June 2018, Facebook continued to represent to consumers that they could control the privacy of their data by using Facebook's desktop and mobile privacy settings to limit to their Facebook Friends the information Facebook could share, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, profile settings, and Privacy Checkup.

174. In fact, regardless of the privacy settings a user checked, Facebook continued to provide access to Covered Information to Whitelisted Developers throughout this period.

175. Therefore, the representations described in Paragraphs 168 and 173 violated the Commission Order.

**Count 4—Failure to Implement and Maintain a Reasonable Privacy Program**

176. Part IV of the Commission Order requires Facebook to implement and maintain a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services. Specifically, the program must contain controls and procedures appropriate to Facebook’s size and complexity, the nature and scope of its activities, and the sensitivity of Covered Information.

177. Among other things, Part IV requires that Facebook design and implement reasonable controls and procedures to address reasonably foreseeable, material risks that could result in the unauthorized collection, use, or disclosure of Covered Information. It also required Facebook to monitor and test the effectiveness of its controls and procedures, and to assess the sufficiency of any safeguards it implemented to control privacy risks.

178. In its initial and biennial assessment reports, Facebook claimed it had implemented controls and procedures to address the privacy risks created by third-party developers’ access to user data.

179. These controls did not include screening the third-party developers or their apps before granting them access to user data. Instead, Facebook relied on enforcing its Platform Policies.

180. Despite substantial reliance on its Platform Policies, however, Facebook did not consistently enforce those policies from 2012 to the present. Rather, the severity of consequences it administered to violators of the Platform Policies, and the speed with which it effectuated such measures, took into account the financial benefit the violator provided to Facebook.

181. Facebook did not inform its assessor that it was engaging in this practice.

182. Therefore, Facebook violated Part IV of the Commission Order.

**Count 5—Misrepresenting the Extent to Which Users Could Control  
the Privacy of Their Data**

183. Part I.B. of the Commission Order prohibits Facebook from misrepresenting “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.”

184. During the period from April 2018 through the present, Facebook represented, expressly or by implication, to its users that they would have to “turn[ ] on” facial-recognition technology.

185. In fact, during this period, for users who still had the Tag Suggestions Setting, Facebook’s facial-recognition technology was turned on by default unless the user opted out.

186. Therefore, the representations described in Paragraph 184 violated Part I.B. of the Commission Order.

**VIOLATION OF SECTION 5 OF THE FTC ACT**

**Count 6—Deceptive Practices Regarding Use of Covered Information Provided for  
Account Security**

187. As described above in Paragraphs 128-43, Facebook represented, directly or indirectly, expressly or by implication, that users’ phone numbers provided for two-factor authentication would be used for security purposes and, in some instances, to make it easier to connect with Friends on Facebook.

188. Facebook failed to disclose, or failed to disclose adequately, that Facebook would also use phone numbers provided by users for two-factor authentication for targeting advertisements to those users.

189. Facebook's failure to disclose or disclose adequately the material information described in Paragraph 188, in light of the representations set forth in Paragraph 187, is a deceptive act or practice.

190. The acts and practices of Facebook 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, 15 U.S.C. § 45(a).

#### **COURT'S POWER TO GRANT RELIEF**

191. Each representation Defendant has made in violation of the Commission Order constitutes a separate violation for which Plaintiff may seek a civil penalty pursuant to Section 5(l) of the FTC Act, 15 U.S.C. § 45(l).

192. Section 5(l) of the FTC Act, 15 U.S.C. § 45(l), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, and Section 1.98(c) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(c), directs that a defendant who violates an order of the Commission after it has become final, and while such order is in effect, "shall forfeit and pay to the United States a civil penalty of not more than \$42,530 for each violation."

193. Sections 5(l) and 13(b) of the FTC Act, 15 U.S.C. §§ 45(l) and 53(b), also authorize this Court to grant an "injunction and such other and further equitable relief" as it may deem appropriate in the enforcement of the Commission Order.



