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—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

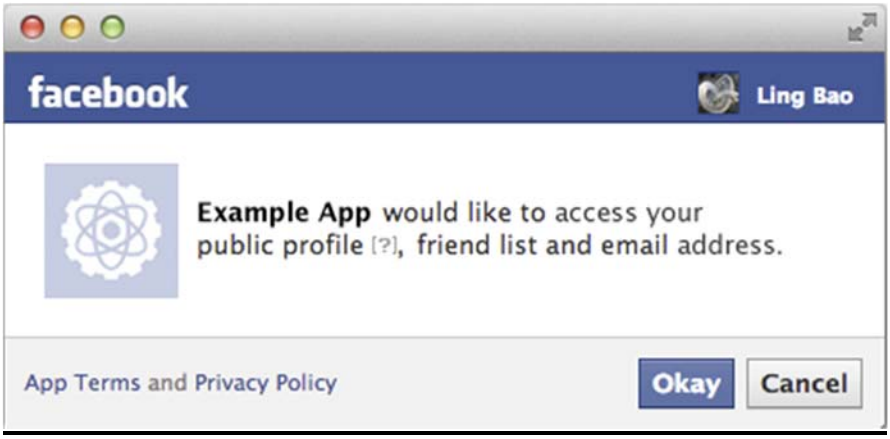
18. At all times material to this Complaint, Facebook maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

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:[1]



[1] 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

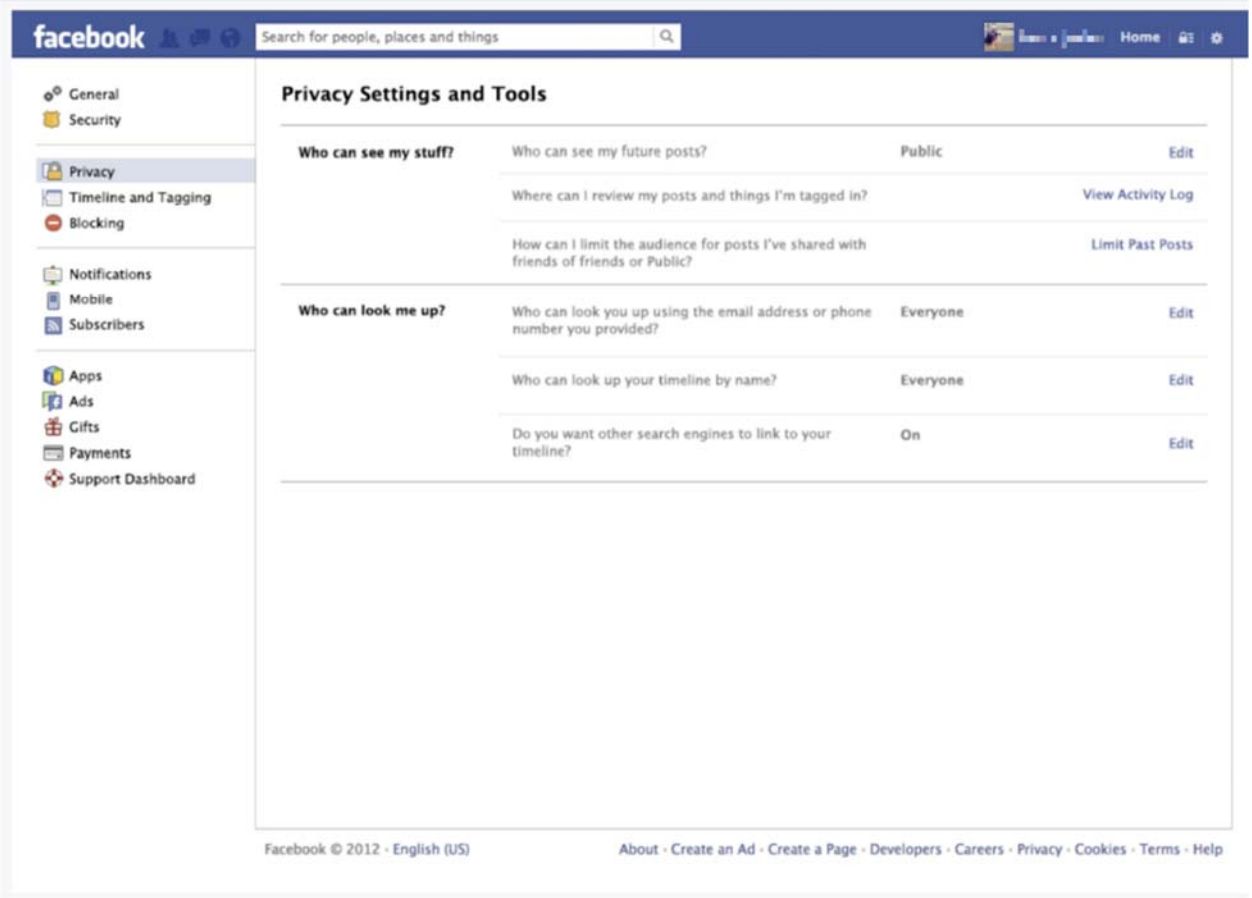
34. Facebook's General Counsel signed the Commission Order on behalf of Facebook. The Commission served the Commission Order in August 2012.

