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;