**PRAYER FOR RELIEF**

194. WHEREFORE, Plaintiff requests this Court, pursuant to 15 U.S.C. §§ 45(l) and 53(b), and pursuant to the Court's own equitable powers:

A. Enter judgment against Defendant and in favor of Plaintiff for violating the Commission Order and the FTC Act as alleged in this Complaint;

B. Award Plaintiff monetary civil penalties from Defendant for each violation of the Commission Order;

C. Enter an injunction to prevent future violations by Defendant of the Commission Order, or as it is subsequently modified by operation of law, and the FTC Act; and

D. Award Plaintiff the costs of bringing this action, as well as such other and further relief as the Court may determine to be just and proper.

DATED: July 24, 2019

**FOR THE UNITED STATES:**

JOSEPH H. HUNT  
Assistant Attorney General  
Civil Division

DAVID M. MORRELL  
Deputy Assistant Attorney General

GUSTAV W. EYLER (997162)  
Director  
Consumer Protection Branch

ANDREW E. CLARK  
Assistant Director

/s/ Lisa K. Hsiao

LISA K. HSIAO (444890)  
Senior Litigation Counsel  
PATRICK R. RUNKLE  
JASON LEE  
Trial Attorneys  
Consumer Protection Branch  
U.S. Department of Justice  
P.O. Box 386  
Washington, DC 20044-0386  
Telephone: (202) 616-0219  
Fax: (202) 514-8742  
Lisa.K.Hsiao@usdoj.gov  
Patrick.R.Runkle@usdoj.gov  
Jason.Lee3@usdoj.gov

*Of Counsel:*

JAMES A. KOHM (426342)  
Associate Director for Enforcement

LAURA KOSS (441848)  
Assistant Director for Enforcement

ROBIN L. MOORE (987108)  
REENAH L. KIM (478611)  
LINDA HOLLERAN KOPP (472355)  
Attorneys  
Federal Trade Commission  
600 Pennsylvania Avenue, NW,  
Mail Stop CC-9528  
Washington, DC 20580  
(202) 326-2167 (Moore), -2272 (Kim), -2267 (Kopp), -  
3197 (fax)  
rmoore1@ftc.gov; rkim1@ftc.gov; lkopp@ftc.gov

## **2012 FTC LEXIS 135**

Federal Trade Commission

July 27, 2012

DOCKET NO. C-4365

### **Reporter**

2012 FTC LEXIS 135 \*

## **In the Matter of FACEBOOK, INC., a corporation**

---

### **Subsequent History:**

Complaint issued by [\*In re Facebook, Inc., 2012 FTC LEXIS 136 \(F.T.C., July 27, 2012\)\*](#)

### **Prior History:**

[\*Facebook, Inc., 2011 FTC LEXIS 271 \(F.T.C., Dec. 2, 2011\)\*](#)

## **Core Terms**

---

privacy, user, third party, terminate, consumer, disclosure, entity, notice, disseminate, delete

## **Action**

---

[\*1]

DECISION AND ORDER

## **Order**

---

### **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 [\*2] 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:

1. Unless otherwise specified, "Respondent" shall mean Facebook, its **[\*3]** 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.
2. "Commerce" shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, [15 U.S.C. § 44](#).
3. "Clear(ly) and prominent(ly)" shall mean:
  - A. 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;
  - B. 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;
  - C. 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 **[\*4]** 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
  - D. 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.
4. "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.
5. "Nonpublic user information" shall mean covered information that is restricted by one or more privacy setting(s).
6. "Privacy setting" **[\*5]** 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.
7. "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.

8. "Third party" shall mean any individual or entity that uses or receives covered information obtained by or on 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, **[\*6]** prevent, or mitigate fraud or security vulnerabilities.

9. "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 **[\*7]** 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 **[\*8]** 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 [\*9] 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 [\*10] 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 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 [\*11] 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 [\*12] 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 [\*13] 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 [\*14] 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 [\*15] 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 [\*16] 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, 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](mailto: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 [\*17] 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, [\*18] 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.