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.[2]

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."

[2] 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[3] 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.

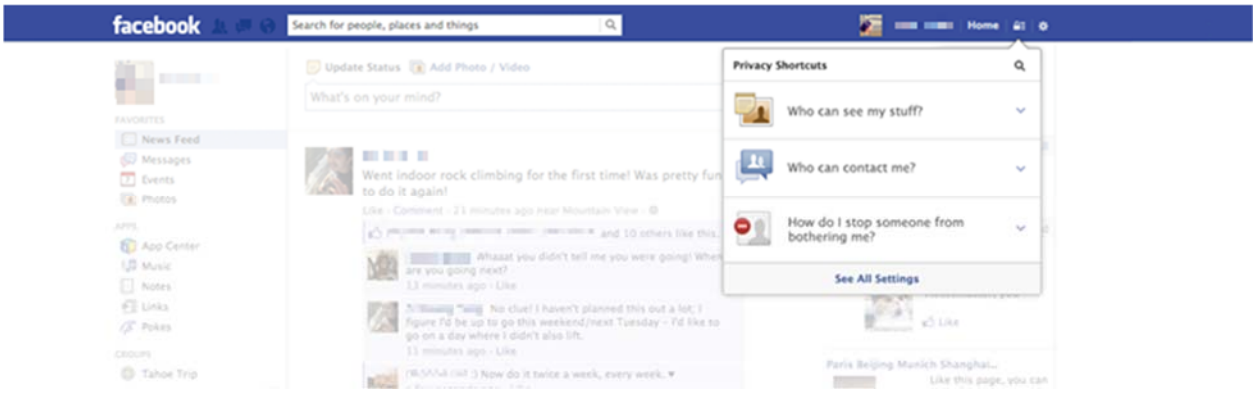
42. The Apps tab did not alert users that it linked to a page containing settings that users had to disable in order to have their privacy choices fully honored.

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:[4]

[3] "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."

[4] 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:[5]

[5] 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.

