The Commercial Face Recognition Act
Section-by-Section Summary

Courtney Matteson, Nchinda Nchinda, Kiran Wattamwar

Section 1: Short Title

Section 2: Definitions

- **"Covered entity":** means a company or individual that uses facial data for facial characterization, facial verification or facial identification, but does not include government entities. The concept of regulating "covered entities" and their "business associates" is modeled after the structure of HIPAA.
- **"Business associates":** means a third-party entity or "vendor" that performs services for the covered entity that involves the use of disclosure of facial data. Business associates include only third parties that are in a valid contractual relationship with covered entities pursuant to this Act. If a business associate uses a form of facial recognition technology, it becomes a "covered entity."
- **"Data subject":** means an individual whose facial data is collected or processed.
- **"Facial data":** means data that represents, is derived from, or is extracted from an image of a data subject's *body*. This includes data captured in-person (i.e. using a CCTV camera or sensor – this type of data has been argued by Facebook in recent litigation to not fall within the definition of "biometric identifier" as defined by the Illinois statute) as well as photos and videos online. This definition is designed to be broad enough to encompass data representing physical characteristics and any data that is extracted from or results from the processing thereof.
- **"Facial database":** means a repository of stored facial data.
- **"Enroll":** means to store facial data in in a way that permits its association with a human identity (i.e. user ID, profile, or other information that connects to a specific individual) at the time of storage. This definition may be different from the way "enroll" has been used in other contexts (i.e. to refer to the mere storage of a "faceprint" or other facial data). Here, the facial data must be stored *and* be linked to an identity to be "enrolled." Therefore, enrollment is what distinguishes "facial verification" from "facial identification." In order for facial identification to reveal the human identity of an anonymous face, the human's facial data must already be enrolled; in contrast, for purposes of this legislation, "facial verification" occurs without enrollment because the algorithm merely compares the similarity of two sets of facial data without associating the facial data with a human identity.
- **Unenroll":** means to store facial data in such a way that does not connect facial data to a human identity and does not permit association of facial data with a human identity.
- **"Facial detection":** means a task whereby a system distinguishes the presence from the absence of a face without storing facial data. This is the least intrusive form of technology regulated, and is therefore the least restricted by this Act.
- **"Facial characterization":** means a task whereby a system uses an automated or semi-automated process to discern a data subject's: 1) demographic information or 2) emotional state (i.e. a smile).
- **"Facial verification":** means a task whereby a system uses an automated or semi-automated process to verify an individual's identity without enrolling the facial data (although it may retain the probe facial data). This is also called one-to-one verification – the system merely checks the likelihood that two faces belong to the same person, but the system does not know the face's human identity. There is nothing inherent to a face verification algorithm that requires that it not enroll the facial data. However, for purposes of this legislation, in order for a use of technology to be regulated as "facial verification," it may not enroll the data. If it does, it will be regulated as a use of facial identification.
- **"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. This is the most comprehensive form of facial recognition technology since it connects a human identity to a previously-anonymous face, and therefore is the most restricted by this Act.

Section 3: Technology Neutrality

- Uses of facial data across all devices and forms of technology are covered by this Act. This provision is meant to ensure that the Act covers any way facial recognition technology could conceivably be deployed in the future, whether used in wearables, body implants, or physical computer installations.

Section 4: Privacy Policy

- **Privacy policy requirements:** covered entities must post a privacy policy describing: 1) all material information pertaining to the way the entity collects, uses, stores, and discloses facial data to third parties; 2) the ways in which data is stored, secured and repurposed, and the length of retention; and 3) instructions for how data subjects can view and request alterations or deletions of their data.
- **Location of privacy policy**: the privacy policy must be posted on the covered entity's Web site, either on the home page, or using a hyperlink from either the home page of the first significant page after entering the Web site, so long as the hyperlink contains the word "privacy" and is displayed so that a reasonable person would notice it. This provision is inspired by the California Online Privacy Protection Act §§ 22575–77.
- **Material adverse change:** if there is a material change in the privacy policy that adversely affects a data subject, covered entities must 1) notify data subjects of the change in policy and how it affects facial data; and 2) re-obtain consent for use for facial identification if the data subject has consented.