July 27, 2012



## **2012 FTC LEXIS 136**

Federal Trade Commission

July 27, 2012; July 27, 2012, Complaint

DOCKET NO. C-4365

### **Reporter**

2012 FTC LEXIS 136 \*

## **In the Matter of FACEBOOK, INC., a corporation**

---

### **Subsequent History:**

Settled by [In re Facebook, Inc., 2012 FTC LEXIS 138 \(F.T.C., Aug. 10, 2012\)](#)

### **Prior History:**

[In re Facebook, Inc., 2012 FTC LEXIS 135 \(F.T.C., July 27, 2012\)](#)

## **Core Terms**

---

user, profile, privacy, platform, advertiser, verify, video, click, restrict access, third party, deactivate, commerce, harbor, delete, personal information, disseminate, display, website, picture, badge, website, facebook, uploaded, network, fail to disclose, birthday, depict, target, site, overridden

## **Action**

---

[\*1]

COMPLAINT

## **Complaint**

---

### **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](http://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 [\*2] 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:

- 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); [\*3]
  - iv. Looking for (*i.e.*, whether a user is looking for friendship, dating, a relationship, or networking);
  - v. Relationships (*e.g.*, marital or other relationship status and the names of family members);
  - vi. Political and Religious Views;
  - vii. Likes and Interests (*e.g.*, activities, interests, music, books, or movies that a user likes); and
  - viii. Education and Work (*e.g.*, the name of a user's high school, college, graduate school, and employer); and
- c. other information that is based on a user's activities on the site over time, such as:
  - i. a Friend List (*i.e.*, a list of users with whom a user has become "Friends" on the site);
  - ii. Pages (*e.g.*, any web page on Facebook's web site, belonging to an organization, brand, interest group, celebrity, or other entity, that a user has clicked an online button to "fan" or "like");
  - iii. Photos and Videos, including any that a user has uploaded or been "tagged in" (*i.e.*, identified by a user such that his or her name is displayed when a user "hovers" over the likeness); and
  - iv. messages that a user posts and comments made in response to other users' content.

7. Each user's profile [\*4] 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, **[\*5]** 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."

[SEE IMAGE IN ORIGINAL]

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."

[SEE IMAGE IN ORIGINAL]

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 **[\*6]** 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 **[\*7]** 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. **[\*8]** 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 **[\*9]** 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 **[\*10]** 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 **[\*11]** (e.g., Photos and Videos of Me, Birthday, Family and Relationships, etc.), and which stated:

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

and

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

(See Privacy Wizard screenshots, Exhibit C).

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

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

26. Facebook's designation of PAI caused harm to users, including, but not limited to [\*12], threats to their health and safety, and unauthorized revelation of their affiliations. Among other things:

- a. certain users were subject to the risk of unwelcome contacts from persons who may have been able to infer their locale, based on the locales of their Friends (e.g., their Friends' Current City information) and of the organizations reflected in their Pages;
- b. each user's Pages became visible to anyone who viewed the user's profile, thereby exposing potentially controversial political views or other sensitive information to third parties -- such as prospective employers, government organizations, or business competitors -- who sought to obtain personal information about the user;
- c. each user's Friend List became visible to anyone who viewed the user's profile, thereby exposing potentially sensitive affiliations, that could, in turn, reveal a user's political views, sexual orientation, or business relationships, to third parties -- such as prospective employers, government organizations, or business competitors -- who sought to obtain personal information about the user; and
- d. each user's Profile Photo became visible to anyone who viewed the user's [\*13] profile, thereby revealing potentially embarrassing or political images to third parties whose access users previously had restricted.

### **Count 2**

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

28. As described in Paragraph 24-26, Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them. Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks. These facts would be material to consumers. Therefore, Facebook's failure to adequately disclose these facts, in light of the representation made, constitutes a deceptive act or practice. [\*14]

### **Count 3**

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

## **SCOPE OF PLATFORM APPLICATIONS' ACCESS TO FACEBOOK USERS' INFORMATION**

### **(Count 4)**

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

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

Allowing [\*15] [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](http://www.facebook.com):

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

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

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

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

31. Contrary to the statements set forth in Paragraph 30, in many instances, a Platform Application could access profile information that was unrelated to the Application's purpose or unnecessary to its operation. For example, a Platform Application with a narrow purpose, such as a quiz regarding a television show, in many instances could access a user's Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook's web site, despite the lack of relevance of this information to [\*16] 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. [\*17] , 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 [\*18] 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 [\*19] don't share your information with advertisers unless you tell us to ([e.g.] to get a sample, hear more, or enter a contest). Any assertion to the contrary is false. Period . . . we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads.