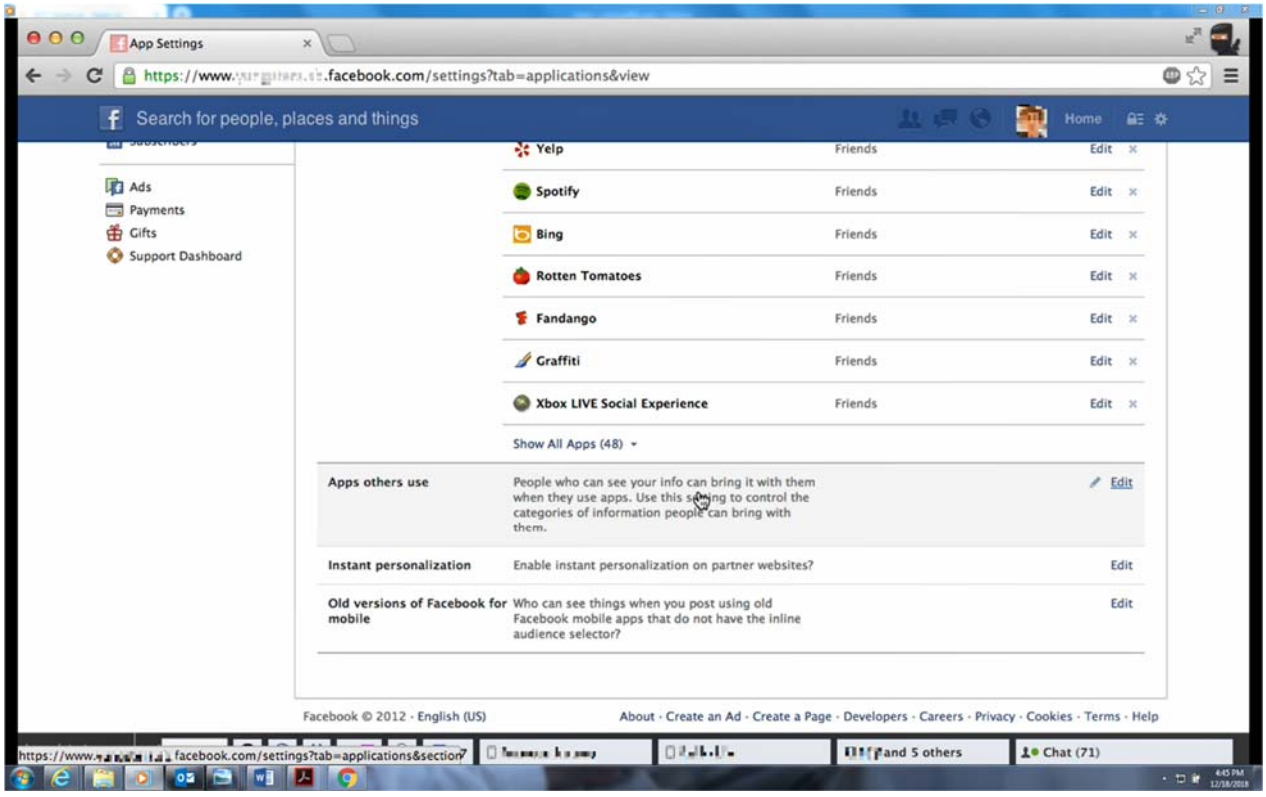
52. The Apps Settings page contained two opt-out settings—the "Apps others use" setting and the "Platform" setting.

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.

