The Commercial Face Recognition Act of 2017

Courtney Matteson, Nchinda Nchinda, Kiran Wattamwar

SECTION 1. SHORT TITLE.— This Act is entitled the "Commercial Face Recognition Act" or "CFRA."

SECTION 2. DEFINITIONS.— For purposes of this Act—

a) **"Covered entity"** means a person who collects, processes, uses or distributes facial data for commercial purposes, but does not include law enforcement or government entities.

b) **"Business associate"** means a person who performs activities that involve the user or disclosure of facial data on behalf of, or provides services to, a covered entity pursuant to a contract that complies with Section 7 of this Act.

c) "**Data subject**" means an individual whose facial data is collected or processed.

d) "**Facial data**" means data that represents, is extracted from, or is derived from, an image of a data subject's face and/or neck, whether captured in-person, through photographs, through video, by sensors or by other means, that represents physical characteristics and that can be used to identify a data subject, whether alone or when combined with another form of facial data.

   i) Forms of facial data include, but are not limited to, any one or combination of the following—

      (1) geometric data, including geometric and spatial measurements and relationships, measurements of illumination, angle, or other visual components;

      (2) data generated from skin texture analysis, including placement of pores, lines, or other features of an individual's skin;

      (3) data generated from a photometric analysis;

(4) faceprints or other digital codes created using algorithms that represent models of a part of the body, including 2-D or 3-D models; and

(5) data generated from body scans such as an x-ray or MRI, except to the extent regulated by specific healthcare or medical services industry legislation.

ii) Facial data does not include: voices, fingerprints, written signatures, writing samples, tattoo descriptions, human biological samples used for valid scientific screening, testing, or transplant, or a photograph or video, unless the photograph or video is processed, shared, or stored for use as a source of facial data.

e) "**Facial database**" means a repository of stored facial data.

f) "**Enroll**" means to store facial data in connection with, or in a way that permits association of facial data with a human identity at the time of storage, which includes, but is not limited to, a user number, user name, or other personally-identifiable information about a data subject.

g) "**Unenroll**" means to store facial data in such a way that does not permit association of facial data with a human identity.

h) "**Facial detection"** means a task whereby a system distinguishes the presence from the absence of a human face, neck or other part of the body without storing data upon completion of the task.

i) "**Facial characterization**" means a task whereby a system uses an algorithm or other automated or semi-automated process, without enrolling a data subject's facial data, to discern a data subject's—

i) demographic information, including, but not limited to, gender, race, age, nationality, or sexual orientation, or

ii) emotional state or mood.

j) "**Facial verification**" means a task whereby a system uses an automated or semi-automated process to compare facial data to a facial database to verify an individual's identity, without enrolling the facial data.

k) "**Facial identification**" means a task whereby a system uses an automated or semi-automated process to compare facial data to known data about an enrolled data subject to identify an individual.

SECTION 3. TECHNOLOGY NEUTRALITY.—

a) This Act applies to all uses of facial data, across all devices and forms of facial data.

SECTION 4. PRIVACY POLICY.—

a) **Privacy policy.** A covered entity shall conspicuously post, in accordance with subsection (b), a privacy policy that includes all material information pertaining to the covered entity's practice for the collection, use, storage, and disclosure of facial data, including—

i) the types of facial data collected and stored and the purposes for collection;

ii) the types of non-facial data linked to the facial data when a data subject is enrolled;

iii) the ways in which facial data is stored and repurposed;

iv) the extent of disclosure of facial data to business associates or unaffiliated entities;

v) the amount of time that facial data will be stored, as well as the measures taken to comply with the standards in Sections 8(b)–(d); and

vi) clear instructions for how the data subject may access, control and request deletion of facial data, as required by Section 7(a).

b) **Location of privacy policy.** The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:

i) a Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the covered entity's Web site;

ii) an icon, text link or other functional hyperlink that hyperlinks to a Web page on which the actual privacy policy is posted, if—

(1) the hyperlink is located on the homepage or the first significant page after entering the Web site;

(2) the hyperlink includes the word "privacy"; and

(3) is so displayed that a reasonable person would notice it;

iii) in the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the service.

c) **Material adverse change.** Following any material adverse change in the terms of the privacy policy, a covered entity shall—

i) notify the data subject in a clear, concise manner, separate from the privacy policy, of the change in policy and how it affects the storage, use, disclosure or disposal of facial data; and

ii) obtain consent prior to resuming using the data subject's facial data for facial identification.