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

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

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

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

37. Contrary to the [\*20] 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](http://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); [\*21] 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 [\*22] or her activities on any Platform Application web site where the advertiser displayed an ad.

#### **Count 5**

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

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

#### **FACEBOOK'S DECEPTIVE VERIFIED APPS PROGRAM**

##### **(Count 6)**

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

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

- a. a Verified Apps badge, the same or similar to the badge depicted below, for display on the application's profile page on [www.facebook.com](http://www.facebook.com); and  
[SEE IMAGE IN ORIGINAL]

- b. a green check mark alongside the Platform Application's name, and higher [\*23] ranking among search results, on [www.facebook.com](http://www.facebook.com) and within Facebook's Application Directory.

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

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

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



- b. the Verified Apps green check mark, described in Paragraph 44(b); and
- c. the following statements on its website:

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

(Press Release, "Facebook Expands Power of Platform Across the Web and Around the World," July 23, 2008, Exhibit [\*24] 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 [\*25] it collected, beyond such steps as it may have taken regarding any other Platform Application.

#### **Count 6**

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

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

#### **FACEBOOK'S DISCLOSURE OF USER PHOTOS AND VIDEOS**

##### **(Count 7)**

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

51. [\*26] 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 [\*27] will not be available to others;

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

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

(Facebook Help Center FAQ, Exhibit N);

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

(Facebook Help Center FAQ, Exhibit O); and

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

(Facebook Help Center FAQ, Exhibit P).

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

## **Count 7**

54. As set forth in Paragraph 52, Facebook has represented, [\*28] 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 [\*29] ("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. **[\*30]** 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. **[\*31]** 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 **[\*32]** 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.

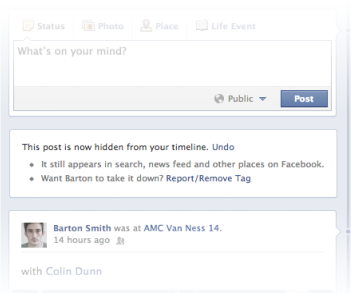
[Read more](#)

Everyone used to have a setting called “Who can look up my timeline by name,” which controlled if someone could be found when other people typed their name into the Facebook search bar. The setting was very limited in scope, and didn’t prevent people from finding others in many other ways across the site.

Because of the limited nature of the setting, we removed it for people who weren’t using it, and have built new, contextual tools, along with education about how to use them. In the coming weeks, we’ll be retiring this setting for the small percentage of people who still have it.

## 2. Understanding: In-product education

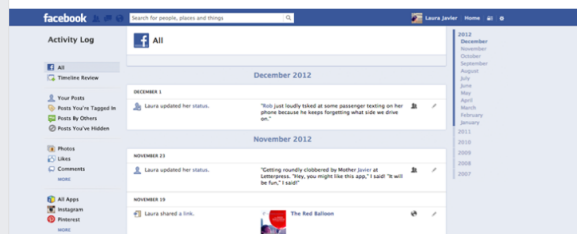
Along with the overall effort to continue bringing privacy controls up front, we’re adding in-context notices throughout Facebook. For example, we’ve created a series of messages to help you understand, in context, that the content you hide from your timeline may still appear in news feed, search and other places.



### Updated Activity Log

Last year we introduced Activity Log. Activity Log makes it easy to see the things you've posted on Facebook, make changes to the audience of past photos and other posts, and choose what appears on your timeline.

The updated Activity Log has new navigation, so you can easily review your own activity on Facebook, such as your likes and comments, photos of you, and posts you've been tagged in. It also has new ways to sort information, for example: Now you can quickly see public photos you're tagged in and have hidden from your timeline, but which still appear in other places on Facebook.



## 3. Action: New tools to manage your content New Request and Removal tool

Within the updated Activity Log, you now have a Request and Removal tool for taking action on multiple photos you're tagged in. If you spot things you don't want on Facebook, now it's even easier to ask the people who posted them to remove them.