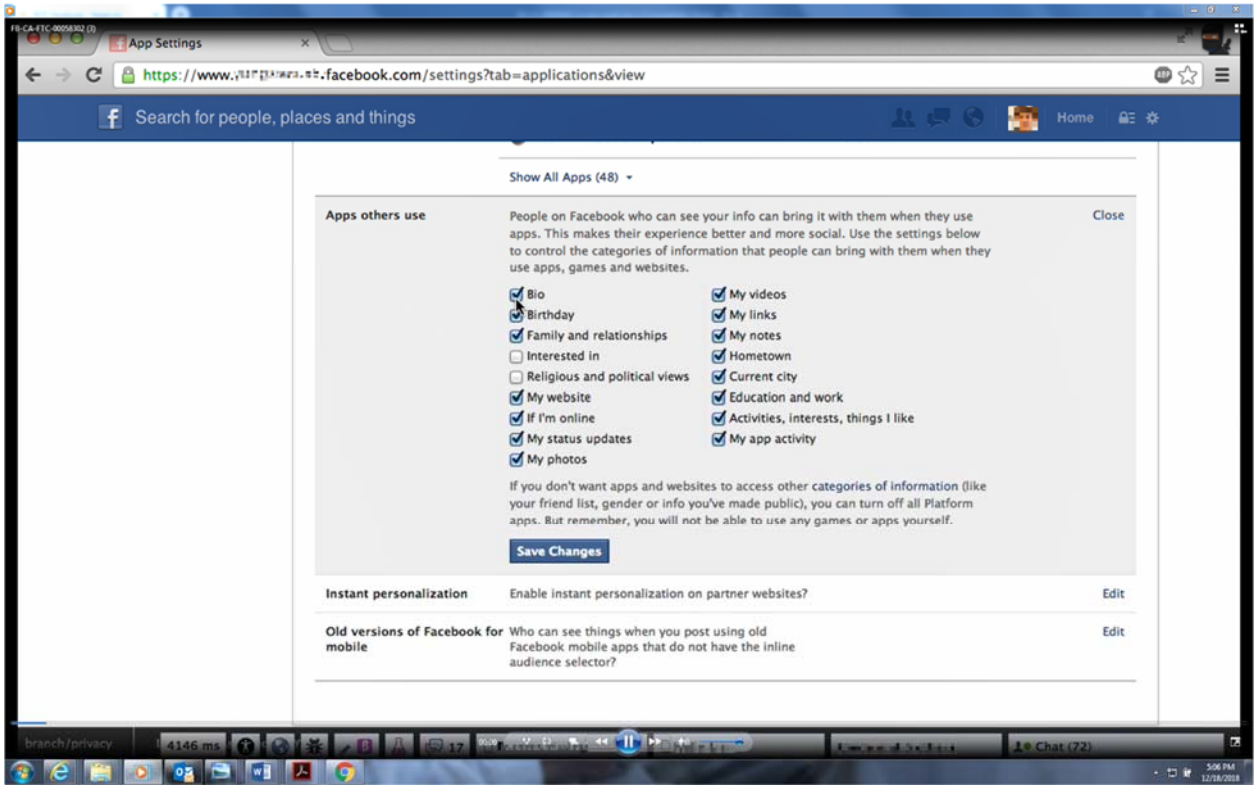
56. The format of the Apps Settings page varied over time. However, at all times relevant to this Complaint, the "Apps others use" setting at the bottom of the page, separate and apart from the privacy settings for the apps the user installed, as shown in the below example:



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:



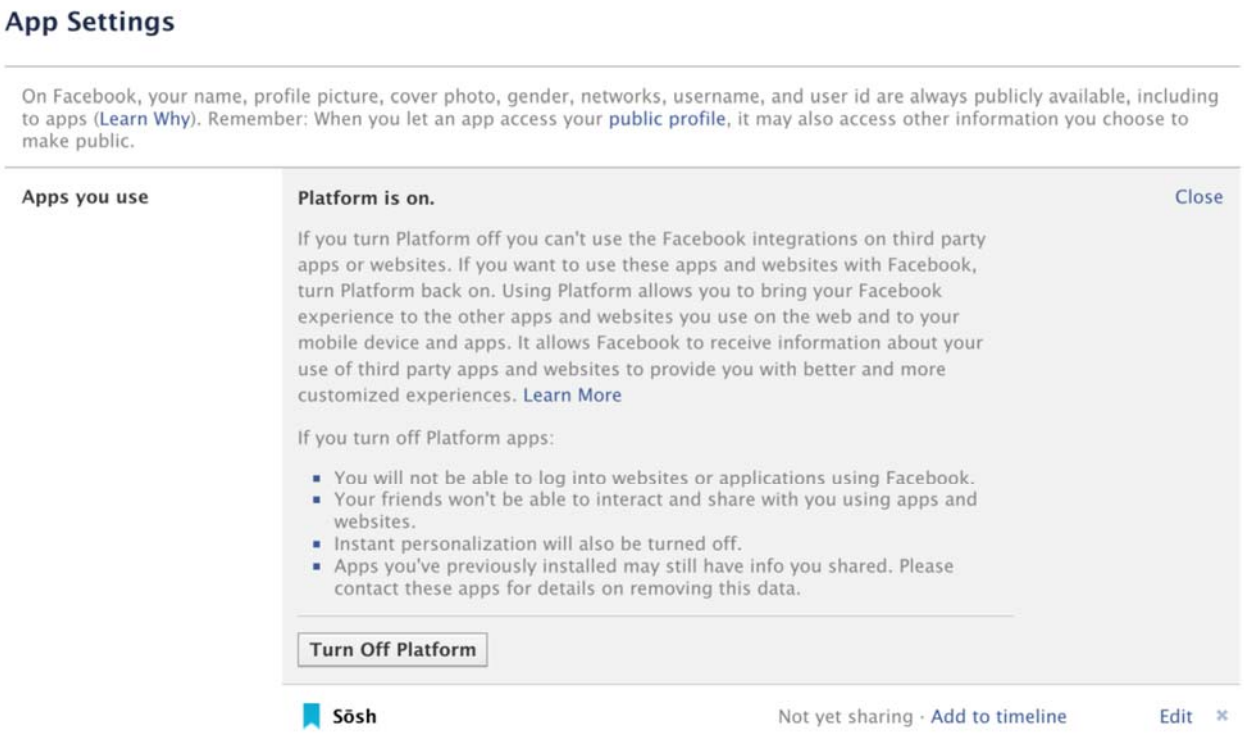
60. By default, all categories of Affected Friend data, except "Religious and political views" and "Interested in," were set to be shared with third-party developers who requested them.