SECTION 5. NOTICE AND CONSENT REQUIREMENTS.—

a) **Form of notice.** A notice complies with this Section only if it is clear, concise, separate from the privacy policy, and through a conspicuous procedure reasonably designed to reach the affected data subject—

i) notifies the data subject of the specific purpose for which the facial data will be used;

ii) notifies the data subject of the length of time the facial data will be retained; and

iii) provides instructions for how to access, or a link to, the privacy policy.

b) **Facial characterization.** A covered entity shall not use a data subject's facial data for facial characterization unless the covered entity provides the data subject with notice as described in subsection (a).

c) **Facial verification.** A covered entity shall not use a data subject's facial data for facial verification unless the covered entity provides the data subject with notice as described in subsection (a).

d) **Enrollment.** Prior to enrolling a data subject's facial data, a covered entity shall—

   i) provide the data subject with notice as described in subsection (a); and

   ii) provide the data subject with instructions, separate from the privacy policy, for how to access, control, and request deletion of facial data, as required by Section 7(a).

e) **Facial identification.** Before or at the time of first use of a data subject's facial data for purposes of facial identification, a covered entity shall—

   i) provide the data subject with notice in accordance with Section 5(a); and

   ii) obtain express consent, in a written, electronic, or other form by which consent can be documented, the data subject's full consent to—

      (1) the specific purpose for which the facial data will be used; and

      (2) the length of time the facial data will be retained.

f) **Exceptions.** Neither notice or consent is required if—

   i) a covered entity uses facial data for facial detection only;

   ii) a covered entity uses facial data for purposes of protecting the covered entity's property and personnel;

iii) a covered entity uses facial data in response to a request by a governmental entity, if the covered entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires the use without delay of information relating to the emergency;

iv) a covered entity uses facial data of human remains in response to a request by a governmental entity to identify human remains;

v) a covered entity uses facial data for internal product development, private testing or research purposes prior to the public deployment of the specific technology; or

vi) a covered entity uses facial data for the sole purpose of determining eligibility for enrollment in a facial identification system, but only if the facial data is immediately destroyed if enrollment is not completed.

SECTION 6. USE RESTRICTIONS AND PROHIBITIONS.—

a) **Use out of context**. A covered entity is prohibited from using facial data for facial identification in a manner that is materially inconsistent with the purpose for which the data subject consented to use, unless the covered entity provides notice and obtains consent in accordance with the requirements of Section 5(e).

b) **Discrimination and provision of benefits.** A covered entity is prohibited from using facial characterization to inform decisions about—

i) employment eligibility, promotion or retention, health care treatment eligibility, credit eligibility, or housing eligibility; or

ii) the provision of goods or services, if the decision is made on the basis of race, gender, ethnicity, religion, and/or age; or

iii) marketing or advertising, if the decision is made on the basis of data related to race, religion, or ethnicity.

c) **Price discrimination.** A covered entity is prohibited from using facial characterization, facial verification or facial identification to make determinations about price of goods or services to be provided to a data subject based on the data subject's facial data.

d) **Consent as a precondition.** A covered entity is prohibited from requiring a person or customer to consent to enrollment, disclosure or use of facial data as a precondition for employment or provision of goods or services except—

i) when the covered entity is a company that provides medical services; and

ii) to the extent necessary for an employer to conduct background checks or implement employee security protocols.

SECTION 7. USER CONTROL.—

a) **In general.** A covered entity or business associate shall provide a data subject with a clear, simple way to—

i) access the facial data the covered entity stores about the data subject, not including any derived or extracted data;

ii) request that the covered entity or business associate—

(1) unenroll the data subject's facial data from the facial database;

(2) discontinue use of the data subject's facial data for facial characterization, facial verification, facial identification, or any combination thereof;

(3) refrain from disclosing facial data with third parties;

(4) challenge a determination when the data subject's data is used as a barrier to access goods or services; and

(5) to the extent practicable, either—

(a) delete any facial data collected by the covered entity, or if deletion is not possible, or

(b) refrain from further processing, use, or disclosure of such data;

b) **Response to requests.** A covered entity shall comply with requests made by data subjects under subsection (a)(ii) within a reasonable time period.

c) **Data disclosed to third parties**. A covered entity shall notify business associates and third parties of and ensure business associates and third parties honor requests made by data subjects under subsection (a)(ii).

d) **Bankruptcy or change of control of facial data.** A covered entity shall provide the data subject with notice, in the form prescribed by Section 5(a), following change of control of facial data, such as a bankruptcy, merger or buy-out of the covered entity which changes the personnel and systems that have access to facial data.