Go to the “Photos of You” tab, select multiple photos, and ask friends to take down the shots you don't like – you can even include a message about why this is important to you. The tool also lets you untag multiple photos at once, keeping in mind that while untagged photos don't appear on your timeline, they can still appear in other places on Facebook, such as search, news feed, or your friends' timelines.



These updates and new tools will begin rolling out at the end of 2012.

[◀ Update to Messaging and a Test](#)

[Introducing Poke for Mobile ▶](#)

**Related News**

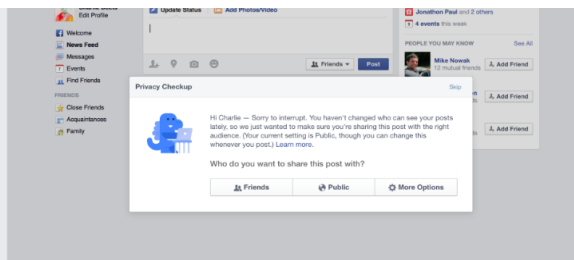
December 5, 2018

**[Response to Six4Three Documents](#)**

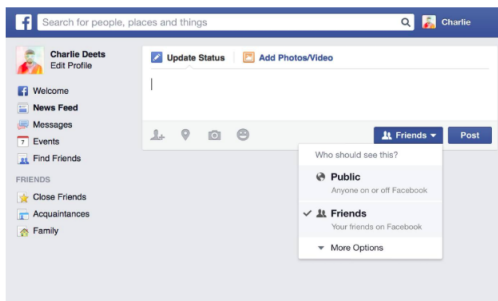
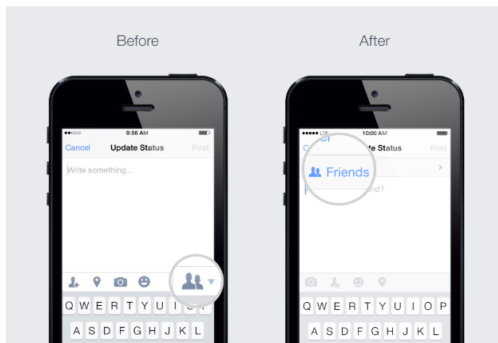
[About](#) [Contact Us](#) [Investor Relations](#) [Privacy](#) [Terms](#)  
Facebook © 2018  
Powered by WordPress.com VIP

Country: [United States \(English\)](#) ▼

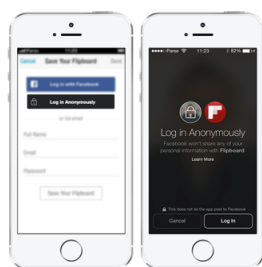




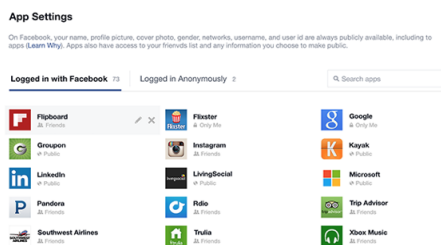
**Simplified Audience Selectors.** On Facebook for iPhone, the audience you're sharing a post with is now at the top of the screen, and on web, people will see a simplified audience selector. We're testing and rolling out similar improvements in other places people use Facebook.



**Anonymous Login and New Controls for Facebook Login.** Anonymous Login is a brand new way to log into apps without sharing any personal information from Facebook. The new Facebook Login gives people the option to pick and choose what information apps get.



**Redesigned App Control Panel.** A new dashboard where people can see a list of apps they use, manage specific permissions, or remove apps entirely.



For more information about choosing who you share with, visit the [Help Center](#).