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).



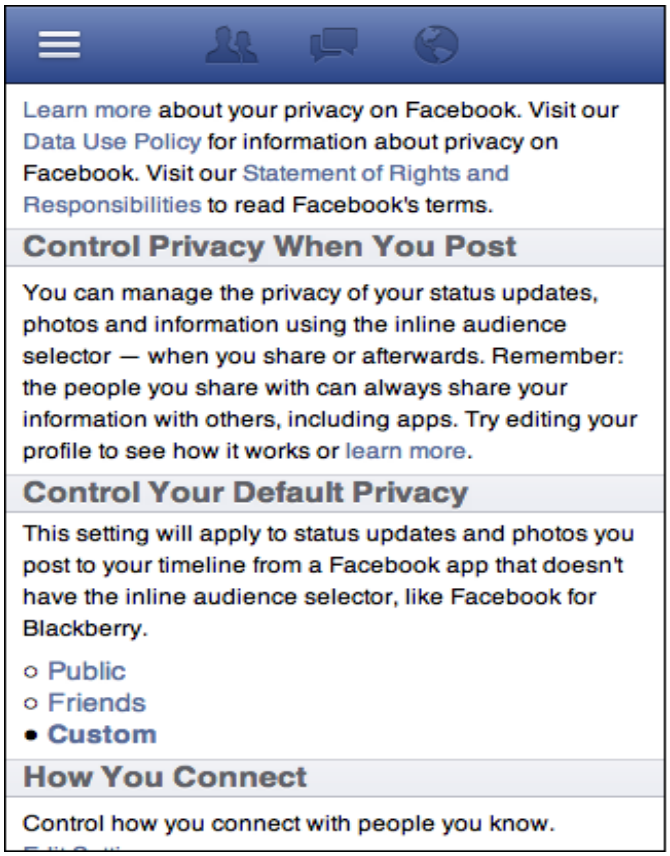
65. This language—which focused on information that would be shared with the user, rather than information Facebook would share about the user—did not inform users that: (a) by default, Facebook shared their Profile Information with third-party developers of Friends' apps; or (b) this setting allowed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



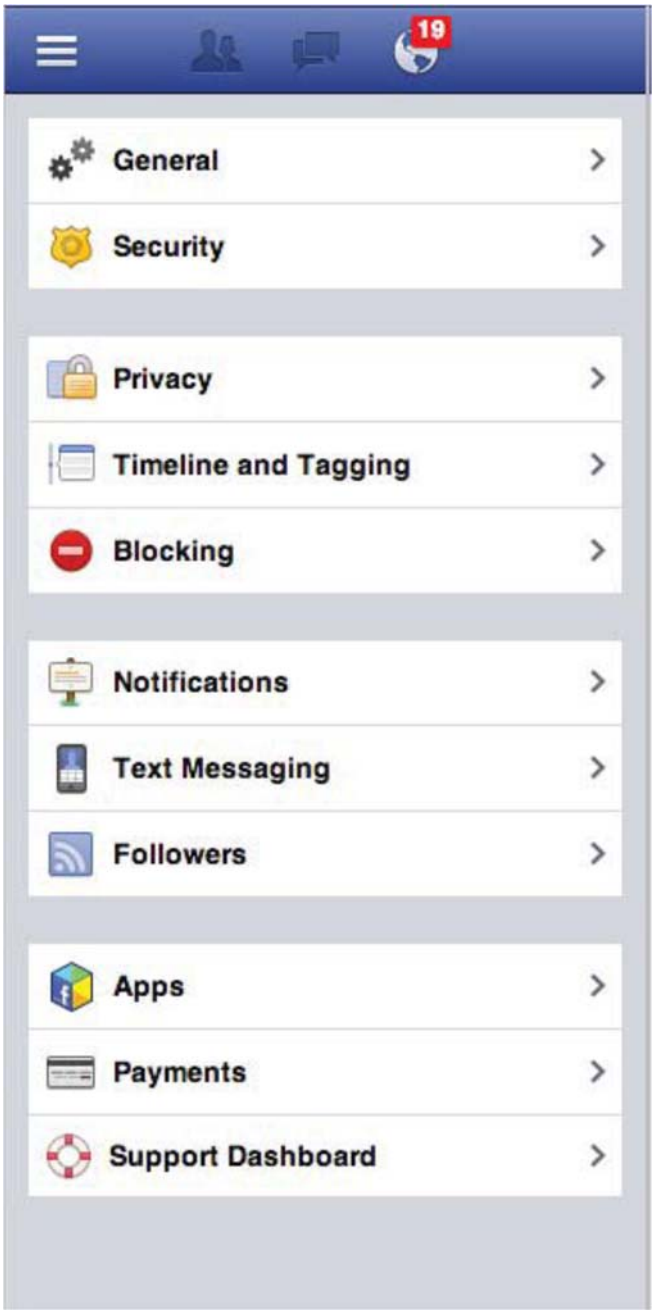
68. The mobile Privacy Settings page purported to allow users to restrict who could see their past and future posts, as well as, for approximately six months, users' birthday and contact information.

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.

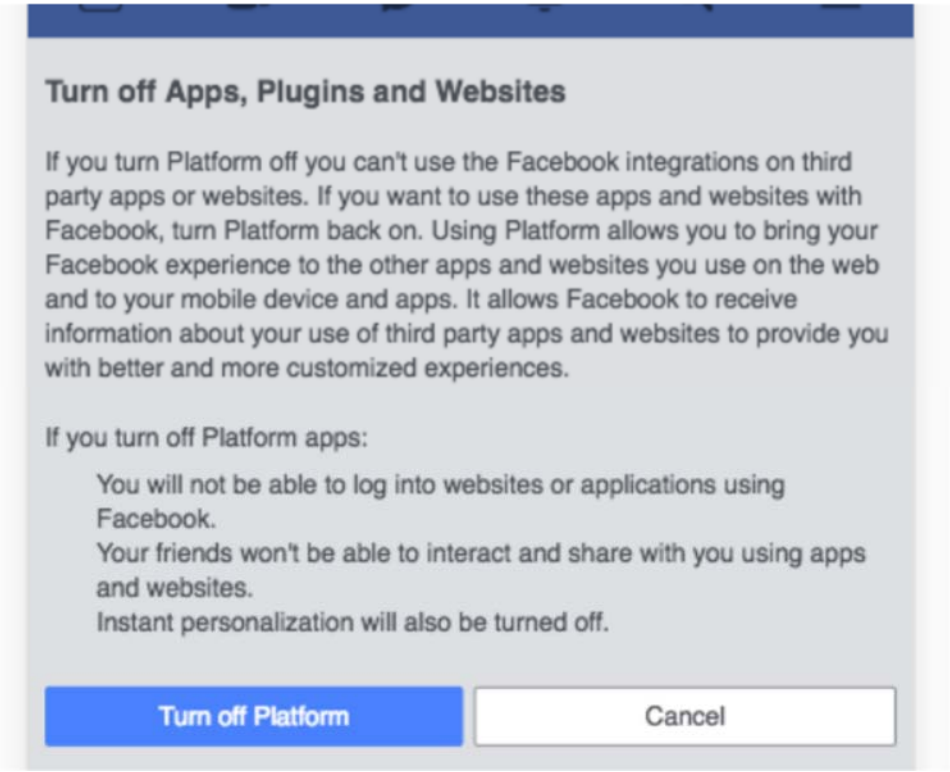
75. The "Apps others use" setting was located separate and apart from the privacy settings for the apps the user installed.

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.

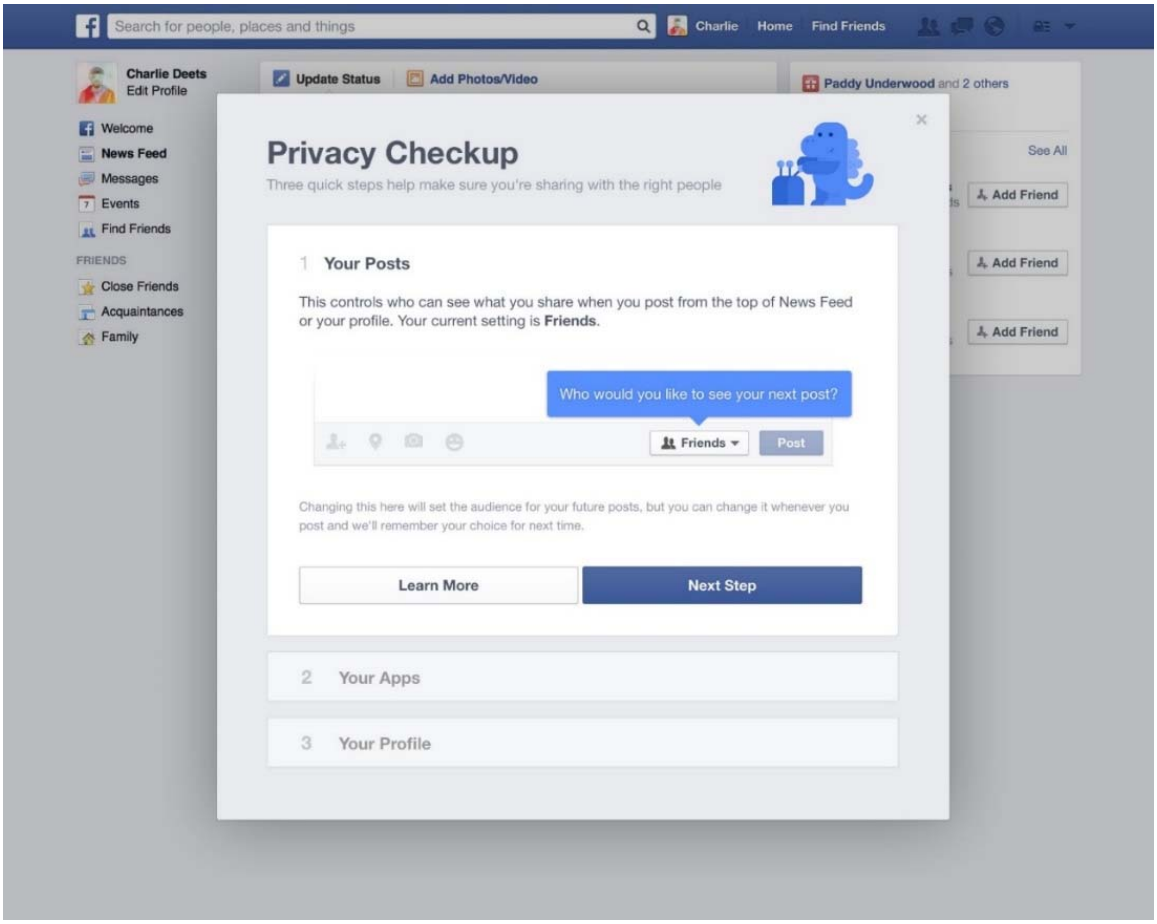
99. These communications with users addressed, among other things, the privacy controls that Facebook made available on its Platform.

