UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

ORDER MODIFYING PRIOR DECISION AND ORDER

The Federal Trade Commission ("Commission") issued a Decision and Order against Facebook, Inc. ("Facebook) in Docket C-4365 on July 27, 2012 ("2012 order").[1] On July 24, 2019, the United States of America, acting upon notification and authorization to the Attorney General by the Commission, filed a complaint ("2019 complaint") in federal district court alleging that 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 they needed to take to implement such controls; (2) misrepresenting the information the Company made accessible to third parties; and (3) failing to establish, implement, and maintain a privacy program reasonably designed to address privacy risks. The complaint also alleged that Facebook violated Section 5 of the FTC Act by misrepresenting how it would use telephone numbers that users provided to enable a security feature.

On April 23, 2020, Judge Timothy J. Kelly in the District for the District of Columbia entered a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief ("Stipulated Order") resolving the 2019 complaint. In Section II of the Stipulated Order, Facebook consented to: (1) reopening the 2012 proceeding in FTC Docket NO. C-4365; (2) waiving its rights under the show cause procedures set forth in Section 3.72(b) of the Commission's Rules of Practice, 16 C.F.R. § 3.72(b); and (3) modifying the 2012 Order with the new Decision and Order set forth below.

In view of the foregoing, the Commission has determined that it is in the public interest to reopen the proceeding in Docket No. C-4365 pursuant to Commission Rule 3.72(b), 16 C.F.R. § 3.72(b), and to issue a new order as set forth below. Accordingly,

IT IS ORDERED that this matter be, and it hereby is, reopened; and

IT IS FURTHER ORDERED that, Facebook having consented to modifying the 2012 order as set forth below, the Commission hereby modifies the 2012 order with the attached Decision and Order.

By the Commission, Commissioners Chopra and Slaughter dissenting.

SEAL
ISSUED: April 27, 2020

April J. Tabor
Acting Secretary

[1] *In the Matter of Facebook*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012).

ATTACHMENT A

[182 3109]

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

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

DECISION AND ORDER

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a)(1) and (*l*), 53(b), and 56(a)(1).

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Decision and Order the Commission previously issued in the matter *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Parts I and IV of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).

3. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.

4. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

5. Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. "**Affected Facial Recognition User**" means any User who has a "Tag Suggestions" setting as of the effective date of this Order, and any User who signs up for Respondent's service after the effective date of this Order and has received the "Tag Suggestions" setting.

B. "**Clear(ly) and Conspicuous(ly)**" means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a video or television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable

members of that group.

C. "**Covered Incident**" means any instance in which Respondent has verified or otherwise confirmed that the Covered Information of 500 or more Users was or was likely to have been accessed, collected, used, or shared by a Covered Third Party in violation of Respondent's Platform Terms.

D. "**Covered Information**" means information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) geolocation information sufficient to identify a 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 that can be used to recognize a User over time and across different devices, websites or online services; (g) a Social Security number; (h) a driver's license or other government issued identification number; (i) financial account number; (j) credit or debit information; (k) date of birth; (l) biometric information; (m) any information combined with any of (a) through (l) above; or (n) Nonpublic User Information.

E. "**Covered Third Party**" means any individual or entity that uses or receives Covered Information obtained by or on behalf of Respondent outside of a User-initiated transfer of Covered Information as part of a data portability protocol or standard, other than: (1) a service provider of Respondent that (i) uses the Covered Information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the Covered Information, or any individually identifiable information derived from such Covered Information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a User and for no other purpose; or (2) any entity that uses the Covered Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, or (ii) to enforce Respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

F. "**Facial Recognition Template**" means data, such as a unique combination of numbers or other alphanumeric characters, that is used to predict if the face of a specific User is represented in an image or other visual content.

G. "**Independent Director**" means a member of the Board of Directors other than an executive officer or employee of Respondent or any other individual having a relationship that, in the opinion of the Independent Nominating Committee, would interfere with the exercise of independent judgment in carrying out the responsibilities of such director.

H. "**Independent Privacy Committee**" means a committee of Respondent's Board of Directors, consisting of Independent Directors, all of whom meet the Privacy and Compliance Baseline Requirements.