◀ A New, Optional Way to Share  
and Discover Music, TV and  
Movies

Facebook Weekly Highlights ▶

**Related News**

December 13, 2018

**Facebook Watch: What We've Built  
& What's Ahead**

[About](#) [Contact Us](#) [Investor Relations](#) [Privacy](#) [Terms](#)  
Facebook © 2018  
Powered by WordPress.com VIP

Country: United States (English) ▼

Privacy Checkup Is Now Rolling Out


https://newsroom.fb.com/news/2014/09/privacy-checkup-is-now-rolling-out/

newsroom Like 495K Share Search in newsroom

Home News Company Info Inside Feed Directory Media Gallery Investor Relations

September 4, 2014

## Privacy Checkup Is Now Rolling Out

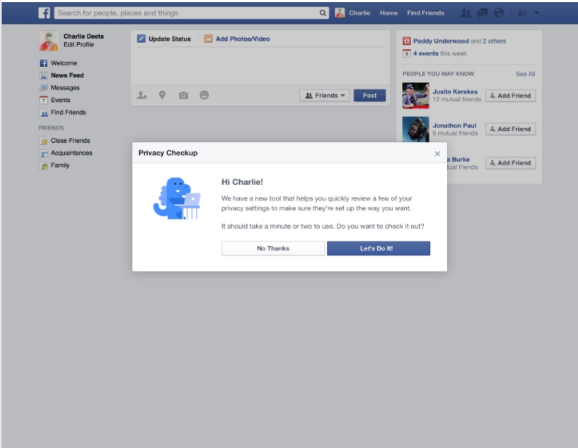


*By Paddy Underwood, Product Manager*

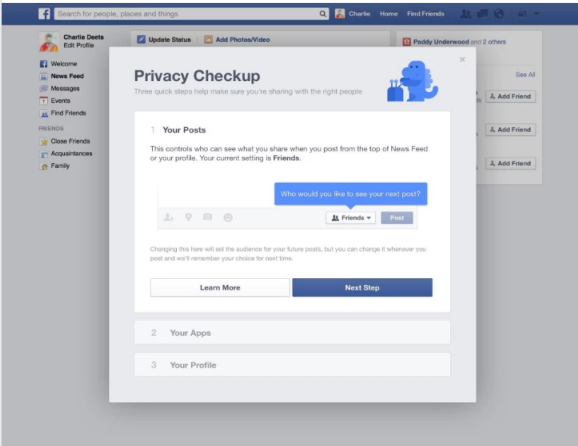
Today, we're starting to roll out Privacy Checkup, which helps you review and control who you're sharing with.

We know you come to Facebook to connect with friends, not with us. But we also know how important it is to be in control of what you share and who you share with.

You'll see the option to take Privacy Checkup when you visit Facebook in the coming days. Click "Let's Do It!" to do the Checkup; it should only take a minute or two.



The first step helps make sure you're sharing with the right people:



The second step shows which apps you've logged into with Facebook. You can edit who sees each app and any future posts it makes for you, or delete the apps you no longer use.

### Contact Us

press@fb.com


### Categories

- Company News
- Product News
- Hard Questions
- Inside Feed
- Community Boost

### Archive

- 2018
- 2017
- 2016
- 2015
- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006

### Featured News




#### Facebook's 2018 Year In Review

December 6, 2018

Today we are revealing our 2018 Year In Review, highlighting the top ways people around the world connected with...

[Read more](#)