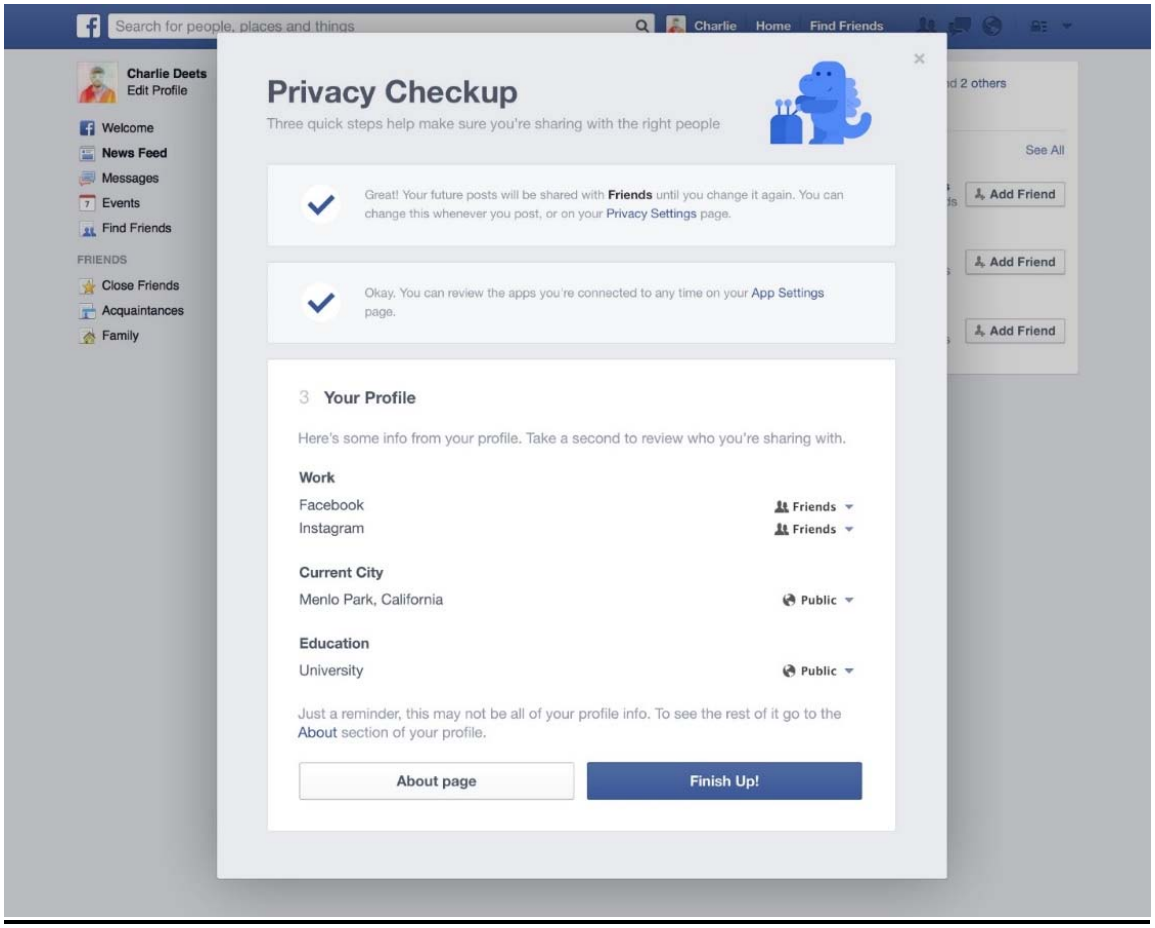
100. Despite these clear statements, Facebook gave third-party developers with a pre-existing, approved app at least one year of continued access to Affected Friends' data. In other words, third-party developers that had a preexisting app on the Facebook Platform as of April 2014 could still access and 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."[6]

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."[7]

---

[6] 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/

[7] 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