I. "**Independent Nominating Committee**" means a committee of Respondent's Board of Directors, consisting of Independent Directors, the charter of which will encompass, among other things, approving for nomination individuals to the Respondent's Board of Directors and to the

Independent Privacy Committee.

J. "**Integrity**" means the protection of information from unauthorized destruction, corruption, or falsification.

K. "**Nonpublic User Information**" means any User profile information (*i.e.*, information that a User adds to or is listed on a User's Facebook profile), or User-generated content (*e.g.*, status updates, photos), that is restricted by one or more Privacy Setting(s).

L. "**Platform Terms**" means Respondent's written terms, policies, and procedures relating to the privacy, confidentiality, or Integrity of Covered Information that apply to Covered Third Parties.

M. "**Principal Executive Officer**" shall mean Mark Zuckerberg for so long as he serves as Chief Executive Officer or President of Respondent, or such other officer (regardless of title) that is designated in Respondent's Bylaws or by resolution of the Board of Directors as having the duties of the principal executive officer of Respondent, acting solely in his official capacity on behalf of Respondent; or if Mark Zuckerberg no longer serves in such a position, then such other individual serving as the Chief Executive Officer of Respondent, or such other officer (regardless of title) that is designated in Respondent's Bylaws or by resolution of the Board of Directors as having the duties of the principal executive officer of Respondent, acting solely in his or her official capacity on behalf of Respondent. In the event that Mark Zuckerberg is not the Principal Executive Officer and such position is jointly held by two or more persons, then each of such persons shall be deemed to be a Principal Executive Officer.

N. "**Privacy and Compliance Baseline Requirements**" shall refer to the requirements that, in the opinion of the Independent Nominating Committee, a member of the Independent Privacy Committee has (1) the ability to understand corporate compliance and accountability programs and to read and understand data protection and privacy policies and procedures, and (2) such other relevant privacy and compliance experience reasonably necessary to exercise his or her duties on the Independent Privacy Committee.

O. "**Privacy Setting**" includes any control or setting provided by Respondent that allows a User to restrict which individuals or entities can access or view Covered Information.

P. "**Representatives**" means Respondent's officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

Q. "**Respondent**" means Facebook, Inc. ("Facebook"), its successors and assigns, acting directly, or through any corporation, company, subsidiary, division, affiliate, website, or other device that it directly or indirectly controls. For purposes of Parts VII and VIII, Respondent means Facebook, and its successors and assigns, and WhatsApp Inc., and its successors and assigns.

R. "**User**" means an identified individual from whom Respondent has obtained information

for the purpose of providing access to Respondent's products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent, including Representatives of 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:

A. Its collection, use, or disclosure of any Covered Information;

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

C. The extent to which Respondent makes or has made Covered Information accessible to third parties;

D. The steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;

E. The extent to which Respondent makes or has made Covered Information accessible to any third party following deletion or termination of a User's account with Respondent or during such time as a User's account is deactivated or suspended; and

F. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. CHANGES TO SHARING OF NONPUBLIC USER INFORMATION

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a User's Nonpublic User Information by Respondent with any Covered Third Party, which materially exceeds the restrictions imposed by a User's Privacy Setting(s), shall:

A. Clearly and Conspicuously disclose (such as in a stand-alone disclosure or notice) to the User, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of Nonpublic User Information that will be disclosed to such Covered Third Parties, (2) the identity or specific categories of such Covered Third Parties, and (3) that such sharing exceeds the restrictions imposed by the Privacy Setting(s) in effect for the User; and

B. Obtain the User's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this Order; or (2) require

Respondent to obtain affirmative express consent for sharing of a User's Nonpublic User Information initiated by another User authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a User's Privacy Setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. § 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III. DELETION OF INFORMATION

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, must ensure that Covered Information cannot be accessed by any Covered Third Party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the User has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its Users from fraud or illegal activity. Nothing in this Part shall be construed to require Respondent to restrict access to any copy of Covered Information that has been posted to Respondent's websites or services by a User other than the User who deleted such information or deleted or terminated such account.