SECTION 8. DISCLOSURE, RETENTION AND DELETION STANDARDS.—

a) **Disclosure.** A covered entity is prohibited from selling, leasing, trading, or otherwise disclosing facial data of a data subject to another person without the data subject's express consent, in a written, electronic, or other form by which consent can be documented unless the disclosure is—

i) made to a business associate, but only if—

(1) the covered entity has entered into a written agreement with the business associate affirming the business associate's responsibility to—

(a) comply with Sections 4, 6, 7, 8, and 9 of this Act;

(b) use facial data only for the purposes for which it was engaged by the covered entity, and not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate;

(c) notify the covered entity immediately upon learning of a material change to its use of facial data or of a data breach involving the facial data; and

(2) one of the following applies—

(a) the disclosure is necessary to provide a product or service affirmatively subscribed to, requested, or expressly authorized by the data subject; or

(b) the disclosure is necessary to effect, administer, enforce or complete a financial transaction that the data subject requested, initiated, or authorized; or

ii) required or expressly authorized by a court order upon an evidentiary showing as required under applicable law; or

iii) as may be necessary for the protection of the rights or property of the covered entity;

iv) to a government entity, if the covered entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency; or

v) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A or in connection with a crime under 18 U.S.C. §§ 2251–2260; or

vi) the disclosure occurs subsequent to, and because of, the sale of the covered entity to another covered entity.

b) **Data security and retention requirements.** A covered entity or business associate who knowingly possesses facial data of a data subject—

i) shall retain the facial data no longer than is reasonably necessary to provide a transaction or deliver a service to a data subject, or if such service is ongoing, is reasonable for the ongoing nature of the service;

ii) shall take reasonable care to guard against unauthorized access to and acquisition of facial data that are in the possession or under the control of the person;

iii) shall develop and maintain adequate measures to ensure the security of facial databases and the facial data contained therein, in accordance with the standards developed and promulgated by the National Institute for Standards and Technology, including but not limited to—

(1) encrypting facial data in at rest in a facial database;

(2) encrypting all facial data transmitted over a network, unless doing so would impose an unreasonable burden on the covered entity or its business associate; and

(3) encrypting all facial data while in transit to third parties in a secure communication channel.

c) **Disposal.** When a covered entity or business associate no longer needs a data subject's facial data for the original purpose for which the facial data was to be used, the covered entity and any business associate to which it has disclosed the data shall, within 120 days and unless prohibited by another law, regulation or court order, remove the data subject's facial data from all facial databases and destroy the facial data.

d) **Data breach notification.** Upon notification of or discovery of a data breach, a covered entity or business associate shall disclose to a data subject the sensitive information of the data subject that was affected by the breach by means of a notice when—

i) the breach may lead to a risk of identity theft or fraud against the data subject; and

ii) there exists sufficient contact information to provide notice; and

iii) the cost of providing notice by the covered entity does not exceed $1000.

SECTION 9. ENFORCEMENT.—

a) **Enforcement by the Federal Trade Commission.** The Commission shall be authorized to bring an enforcement action for violations of Sections 4, 5, 6, 7 and 8 of this Act under the Federal Trade Commission Act (15 U.S.C. 41 *et seq.*); such violations shall be treated as an unfair or deceptive act or other practice prohibited under Section 18(a)(1)(B) of the Federal Trade Commission Act, subject to enforcement by the Commission under Section 5(b) of the Federal Trade Commission Act.

b) Nothing in this Act should be construed as providing a private right of action.

SECTION 10. CONSUMER EDUCATION.—

a) The Federal Trade Commission shall create and maintain a public webpage to educate the general public—

i) about the tools available to express preferences regarding the collection, enrollment and use of personal information for commercial face recognition purposes; and

ii) how to use such tools.

SECTION 11. PENALTIES.—

a) Covered entities that willfully violate or fail to comply with the regulations set by this Act may be liable for $25,000 for each violation. Nothing in this Act shall diminish or restrict the application of other penalties that may arise under other state and federal laws.

SECTION 12. SEVERABILITY.—

a) If any provision of this Act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 13. PREEMPTION.—

a) The provisions of this Act preempt only the provisions of State or local law that conflict with the provisions of this Act. The Act shall not be construed to preempt State or local laws the provide data subjects with a greater level of protection vis-a-vis covered entities.

SECTION 14. CONSTRUCTION—

a) Nothing in this Act shall be construed to apply in any manner to a financial institution or an affiliate of a financial institution to the extent that it conflicts with Title V of the Gramm-Leach Bliley Act of 1999 and the rules promulgated thereunder.

b) Nothing in this Act shall be construed to apply in a manner that conflicts with the Health Insurance Portability and Accountability Act of 1996 and the rules promulgated thereunder.