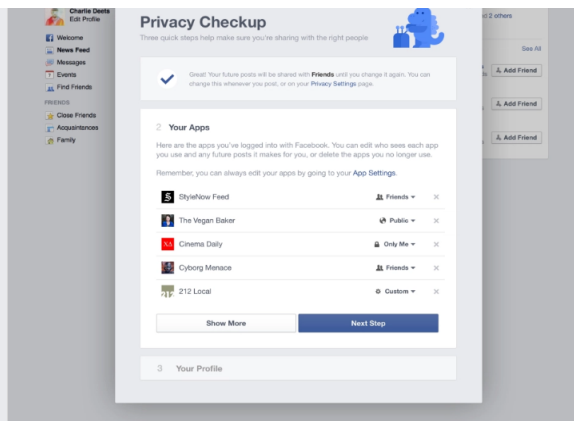


#### People Raise Over \$1 Billion for the Causes They Care About on Facebook

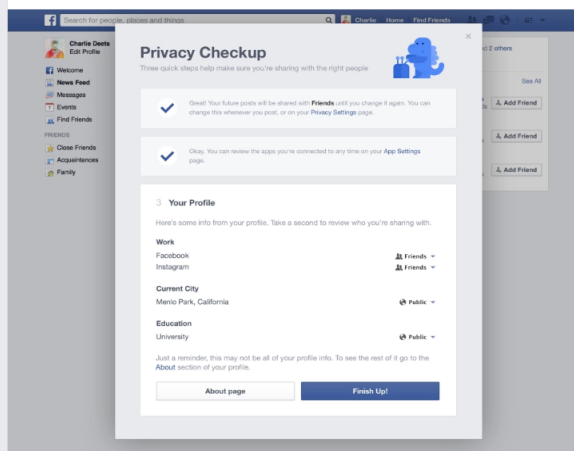
November 14, 2018

People have raised over \$1 billion on Facebook for nonprofit and personal causes, helping to raise awareness and make...

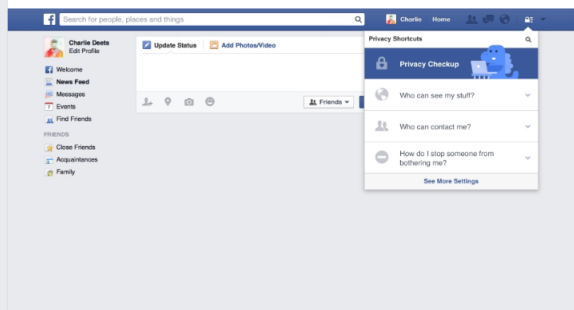
[Read more](#)



The final step helps you review and edit the privacy of key pieces of information on your profile:



You can also reach Privacy Checkup at any time by clicking Privacy Shortcuts:



#### Downloads:

Screenshots

Category: Product News

[Like 28](#) [Share](#) [Email](#)

[The 2014 Emmy Awards on Facebook](#)

[2014 NFL Season Kicks Off on Facebook](#)

#### Related News

December 5, 2018

[Response to Six4Three Documents](#)

## CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

**I. (a) PLAINTIFFS**

United States of America

(b) County of Residence of First Listed Plaintiff

(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Lisa K. Hsiao, Patrick R. Runkle, Jason Lee, Consumer Protection Branch  
USDOJ, PO Box 386, Washington DC 20044-0386

**DEFENDANTS**

Facebook, Inc.

County of Residence of First Listed Defendant San Mateo

(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

M. Sean Royall, Gibson, Dunn & Crutcher LLP  
1050 Connecticut Ave. NW, Washington DC 20036

**II. BASIS OF JURISDICTION** (Place an "X" in One Box Only)

- ☒ 1 U.S. Government Plaintiff
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question (U.S. Government Not a Party)
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

**III. CITIZENSHIP OF PRINCIPAL PARTIES** (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- |   | PTF                        | DEF                        |   | PTF                        | DEF                        |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State                   | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State     | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State                | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation  | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

**IV. NATURE OF SUIT** (Place an "X" in One Box Only)Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<b>PERSONAL INJURY</b> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <b>PERSONAL PROPERTY</b> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <b>PROPERTY RIGHTS</b> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <b>SOCIAL SECURITY</b> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<b>REAL PROPERTY</b> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<b>CIVIL RIGHTS</b> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<b>PRISONER PETITIONS</b> <b>Habeas Corpus:</b> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <b>Other:</b> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<b>FEDERAL TAX SUITS</b> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	
		<b>LABOR</b> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act		
		<b>IMMIGRATION</b> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions		

**V. ORIGIN** (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (specify)
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

15 U.S.C. Section 45

Brief description of cause:

Violations of FTC Consent Order and FTC Act

**VII. REQUESTED IN COMPLAINT:**

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

**DEMAND \$**

CHECK YES only if demanded in complaint:

**JURY DEMAND:** ☐ Yes ☒ No**VIII. RELATED CASE(S) IF ANY**

(See instructions):

JUDGE

DOCKET NUMBER

DATE

7/24/2019

SIGNATURE OF ATTORNEY OF RECORD

/s/ Lisa K. Hsiao

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE