212 3091

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of **FACEBOOK, Inc.,** ***a corporation.*** **Respondent.**	**Docket No. C-4365** **REDACTED PUBLIC VERSION**

ORDER TO SHOW CAUSE WHY THE COMMISSION SHOULD NOT MODIFY THE ORDER AND ENTER THE PROPOSED NEW ORDER

The Federal Trade Commission ("Commission") "may at any time, after notice and opportunity for hearing, reopen and alter, modify, or set aside, in whole or in part any . . . order made or issued by it under this section." 15 U.S.C. § 45(b). The Commission may do so "whenever in the opinion of the Commission conditions of fact or of law have so changed as to require such action or if the public interest shall so require." *Id*. As discussed below, the facts establish good cause to believe the public interest and changed conditions of fact require modifications to the Commission's April 27, 2020 Order Modifying Prior Decision and Order. Accordingly, pursuant to Commission Rule of Practice 3.72(b), the Commission issues this Order to Show Cause Why the Commission Should Not Modify the Order and Enter the Proposed New Order. This Show Cause Order details the basis for modification and the changes it proposes to make in response.[1] *See* 16 C.F.R. § 3.72(b). Based on the record detailed below, the Commission finds good cause to enter the proposed order modifying the 2020 Order, as set forth in the attached Proposed Decision and Order. Respondent must file any Answer to this Order to Show Cause within thirty (30) days after service. In accordance with Commission Rule 3.72(b)(1), if Respondent should fail to respond within 30 days, Respondent may be deemed to have consented to the proposed order modifications. 16 C.F.R. § 3.72(b). If Respondent files an Answer, Commission Rule 3.72(b) sets forth the next steps whereby the Commission will first consider Respondent's Answer and then determine what process is appropriate to resolve any issues that arise from that Answer. Once it concludes that process, the Commission will determine whether to make the attached Proposed Decision and Order final or modify it in any way.

[1] The full record supporting the Commission's findings is contained in the attached Preliminary Finding of Facts ("PFF").

Procedural History

2012 Order

The Commission issued a 2012 Complaint against Respondent Facebook, Inc. ("Facebook" or the "Company") in Docket C-4365. The Complaint charged Facebook with unfair or deceptive acts or practices in violation of Section 5(a) of the Federal Trade Commission (FTC) Act, 15 U.S.C. § 45(a) ("Section 5"). Among other things, the Complaint alleged that Facebook promised users they could restrict the sharing of their non-public personal information to limited audiences, when in fact such limitations did not prevent Facebook from sharing the users' information with third-party developers. In addition, Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible, but Facebook continued allowing access to such content even after account deactivation or deletion. Facebook also changed its website, making certain information public that users previously may have designated private – without warning or first obtaining users' approval.

Facebook agreed to a consent order to settle the 2012 Complaint. *See* Decision and Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (July 27, 2012) ("2012 Order"). The 2012 Order barred Facebook from making misrepresentations about the privacy or security of consumers' information ("Covered Information") and required it to obtain users' affirmative express consent before sharing their information with third parties in a manner that materially exceeded their privacy settings. The Order also required Facebook to prevent anyone from accessing a user's information more than 30 days after the user had deleted their account. Finally, the Order required Facebook to establish and maintain a comprehensive privacy program and obtain independent third-party assessments of its program.

2020 Order

In 2019, acting upon the Commission's notification and authorization, the United States Department of Justice (DOJ) filed a Complaint in the United States District Court for the District of Columbia. The 2019 Complaint alleged Facebook violated the 2012 Order in three ways: (1) by misrepresenting the extent to which users could control the privacy of their data and the steps required to implement such controls; (2) by misrepresenting the information the Company made accessible to third parties; and (3) by failing to establish, implement, and maintain a privacy program reasonably designed to address privacy risks. Specifically, users relied on Facebook's deceptive settings and statements to restrict the sharing of their information, when in fact third-party developers could still access and collect their data. Moreover, Facebook took inadequate steps to address the risks posed by the third-party developers on its platform. Additionally, Facebook misrepresented users' ability to control the use of facial recognition technology. The 2019 Complaint also alleged Facebook violated Section 5 of the FTC Act when it told users it would collect their telephone numbers to enable a security feature, but did not disclose it also used those numbers for advertising.

To resolve the 2019 case, Facebook agreed to a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief on or about July 23, 2019. Pursuant to this agreement, Facebook consented to reopening the administrative proceedings at docket number C-4365, to modify the 2012 Order with a revised Decision and Order. *See* Stipulated Order for Civil Penalty,

Monetary Judgment, and Injunctive Relief, Part II, *United States v. Facebook, Inc.*, Case No. 19-cv-2184 (D.D.C. Apr. 23, 2020). Upon the District Court's approval and entry of the Stipulated Order, the Commission issued a modified administrative order that expanded and clarified the 2012 Order. *See* Order Modifying Prior Decision and Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (Apr. 27, 2020) ("2020 Order" or "Order"). Among other things, the 2020 Order expanded the privacy program and assessment provisions, mandating that Facebook conduct a "privacy review" of every new or modified product, service, or practice before implementation, and document its risk mitigation determinations. The Order also required the Company to exercise more rigorous oversight over third-party apps and take appropriate enforcement action against third-party developers who violate its platform terms and policies. It further required the Company to implement greater data security protections for user passwords and other Covered Information. Additionally, the Order imposes new restrictions on Facebook's use of facial recognition technology and telephone numbers obtained to enable a security feature. The Company also must report incidents involving the compromise of data for 500 or more users and document its efforts to address them.

Facts

Commission staff's investigation of Respondent's compliance with the 2020 Order showed the following:

Respondent

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

Since 2004, Respondent has operated a social networking service through its Facebook website (www.facebook.com) and mobile application that connects users with others on the platform. Respondent also owns and operates mobile messaging apps Messenger and WhatsApp, and offers photo and video sharing on the Instagram app. Additionally, Respondent offers third-party developers and businesses products and tools with which to integrate and use the Company's services. Among other things, Respondent uses consumers' information to serve targeted advertising both on and off the Facebook platform. Along with its advertising tools, Respondent also provides shopping and payment options for businesses and consumers. In addition, Respondent's offerings include hardware such as the Portal line of video-calling devices and augmented reality/virtual reality (AR/VR) headsets and accessories, as well as an associated app and app store through which third-party developers can offer games and apps that integrate with the AR/VR devices.

On October 29, 2021, Respondent notified the Commission it changed its name to Meta Platforms, Inc., and reported that Meta Platforms, Inc. would replace Facebook, Inc. as Respondent in the Commission's Orders.[2]

[2] PFF ¶ 1.

Independent Assessor's Findings Concerning Respondent's Privacy Program

Part VII of the 2020 Order requires Respondent to establish, implement, and maintain a comprehensive privacy program that "protects the privacy, confidentiality, and integrity of the Covered Information collected, used, or shared" by Respondent within 180 days of the Order (i.e., by October 24, 2020). The Order specifies detailed minimum requirements for the program and requires Respondent to obtain initial and biennial assessments of its privacy program from an independent third-party professional.

Specifically, Part VIII of the Order states, "in connection with compliance with Part VII of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ('Assessments') . . . from one or more qualified, objective, independent third-party professionals ('Assessor(s)') . . . who: (1) uses procedures and standards generally accepted in the profession; [and] (2) conducts an independent review of the Mandated Privacy Program."

Respondent selected and, together with DOJ, Commission staff approved Protiviti, Inc. as Respondent's Independent Assessor ("Assessor").[3]

On July 1, 2021, pursuant to Part VIII of the Order, Respondent submitted the Assessor's initial report for October 25, 2020 to April 22, 2021.

In this report, the Assessor found although "the key foundational elements necessary for an effective program are now in place, . . . their maturity and completeness vary from [redacted]" Thus, the Assessor concluded "the gaps and weaknesses noted within our review demonstrate that substantial additional work is required, and additional investments must be made, in order for the program to mature [redacted]"[4]

Through its testing and analysis, the Assessor identified [redacted] individual gaps and weaknesses [redacted] into which Respondent's privacy program is organized, as outlined below.[5] While these issues varied in significance, the Commission staff's investigation showed the most serious deficiencies and sheer number of total gaps and weaknesses overall present substantial risks to the public.

Privacy Risk Assessment

Respondent created its Risk Assessments and Remediation control domain to address the Order's requirement that it conduct privacy "risk assessments."[6] Specifically, Part VII.D requires Respondent to "assess and document" risks to the privacy, confidentiality, or integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of such information. Respondent must conduct company-wide risk assessments annually, and

[3] PFF ¶¶ 4-5.

[4] PFF ¶¶ 19-21

[5] PFF ¶¶ 22, 30-1068.

[6] PFF ¶¶ 30-31

assessments for risks related to Covered Incidents within 30 days of such incidents. Part VII.E then requires that Respondent develop safeguards to control for the risks it identifies.

Respondent performed a company-wide risk assessment ("PRA 1.0") [redacted][7]

The Assessor identified multiple deficiencies in Respondent's [redacted]. Those deficiencies included: [redacted][8]

Privacy Review

[redacted] Privacy Review control domain [redacted][9]

While the Assessor found Respondent [redacted].[10] [redacted][11]

[redacted] Specifically, at his

[7] PFF ¶¶ 32-85.

[8] PFF ¶¶ 86-170.

[9] PFF ¶¶ 171-182.

[10] PFF ¶¶ 183-184.

[11] PFF ¶¶ 185-357.

February 2022 deposition, Chief Executive Officer Mark Zuckerberg [redacted] Zuckerberg explained: [redacted][12]

Third-Party Risk Management

[redacted] Third-Party Risk Management control domain. The Order directs Respondent to consider the risks posed by its data-sharing arrangements with these third parties, and to develop appropriate safeguards to control for such risks. With respect to Covered Third Parties who access Covered Information for use in an independent third-party consumer application or website, the Order also specifies the types of compliance-monitoring measures Respondent must undertake and requires Respondent to enforce its policies against third parties who fail to comply with its terms governing the appropriate use and protection of Covered Information.[13]

The Assessor identified [redacted] gaps and weaknesses across the [redacted] in Respondent's [redacted] The Assessor concluded [redacted][14] These problems are particularly significant because they involve the same areas that precipitated the Commission's previous action.

Incident Management

As part of its Incident Management control domain, Respondent [redacted]

[12] PFF ¶¶ 358-370.

[13] PFF ¶¶ 371-391.

[14] PFF ¶¶ 392-571.

[redacted].[15]

The Assessor found [redacted]. During testing, however, the Assessor discovered that [redacted].[16] The Assessor identified [redacted].[17]

Data Life Cycle Management

[redacted] To that end, Respondent organized a central team to oversee its data management programs and verify its compliance with pertinent Order provisions. [redacted] First, the Order requires Respondent to ensure Covered Third Parties cannot access Covered Information from servers under Respondent's control beyond a reasonable period (not to exceed 30 days) after a user has deleted such information or terminated their account. Second, the Order requires Respondent to implement procedures designed to ensure it deletes user-provided Covered Information from servers under its control, or de-identifies the information so it is no longer associated with the user's account or device. Respondent must complete this process within a reasonable period (not to exceed 120 days) from the time the user deletes such information or their account.[18]

The Assessor identified gaps and weaknesses in [redacted]. Specifically, the Assessor observed [redacted]. The Assessor's key findings in this area concern [redacted].

[15] PFF ¶¶ 572-574, 577.

[16] PFF ¶¶ 575-576, 578-581.

[17] PFF ¶¶ 581-596.

[18] PFF ¶¶ 697-617.

Additionally, the Assessor identified deficiencies [redacted][19]

Security for Privacy

Respondent's Security for Privacy control domain [redacted][20]

[redacted].[21]

Employee Training

To satisfy the Order's training requirement, [redacted][22]

The Assessor identified [redacted][23]

Transparency, Notice, and Choice

[redacted].[24]

The Assessor identified gaps and weaknesses [redacted] First, the Assessor found, [redacted]

[19] PFF ¶¶ 618-705.

[20] PFF ¶¶ 706-725.

[21] PFF ¶¶ 7296-756.

[22] PFF ¶¶ 757-759.

[23] PFF ¶¶ 760-797.

[24] PFF ¶¶ 868.

[redacted] Second, [redacted] [25] In addition, the Assessor identified gaps and weaknesse [redacted] [26]

Compliance Reporting

Respondent established its Compliance Monitoring, Enforcement, and Reporting control domain to manage its privacy program compliance generally. [redacted] [27]

[redacted] Specifically, Part VII.E.2.c of the 2020 Order requires Respondent to prepare a Quarterly Privacy Review Report (QPRR) for the Principal Executive Officer. [redacted] In addition, the Assessor observed [redacted] [28]

Internal Policies and Procedures

To satisfy the Order's documentation requirements, Respondent [redacted] [29]

The Assessor identified [redacted]. First, [redacted], the Assessor found [redacted]. Second, the Assessor found [redacted] [30]

Other Issues

Additionally, the Assessor [redacted] For instance, the Assessor found [redacted]

[25] PFF ¶¶ 869-885.

[26] PFF ¶¶ 885-898.

[27] PFF ¶¶ 899-908.

[28] PFF ¶¶ 909-950.

[29] PFF ¶¶ 951-959.

[30] PFF ¶¶ 960-980.

[redacted][31]

The Assessor also found [redacted][32]

Respondent's Misrepresentations

Part I of the 2020 Order states, in relevant part, that Respondent, "in connection with any product or service, shall not misrepresent in any manner, expressly or by implication, the extent to which Respondent maintains the privacy or security of Covered Information, including, but not limited to . . . The extent to which Respondent makes or has made Covered Information accessible to third parties." 2020 Order, Part I.C.

Part I of the 2012 Order (which remained in effect until April 27, 2020) states, in relevant part, 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: . . . the extent to which Respondent makes or has made covered information accessible to third parties." 2012 Order, Part I.C.

90-Day Limitation Feature

From 2018 through June 2020, Respondent misrepresented the extent to which third-party developers could receive non-public information.

Specifically, on or about April 11, 2018, Respondent announced it would remove app developers' access to a user's data if that user had not used the app in the prior 90 days (the "90-Day Limitation"). Respondent represented these "Expired Apps" would be permitted to retain data they had obtained while the user was still active but would be unable to continue obtaining the user's nonpublic information.[33]

Respondent conveyed the change to users through representations in several places: the Apps and Websites setting; the Help Center; and the Data Policy.[34]

[31] PFF ¶¶ 981-1030.

[32] PFF ¶¶ 1031-1068.

[33] PFF ¶¶ 1071-1079.

[34] PFF ¶¶ 1080-1094.

Yet Respondent, in some instances, continued to share users' nonpublic information with Expired Apps. Moreover, this sharing had been occurring since Respondent launched the feature in April 2018.[35]

Messenger Kids Product

From December 2017 to July 2019, Respondent made misrepresentations relating to its Messenger Kids ("MK") product, a free messaging and video calling application specifically intended for users under the age of 13.[36]

Beginning in December 2017 and throughout its operation, Respondent represented that MK users could communicate in MK with only parent-approved contacts. However, coding errors allowed children to participate in group text chats and group video calls with unapproved contacts under certain circumstances.[37]

Specifically, from June 2018 to July 2, 2019, when MK users initiated a group text chat on Android devices by simultaneously selecting multiple contacts to participate in the chat, the app failed to check whether secondary contacts were approved to chat with each other. This coding gap allowed certain MK users to communicate with unapproved contacts in group text chats.[38]

Separately, beginning in November 2018, a coding error allowed Messenger users to add other individuals to ongoing video calls with MK users through a feature called escalation. Technical safeguards implemented to prevent MK users from communicating with unapproved contacts failed to work with Respondent's escalation feature on Messenger, again permitting MK users to communicate with unapproved contacts on group video calls. Respondent did not fix this problem until January 2019. Similarly, in May 2019, yet another coding issue allowed certain Messenger users to add individuals to ongoing video calls with MK users. Respondent failed to correct this problem until July 2019.[39]

Conclusions

The Commission has jurisdiction over Respondent's acts and practices.