Additionally, Respondent and its Representatives shall further implement procedures designed to ensure that Covered Information entered by the User (such as User-generated content) is deleted from servers under Respondent's control, or is de-identified such that it is no longer associated with the User's account or device, within a reasonable period of time (not to exceed 120 days) from the time that the User has deleted such information, or his or her account, except (1) as required by law; (2) where necessary for the safety and security of Respondent's products, services, and Users, including to prevent fraud or other malicious activity; (3) where stored solely for backup or disaster recovery purposes (subject to a retention period necessary to provide a reliable service); or (4) where technically infeasible given Respondent's existing systems. If a User deletes an individual piece of Covered Information but does not delete his or her account, nothing in this paragraph shall be construed to require deletion or de-identification of metadata (*e.g.*, logs of User activity) that may remain associated with the User's account after the User has deleted such information. Respondent may seek modification of this paragraph pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. § 2.51(b) to address relevant developments that affect compliance with this paragraph, including, but not limited to, technological changes or changes in methods of deleting data.

IV. LIMITATIONS ON THE USE OR SHARING OF TELEPHONE NUMBERS SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, shall not use for the purpose of serving advertisements, or share with any Covered Third Party for such purpose, any telephone number that Respondent has identified through its source tagging system as being obtained from a User prior to the effective date of this Order for the specific purpose of enabling an account security feature designed to protect against unauthorized account access (*i.e.*, two-factor authentication, password recovery, and login alerts). Nothing in Part IV will limit Respondent's ability to use such telephone numbers if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

V. COVERED INFORMATION AND USER PASSWORD SECURITY

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, must implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security of Covered Information. In addition to any security-related measures associated with Respondent's Privacy Program under Part VII of this Order, the information security program must contain safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Covered Information. Specifically with respect to the collection, storage, transit, or use of User passwords, such safeguards shall include:

A. Not requesting or requiring, as part of the User log-in, authentication, or account creation process, User passwords to independent, third-party consumer applications, websites, or other services;

B. Cryptographically protecting or otherwise securing User passwords when stored and when in transit over the Internet or other similar transmission channel; and

C. Implementing regular automated scans designed to detect whether any User passwords are stored in plaintext within Respondent's data warehouse, and cryptographically protecting, deleting, or otherwise rendering unreadable any such passwords.

VI. FACIAL RECOGNITION TEMPLATES

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, in or affecting commerce, shall not create any new Facial Recognition Templates, and shall delete any existing Facial Recognition Templates within ninety (90) days from the effective date of this Order, for any Affected Facial Recognition User, unless Respondent Clearly and Conspicuously discloses (such as in a stand-alone disclosure or notice), separate and apart from any "privacy policy," "data policy," "statement of rights and responsibilities" page, or other similar documents, how Respondent will use, and to the extent applicable, share, the Facial Recognition Template for such User, and obtains such User's affirmative express consent.

VII. MANDATED PRIVACY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with any product, service, or sharing of Covered Information, shall establish and implement, and thereafter maintain a comprehensive privacy program ("Privacy Program") that protects the privacy, confidentiality, and Integrity of the Covered Information collected, used, or shared by Respondent. To satisfy this requirement, Respondent must, within 180 days of the effective date of this Order, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Privacy Program that includes: (1) the documented risk assessment required under Part VII.D. of this Order; (2) the documented safeguards required under Part VII.E. of this Order, including any known alternative procedures that would mitigate the identified risks to the privacy, confidentiality, or Integrity of the Covered Information, but which were not implemented and each reason such procedure(s) were not implemented; (3) a description of the training required under Part VII.G. of this Order; and (4) a description of the procedures adopted for implementing and monitoring the Privacy Program, including procedures used for evaluating and adjusting the Privacy Program as required under Part VII.J. of this Order;

B. Provide the written program required under Part VII.A. of this Order, and any evaluations thereof or adjustments thereto, to the Principal Executive Officer and to the Independent Privacy Committee created in response to Part X of this Order at least once every twelve (12) months;

C. Designate a qualified employee or employees to coordinate and be responsible for the Privacy Program ("Designated Compliance Officer(s)"), one of whom will be the Chief Privacy Officer for Product, subject to the reasonable approval of the Independent Privacy Committee, and who may only be removed from such position by Respondent with an affirmative vote of a majority of the Independent Privacy Committee;

D. Assess and document, at least once every twelve (12) months, internal and external risks in each area of its operation (*e.g.*, employee training and management; developer operations; partnerships with Covered Third Parties; sharing of Covered Information with Covered Third Parties or Facebook-owned affiliates; product research, design, and development; and product marketing and implementation) 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 shall further assess and document internal and external risks as described above as they relate to a Covered Incident, promptly following verification or

confirmation of such an incident, not to exceed thirty (30) days after the incident is verified or otherwise confirmed;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