Section 5: Notice and Consent Requirements

- **Form of notice:** in order for notice to comply with this Act, it must be clear, concise, separate from the privacy policy, and through a "conspicuous procedure" that is reasonably designed to reach the affected data subject.
    - Content of notice: it must notify the data subject of the specific purpose for which the facial data will be used as well as the period of time for which the facial data will be retained; and must provide instructions for how to access the privacy policy (or provide a link to it).
- **Notice and consent requirements**: whether notice and/or consent is required depends on what is occurring with the facial data:
    - At collection: the general rule is that notice and consent are not required for collection. At enrollment: if a data subject's facial data is enrolled, the covered entity must provide notice and instructions for how to access, control, and request deletion of the data. Therefore, notice for *collection* is only required if the facial data is connected to a human identity.
    - Use for facial characterization: notice is required before first use, but consent is not required.
    - Use for facial verification: notice is required before first use, but consent is not required.
    - Use for facial identification: before a covered entity uses a data subject's facial data for facial identification, a covered entity must provide notice and obtain the data subject's express consent in writing (or other electronic form) to 1) the specific purpose for which the data will be used and 2) the length of time the data will be retained.
- **Exceptions:** neither notice or consent is required in certain circumstances.
    - Facial detection: notice and consent are not required if an entity is only figuring out whether or not a human face or body part exists in the captured facial data.
    - Protection of property/personnel: notice and consent are not required if technology is being used to protect the property or personnel of the covered entity. This exception is designed to allow entities to use facial identification to identify specific criminals or who may be a danger to personnel or who may steal the covered entity's property. For example, a retailer is permitted to use facial identification to spot convicted shoplifters who enter its store.
    - Emergency use for government: notice and consent are not required if the authorities in good faith believe that there is a serious emergency and people are in danger of death or injury. For

example, this exception would allow a covered entity to identify a suspected kidnapper without obtaining his consent. However, this does not require the covered entity to use the technology to help the government – it merely grants an exception to the notice and consent requirement. This language comes from § 2702(c) of the Stored Communications Act (SCA).

- Human remains: notice and consent are not required if facial identification is being used to identify human remains. This language is inspired by a proposed bill in Alaska, House Bill No. 72, which regulates the use of biometric information.
- Internal research and product development: notice and consent are not required if technology is only being used for internal product development, private testing or research purposes prior to the public deployment of the technology. However, companies must delete irrelevant data within 120 days unless it is used for outward-facing technology (which would then require consent). This exception allows companies to test algorithms for accuracy in development.
- Determining eligibility for enrollment: no notice or consent are required for transient use as needed to determine if the user has or has not consented to use for facial identification (the entity needs to algorithmically process the data). If the data subject is eligible and subsequently enrolled, notice must be provided.

Section 6: Use Restrictions and Prohibitions

- **Use out of context:** facial data cannot be used 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. For example, if a data subject consents to Facebook's use of her facial data for Tag Suggestions, Facebook cannot then use her facial data to reveal her identity using a CCTV camera in a club without obtaining her express consent and providing notice.
- **Discrimination and provision of benefits**: covered entities cannot use *facial characterization* to inform certain decisions about provision of goods/services.
  - Certain employment, credit, healthcare, or housing decisions: facial characterization cannot be used. This is meant to prevent demographic discrimination in employment decisions and in decisions about the provision of essential services.
  - Provision of goods or services: use of facial characterization to inform decisions is only prohibited if facial characterization is based on race, gender, ethnicity, religion, and/or age. Covered entities may use facial characterization of emotions, moods, other variables to inform decisions about provision of goods or services. However, entities may use of *facial identification* to inform decisions about the provision of goods or services; for example, a store can exclude a known shoplifter for security purposes, and under the notice and consent exception for protection of property, need not notify the shoplifter or obtain his/her consent.
  - Marketing or advertising: use of facial characterization to inform decisions about what audience to market to, or about which ad to project on a digital sign, is prohibited if the decision is made on the basis of data related to race, religion or ethnicity. Ads may nonetheless be targeted to specific individuals using *facial identification* or by using facial characterization to detect emotions, age, or gender, but this provision prevents passersby a digital sign classifying individuals based on race, ethnicity, or religion, classifications that in many cases have heightened protection under the law.
- **Price discrimination**: use of facial characterization, facial verification or facial identification to determine the price of goods or services offered to specific individuals is prohibited.
- **Consent as a precondition**: covered entities are 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 when the covered entity is a company that provides medical services (use and manipulation of images and derived data may be necessary); and to the extent necessary for an

employer to conduct background checks or implement employee security protocols. This provision is inspired by Illinois House Bill 2411, which contains proposed amendments to the Illinois Biometric Information Privacy Act.