Respondent is engaged in acts and practices that have been and are affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

Respondent was subject to the Commission's 2012 Order until its modification on April 27, 2020, and has been subject to the Commission's 2020 Order since.

Based on the facts summarized above, and cited specifically in the attached Preliminary

[35] PFF ¶¶ 1095-1122.

[36] PFF ¶¶ 1139-1151.

[37] PFF ¶¶ 1152-1166.

[38] PFF ¶¶ 1152-1156.

[39] PFF ¶¶ 1157-1166.

Finding of Facts, the Commission has reason to believe Respondent failed to establish and implement an effective privacy program as mandated by Part VII of the 2020 Order.

In addition, the Commission has reason to believe Respondent misrepresented the extent to which Expired Apps could continue to receive users' nonpublic information. Respondent's misrepresentations regarding its 90-Day Limitation feature violated Section 5 of the FTC Act, Part I of the 2012 Order for the period prior to April 27, 2020, and Part I of the 2020 Order thereafter.

The Commission also has reason to believe Respondent's Messenger Kids product allowed children to communicate with contacts who were not approved by their parents, in contravention of Respondent's representations and notice to parents. Respondent's misrepresentations regarding Messenger Kids violated Part I of the 2012 Order, Section 5 of the FTC Act, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6502, and the Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. Part 312.

Based on the foregoing, the Commission has good cause to believe the public interest and changed conditions require it to reopen the proceeding in Docket No. C-4365 pursuant to Section 3.72(b) of the Commission's Rules of Practice, 16 C.F.R. § 3.72(b), and modify the 2020 Order. *See* 15 U.S.C. § 45(b) and 16 C.F.R. § 3.72(b).

Based on the foregoing, the Commission has good cause to believe Respondent violated the Commission's Orders, Section 5, COPPA, and the COPPA Rule, and will likely continue to commit privacy violations in the future absent further enforcement action by the Commission. Respondent's non-compliance constitutes changed conditions demonstrating that additional modifications to the Order are needed to clarify and strengthen its requirements, and thus provide enhanced protections for consumers. Therefore, given these circumstances, the Commission proposes modifying the Order as follows, to better achieve its objectives.

Proposed Order Modifications

Based on the record detailed above, the Commission finds good cause to enter the proposed order modifying the 2020 Order, as set forth in the attached Proposed Decision and Order. These modifications include the following changes, which strengthen and enhance the Order's protections:

- Use of Teens' and Children's Information. A new provision imposes strict limitations on Respondent's ability to use information it collects from children and teens (i.e., users under the age of 18). Under this provision, Respondent would be permitted to collect and use minors' information only to provide the service (e.g., to maintain the teen's Instagram feed) and for security purposes (e.g., to detect potentially fraudulent accounts). Under no circumstance would the Company be able to monetize that information or use it for its own commercial gain – whether for advertising, enriching its own data models and algorithms, or providing other benefits to the Company – even after the minor turns 18.

- Pause on New Products and Features. A new provision prohibits Respondent from releasing any new or modified product, service, or feature until it can demonstrate –

through written confirmation from the qualified, independent third-party assessor – that its privacy program fully complies with the Order and has no material gaps or weaknesses.

- Other Modifications.
    - Extend existing protections to Respondent's future uses of facial recognition templates;
    - Broaden the protections that require Respondent to provide conspicuous notice and obtain the user's affirmative express consent for changes in its data practices;
    - Expand Respondent's mandatory reporting obligations expressly to include its own violations of its commitments;
    - Safeguard the information held by businesses that Respondent acquires; and
    - Strengthen existing privacy program provisions relating to privacy risk assessments and safeguard adjustments; Privacy Review; third-party monitoring; data inventory and access controls, and employee training.

* * * * *

Accordingly, **IT IS ORDERED** that Respondent must file its answer to this Order to Show Cause within thirty (30) days after service.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: May 3, 2023