1. Specifically with respect to any Covered Third Party that obtains or otherwise has access to Covered Information from Respondent for use in an independent, third-party consumer application or website, such safeguards shall include:

a. Requiring an annual self-certification by each Covered Third Party that certifies: (i) its compliance with each of Respondent's Platform Terms; and (ii) the purpose(s) or use(s) for each type of Covered Information to which it requests or continues to have access, and that each specified purpose or use complies with Respondent's Platform Terms;

b. Denying or terminating access to any type of Covered Information that the Covered Third Party fails to certify pursuant to Part VII.E.1.a.(ii) above, or, if the Covered Third Party fails to complete the annual self-certification, denying or terminating access to all Covered Information unless the Covered Third Party cures such failure within a reasonable time, not to exceed thirty (30) days;

c. Monitoring Covered Third Party compliance with Respondent's Platform Terms through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months; and

d. Enforcing against any Covered Third Party violations of Respondent's Platform Terms based solely on the severity, nature, and impact of the violation; the Covered Third Party's malicious conduct or history of violations; and applicable law;

2. Specifically with respect to Respondent's collection, use, or sharing of Covered Information in any new or modified product, service, or practice, such safeguards shall include:

a. Prior to implementing each new or modified product, service, or practice, (i) conducting a privacy review that assesses the risks to the privacy, confidentiality, and Integrity of the Covered Information, the safeguards in place to control such risks, and the sufficiency of the User notice and, if necessary, consent; and (ii) documenting a description of each reviewed product, service, or practice that was ultimately implemented; any safeguards being implemented to control for the identified risks; and the decision or recommendation made as a result of the

review (*e.g.*, whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

b. For each new or modified product, service, or practice that presents a material risk to the privacy, confidentiality, or Integrity of the Covered Information (*e.g.*, a completely new product, service, or practice that has not been previously subject to a privacy review; a material change in the sharing of Covered Information with a Facebook-owned affiliate; a modified product, service, or practice that includes a material change in the collection, use, or sharing of Covered Information; a product, service, or practice directed to minors; or a product, service, or practice involving health, financial, biometric, or other similarly sensitive information), producing a written report ("Privacy Review Statement") that describes:

(i) The type(s) of Covered Information that will be collected, and how that Covered Information will be used, retained, and shared;

(ii) The notice provided to Users about, and the mechanism(s), if any, by which Users will consent to, the collection of their Covered Information and the purposes for which such information will be used, retained, or shared by Respondent;

(iii) Any risks to the privacy, confidentiality, or Integrity of the Covered Information;

(iv) The existing safeguards that would control for the identified risks to the privacy, confidentiality, and Integrity of the Covered Information and whether any new safeguards would need to be implemented to control for such risks; and

(v) Any other known safeguards or other procedures that would mitigate the identified risks to the privacy, confidentiality, and Integrity of the Covered Information that were not implemented, such as minimizing the amount or type(s) of Covered Information that is collected, used, and shared; and each reason that those alternates were not implemented;

c. The Designated Compliance Officer(s) shall deliver a quarterly report ("Quarterly Privacy Review Report") to the Principal Executive Officer and to the Assessor that provides: (i) a summary of the Privacy Review Statements generated during the prior fiscal quarter under Part VII.E.2.b, including a detailed discussion of the material risks to the privacy, confidentiality, and Integrity of the Covered Information that were identified and how such risks were addressed; (ii) an appendix with each Privacy Review Statement generated during the prior fiscal quarter under Part VII.E.2.b; and (iii) an appendix that lists all privacy decisions generated during the prior fiscal quarter under Part VII.E.2.a;

d. The appendices required under Part VII.E.2.c.(ii) and (iii) shall be provided to the Assessor no fewer than twenty-one (21) days in advance of the quarterly meeting of the Independent Privacy Committee as specified in Part X.A.5. A copy of the summary in the Quarterly Privacy Review Report required under VII.E.2.c.(i) shall be provided to Assessor no fewer than fourteen (14) days in advance of the quarterly meeting; and

e. A copy of the Quarterly Privacy Review Report shall also be furnished, upon request, to the Commission;