Section 7: User Control

- **Requests to access, alter, or delete:** covered entities must allow data subjects to monitor and control the use of their facial data. Specifically, data subjects must be able to:
    - access the facial data the covered entity or business associate possesses (except for any derived or extracted data that could reveal trade secrets that pertain to the covered entity's proprietary technology); and
    - request that the entity 1) unenroll their facial data; 2) stop using their facial data for one or all forms of facial recognition technology; 3) stop disclosing the data; 4) challenge a determination when facial data has been used as a barrier to goods or services (for example, if an individual is identified as a shoplifter and escorted out of the store, he must be able to challenge the determination in case it was inaccurate); and 5) delete the data if possible.
- **Response to requests:** covered entities must respond to data subjects' requests promptly and forward requests to business associates as needed.
- **Bankruptcy or change of control:** covered entities must notify data subjects following change of control of facial data, such as a bankruptcy, merger or buy-out which changes the personnel and systems that have access to facial data.

Section 8: Disclosure, Retention, and Deletion Standards

- **Disclosure:** covered entities are prohibited from disclosing facial data of an enrolled data subject to another person, unless the disclosure falls within a set of exceptions:
    - Disclosure to business associate: a covered entity can disclose facial data to a business associate (i.e. a vendor), but only if under an agreement and for certain purposes. First, the business associate must agree to 1) comply with the Act; 2) use facial data only for the purposes for which it was engaged and not for its own independent purposes; and 3) 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. Finally, disclosure can only occur if the disclosure is necessary to provide a product or service or complete a financial transaction the data subject affirmatively requested.
    - Disclosure based on court order: covered entity is permitted to disclose if required or authorized by a court order. This provision does not intend to set the evidentiary standard.
    - Protection of property or rights: disclosure is permitted if necessary to protect property or rights of covered entities. This is inspired by § 2702(c)(3) of the SCA.
    - Emergency exception: disclosure to government entity is permitted in the case of an emergency involving death or serious injury. This is inspired by § 2702(c)(4) of the SCA.
    - Missing children: disclosure to the National Center for Missing and Exploited Children is permitted, in connection with a report submitted thereto under section 2258A or in connection with a crime under 18 U.S.C. §§ 2251–2260. This inspired by § 2702(c)(5) of the SCA, but since the covered entity won't necessarily be an electronic or remote communications service provider (who are required to report under 18 U.S.C. § 2258A), the exception is broadened so as to not condition the exception upon the report.
    - Sale/change of control: disclosure is permitted if covered entity is sold to another entity, but notice will need to be provided to affected data subjects under Section 7.

  when the covered entity is sold to another covered entity
- **Data security and retention:** covered entities are required to retain data only as long as is necessary to deliver a service; must take reasonable care to protect data and systems against unauthorized

access, shall develop and maintain adequate security measures in accordance with NIST standards, and will use encryption at rest and in transit.

- **Disposal:** Covered entities and business associates will not retain data longer than necessary for the original purpose it was collected. Data must be deleted within 120 days. This is inspired by Section 18.13.230 of House Bill No. 72, a proposed statute in Alaska regulating biometric identity systems.
- **Data Breach Notification:** Covered entities must disclose what sensitive data of a data subject was compromised by a data breach if the data breach may lead to a risk of identity theft or fraud against the data subject, and so long as the cost to notify the data subject does not exceed $1000, and so long as the contact information is accessible.

Section 9: Enforcement

- The Federal Trade Commission is charged with enforcement of this Act against both covered entities and business associates for violations of Sections 4, 5, 6, and 7 of the Act. There is no private right of action available.

Section 10: Consumer Education

- The Federal Trade Commission is required to create and maintain a public webpage to educate the general public about the tools available to express preferences regarding the collection, enrollment and use of personal information for commercial face recognition purposes and how to use such tools.

Section 11: Penalties

- 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. This is inspired by Texas Business and Commerce Code § 503.001, regulating the capture or use of biometric identifiers, which does not provide for a private right of action, but rather allows the State Attorney General to impose a $25,000 penalty for each violation. This is significantly greater than the $10,000 per violation under the FTC Act, but seems reasonable to incentivize compliance since there is no private right of action available.

Section 12: Severability

- If any provision of the Act or its application is held invalid, the invalidity does not affect other provisions or applications of this Act that can still be enforced without the invalid provision. This is meant to ensure that the Act remains intact even if some portion of the law is struck down.

Section 13: Preemption

- This Act preempts only the provisions of state or local law that conflict this Act's provisions, but does not preempt laws that provide data subjects with greater levels of protection.

Section 14: Construction

- This provision ensures that this new legislation does not affect application of any overlapping provisions of the Gramm-Leach-Bliley Act or HIPAA and their associated rules. For example, to the extent that HIPAA regulates the use or disclosure of certain biometric identifiers that could overlap with those regulated by this Act, this statute will not interfere with HIPAA's enforcement.