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

[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

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

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

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 thh4 (r)-mpat(e)-2pm5 (i

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 0 Td [(.D)2 (. of)

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

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

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 u004 Tw [(VII.on)]TJoart

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 re