3. Specifically with respect to Respondent's employees' access to Covered Information maintained in Respondent's data warehouse(s), such safeguards shall include designing, implementing, and maintaining access policies and controls that limit employee access to any table(s) or other comparable data storage units known to contain Covered Information to only those employees with a business need to access such Covered Information;

4. Specifically with respect to Respondent's sharing of Covered Information with any other Facebook-owned affiliate, Respondent shall design, implement, maintain, and document safeguards that control for risks to the privacy, confidentiality, and Integrity of such Covered Information, based on the volume and sensitivity of such Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information; and

5. Specifically with respect to facial recognition, such safeguards shall include:

a. Prior to using or sharing any Facial Recognition Template for a User in a manner that materially exceeds the types of uses or sharing disclosed to that User at the time that User's consent was previously obtained,

(i) Clearly and Conspicuously disclosing (such as in a stand-alone disclosure or notice), separate and apart from any "privacy policy," "data policy," "statement of rights and responsibilities" page, or other similar document, how Respondent will use or, to the extent applicable, share, such Facial Recognition Template; and

(ii) Obtaining the User's affirmative express consent;

b. Nothing in this provision shall limit Respondent's ability to use Facial Recognition Templates for fraud prevention or remediation, or protecting the safety, reliability and security of Respondent's platform or Users, so long as Respondent discloses these types of uses in Respondent's privacy policy or similar document;

F. Assess, monitor, and test, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the effectiveness of any safeguards put in place pursuant to Part VII.E. of this Order to address the risks to the privacy, confidentiality, or Integrity of Covered Information, and modify the Privacy Program based on the results;

G. Establish regular privacy training programs for all employees on at least an annual basis, updated to address any internal or external risks identified by Respondent in Part VII.D. of this Order and safeguards implemented pursuant to Part VII.E. of this Order, that includes training on the requirements of this Order;

H. Select and retain service providers capable of safeguarding Covered Information they receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Information;

I. Consult with, and seek appropriate guidance from, independent, third-party experts on data protection and privacy in the course of establishing, implementing, maintaining, and updating the Privacy Program; and

J. Evaluate and adjust the Privacy Program in light of any material changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Part VII.D. of this Order, and any other circumstances that Respondent knows or has reason to believe may have a material impact on the effectiveness of the Privacy Program. Respondent may make this evaluation and adjustment to the Privacy Program at any time, but must, at a minimum, evaluate the Privacy Program at least once every twelve (12) months and modify the Privacy Program as necessary based on the results.

VIII. INDEPENDENT PRIVACY PROGRAM ASSESSMENTS

IT IS FURTHER ORDERED that, in connection with compliance with Part VII of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessment must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)"), selected by the Respondent, subject to the reasonable approval of the Independent Privacy Committee and subject to Part VIII.B, who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Mandated Privacy Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and furnishes such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission ("Associate Director") with the name(s) and affiliation(s) of the person(s) selected to conduct the Assessment, which the

Associate Director shall have the authority to approve;

C. The reporting period for the Assessments must cover: (1) the first 180 days after the Privacy Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must: (1) determine whether Respondent has implemented and maintained the Privacy Program required by Part VII.A-J of this Order, titled Mandated Privacy Program; (2) assess the effectiveness of Respondent's implementation and maintenance of each subpart in Part VII of this Order; (3) identify any gaps or weaknesses in the Privacy Program; and (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. To the extent that Respondent revises, updates, or adds one or more safeguards required under Part VII.E. of this Order in the middle of an Assessment period, the Assessment shall assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard;

E. Respondent and its Representatives must disclose all material facts to the Assessor(s), and must not misrepresent in any manner, expressly or by implication, any fact material to the Assessor(s)' (1) determination of whether Respondent has implemented and maintained the Mandated Privacy Program required by Part VII of this Order; (2) assessment of the effectiveness of the implementation and maintenance of subparts VII.A-J of this Order; or (3) identification of any gaps or weaknesses to the Mandated Privacy Program;

F. Respondent and its Representatives, whether acting directly or indirectly, must provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

G. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Mandated Privacy Program, and did not rely primarily on assertions or attestations by Respondent's management;

H. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit each Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109." Each Assessment shall be retained by Respondent until this Order is terminated, and shall be provided to the Associate Director within ten (10) days of Request; and

I. The Assessor may only be removed by Respondent from such position, subject to Part VIII.B, with the affirmative vote of a majority of the Independent Privacy Committee.

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent must submit a report within thirty (30) days following Respondent's verification or confirmation of a Covered Incident, and subsequently updated every thirty (30) days until the incident is fully investigated and any remediation efforts are fully implemented, to the Assessor(s) and to the Commission, that includes, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. An overview of the facts relating to the Covered Incident, including the causes of the Covered Incident;

C. A description of each type of Covered Information that was accessed, collected, used, destroyed, or shared without the User's authorization or consent;

D. The number of Users whose Covered Information was accessed, collected, used, destroyed, or shared without the User's authorization or consent; and

E. An overview of the acts, if any, that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access.

Unless otherwise directed by a Commission representative in writing, all reports to the Commission pursuant to this Order must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109."

X. MANDATED INDEPENDENT PRIVACY COMMITTEE AND OTHER GOVERNANCE MATTERS

IT IS FURTHER ORDERED that:

A. Within one hundred and twenty (120) days after entry of this Order, Respondent shall create the Independent Privacy Committee, including adopting a new committee charter or amending the charter of an existing committee. The adopted or amended charter for such committee shall include the following qualifications, authority, and responsibilities, including:

1. The committee shall hold at least four regularly-scheduled meetings each year;

2. Each member of the committee shall be an Independent Director, and each of the members of the committee shall meet the Privacy and Compliance Baseline Requirements;

3. Each quarter, the Respondent shall cause the committee to receive a briefing from

management regarding (i) the state of the Privacy Program, (ii) Respondent's compliance with the Order, and (iii) material risks to the privacy, confidentiality, and Integrity of the Covered Information that have been discovered since the most recent meeting of the committee or that were raised by management in a prior meeting with the committee and continue to persist;

4. On at least an annual basis, management shall conduct a review for the committee of the Privacy Program and discuss Respondent's assessment of material risks to the privacy, confidentiality, and Integrity of the Covered Information and the steps Respondent has taken or plans to take to monitor or mitigate such risks, including Respondent's procedures and any related policies with respect to risk assessment and risk management;

5. The committee shall meet with the Assessor at least quarterly, and at the conclusion of each biennial Assessment;

a. At each quarterly meeting, the Assessor shall review with management and the committee (i) the Assessor's ongoing assessment of the Privacy Program, and (ii) any material risks to the privacy, confidentiality, and Integrity of the Covered Information that have been identified by the Assessor since the Assessor's most recent meeting with the committee, or that were raised by the Assessor in a prior meeting with the committee and continue to persist;

b. At each quarterly meeting, the committee (together with any other Independent Directors in attendance) shall meet with the Assessor in an executive session without management present to discuss matters involving the Assessment or other privacy-related issues or risks, as appropriate; and

c. At the meeting to review the biennial Assessment with the Assessor, the Assessor and the committee shall review the various elements of the Assessment, as well as (1) any material issues raised by the most recent Assessment or material unresolved issues from prior Assessments, and (2) in an executive session without management present, any problems or difficulties with management. Following the review of the biennial Assessment (at either the same meeting or the following meeting), management shall review with the committee its proposed remediation plans to address any such issues raised in the Assessment; and

6. The committee shall evaluate the independence of the Assessor, and the Assessor shall not be appointed or removed by Respondent, subject to Part VIII.B, without the prior approval of a majority of the committee;

B. Within one hundred and twenty (120) days after entry of this Order, Respondent shall create the Independent Nominating Committee, including adopting a new committee charter or amending the charter of an existing committee to provide that such committee shall have the following authority and responsibilities, including:

1. The committee shall have the sole authority to recommend the appointment of directors, or the nomination of candidates for election, to Respondent's Board of Directors,

such that Respondent's Board of Directors may not approve any such appointment or nomination in the absence of a favorable recommendation from the committee;

2. The committee shall have the sole authority to recommend the appointment of directors to, or the removal of directors from, the Independent Privacy Committee, such that Respondent's Board of Directors may not approve any such appointment or removal in the absence of a favorable recommendation from the committee; and

3. The committee shall determine whether the members of the Independent Privacy Committee qualify as Independent Directors and whether each member of the Independent Privacy Committee meets the Privacy and Compliance Baseline Requirements. The foregoing determinations shall be made prior to, or concurrent with, the formation of the Independent Privacy Committee for the initial members; and prior to, or concurrent with, the appointment of each new director to the Independent Privacy Committee for future members;

C. Within one hundred and eighty (180) days after entry of this Order, Respondent shall adopt and file an amendment to Respondent's Certificate of Incorporation (the "Charter Amendment") in accordance with applicable Delaware law modifying the provisions of Article VI, Section 4 thereof with respect to the removal of directors as set forth in the form attached hereto as Exhibit 1, for the purpose of adding a new Article VI, Section 4(b) (hereafter "Supplemental Removal Provision"). Respondent shall not further alter or amend the Supplemental Removal Provision of Respondent's Certificate of Incorporation for the term of the Order. Notwithstanding the foregoing, in the event that, prior to the effectiveness of the Charter Amendment, any person commences any legal or administrative proceeding or action (an "Action"), or any governmental or regulatory entity or body, or any court, tribunal, or judicial body, in each case whether federal, state, or local, issues or grants any order, judgment, decision, decree, injunction, or ruling that has the effect of delaying, restraining, enjoining, prohibiting, or otherwise preventing the approval, filing, or effectiveness of the Charter Amendment (individually or collectively, a "Restraint") within 180 days after entry of this Order, that time period shall be extended and Respondent shall be deemed to be in compliance with the Order so long as: (a) Respondent diligently pursues in good faith the favorable resolution of such Action, and (b) Respondent adopts and files the Charter Amendment in accordance with applicable Delaware law as promptly as reasonably practicable following the resolution of the Action and at such time as such Restraint (if any) is withdrawn, vacated, or terminated; and

D. Nothing in this Order shall be construed to expand, modify, or alter the fiduciary duties of the members of the Respondent's Board of Directors or any committee thereof.

XI. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent shall:

A. Within forty-five (45) days after the end of each full fiscal quarter (but in no event later than the first meeting of the Independent Privacy Committee with respect to such fiscal quarter (as provided in Part X.A)) following the anniversary of the effective date of this Order, provide the Commission with its certification, signed by the Principal Executive Officer and the Designated

Compliance Officer(s) on behalf of Respondent, that, with respect to such fiscal quarter: (1) Respondent has established, implemented, and maintained a Privacy Program that complies in all material respects with the requirements of Part VII of this Order; and (2) Respondent is not aware of any material noncompliance with Part VII that has not been corrected or disclosed to the Commission. In making this certification on behalf of Respondent, the Principal Executive Officer shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII, provided by knowledgeable personnel charged with implementing the Privacy Program; and (c) the Principal Executive Officer's review of the summaries in the Quarterly Privacy Review Report required under Part VII.E.2.c.(i) for such fiscal quarter, as well as any material issues raised in Covered Incident Reports required under Part IX for such fiscal quarter. The Designated Compliance Officer(s) shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII, provided by knowledgeable personnel charged with implementing the Privacy Program; (c) material issues identified in the Quarterly Privacy Review Report required under Part VII.E.2.c.; and (d) material issues raised in the Covered Incident Reports required under Part IX for such fiscal quarter; and

B. Within forty-five (45) days after the end of the first full fiscal quarter (but in no event later than the first meeting of the Independent Privacy Committee with respect to such fiscal quarter (as provided in Part X.A.)) following the anniversary of the effective date of this Order and every year thereafter, provide the Commission with its certification, signed by the Principal Executive Officer and the Designated Compliance Officer(s) on behalf of Respondent, that: (1) Respondent has established, implemented, and maintained the requirements of this Order in all material respects; and (2) Respondent is not aware of any material noncompliance with this Order that has not been corrected or disclosed to the Commission. In making this certification on behalf of Respondent, the Principal Executive Officer shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII of this Order, provided by knowledgeable personnel charged with implementing the Privacy Program; and (c) the Principal Executive Officer's review of the written program required under Part VII.A. of this Order and the summaries in the Quarterly Privacy Review Reports required under Part VII.E.2.c.(i) for the preceding year, as well as any material issues raised in Covered Incident Reports required under Part IX for the preceding year. The Designated Compliance Officer(s) shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII, provided by knowledgeable personnel charged with implementing the Privacy Program; (c) material issues identified in the Quarterly Privacy Review Reports required under Part VII.E.2.c. for the preceding year; and (d) material issues raised in the Covered Incident Reports required under Part IX for the preceding year.

Unless otherwise directed by a Commission representative in writing, Respondent shall submit all certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re Facebook, Inc*., FTC File No. 182-3109."

XII. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury;

B. For five (5) years after entry of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Part titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities; and

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XIII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One hundred eighty (180) days after entry of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, which: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business; (4) describes in detail whether and how Respondent is in compliance with each Part of this Order; and (5) provides a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission;

B. For twenty (20) years after entry of this Order, Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) Respondent's corporate structure; or (3) the structure of any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order;

C. Respondent must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing;

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that, to the best of my knowledge and reasonable belief, the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature; and

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "*In re Facebook, Inc.*, FTC File No. 182-3109."

XIV. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after entry of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. All widely-disseminated statements by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any Covered Information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different Privacy Setting made available to Users (including screenshots/screencasts of Privacy Settings and the User interfaces, consent flows, and paths a User must take to reach such settings);

B. Records sufficient to identify the types of Covered Information that Respondent provides or makes available to any Covered Third Party that is subject to the requirements of Part VII.E.1., including records identifying: (1) the specific data fields to which access was granted; (2) the means by which the information was provided or made available; (3) the identity of the Covered Third Party to which access was granted; (4) the self-certifications provided by the Covered Third Party (as described in Part VII.E.1); and (5) the date(s) when access was provided;

C. All consumer complaints directed at Respondent or forwarded to Respondent by a Covered Third Party that relate to the conduct prohibited by this Order and any responses to such complaints;

D. Any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order;

E. Each materially different document relating to Respondent's attempt to obtain the consent of Users referred to in Part II titled Changes To Sharing Of Covered Information, along with documents and information sufficient to show each User's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of Users for whom each such Privacy Setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent;

F. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment; and

G. All records necessary to demonstrate full compliance with each Part of this Order, including all submissions to the Commission.

XV. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69;

B. For matters concerning this Order, the Commission is authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview any employee or other person affiliated with Respondent who has agreed to such an interview. The person interviewed may have counsel present; and

C. The Commission may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVI. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided*, *however*, that the filing of such a complaint will not affect the duration of:

A. Any Part in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

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

By the Commission.

April Tabor
Acting Secretary

SEAL:
ISSUED:

ARTICLE VI: MATTERS RELATING TO THE BOARD OF DIRECTORS

4. Term and Removal.

(a) Each director shall hold office until such director's successor is elected and qualified, or until such director's earlier death, resignation or removal. Any director may resign at any time upon notice to the corporation given in writing or by any electronic transmission permitted in the corporation's Bylaws or in accordance with applicable law. No decrease in the number of directors constituting the Whole Board shall shorten the term of any incumbent director.

(b) Notwithstanding anything in this Section 4 of this Article VI to the contrary, subject to the rights of the holders of any series of Preferred Stock with respect to directors elected thereby, from and after the effectiveness of the Classified Board, no director may be removed except for cause and only by the affirmative vote of the holders of at least a majority of the voting power of the then-outstanding shares of capital stock of the corporation then entitled to vote at an election of directors voting together as a single class.

(c) For so long as the [Federal Trade Commission Decision & Order] (the "***Order***") remains in effect, (i) no director serving on the Independent Privacy Committee, as that term is defined in the Order (any such director, a "***Privacy Committee Delegate***"), shall be removed solely for reasons related to actions taken in good faith in furtherance of such Privacy Committee Delegate's duties as a member of the Independent Privacy Committee as set forth in the Order (a "***Privacy Reason***"), except by the affirmative vote of the holders of at least two-thirds of the voting power of the then-outstanding shares of the capital stock of the corporation entitled to vote generally in the election of directors, voting together as a single class, and (ii) no Privacy Committee Delegate shall be removed for reasons other than a Privacy Reason with the intent to circumvent the requirements of clause (i) above, except by the affirmative vote of the holders of at least two-thirds of the voting power of the then-outstanding shares of the capital stock of the corporation entitled to vote generally in the election of directors, voting together as a single class.