Discussion Draft
Privacy Best Practice Recommendations For Commercial Facial Recognition Use

These Privacy Best Practice Recommendations for Commercial Facial Recognition Use serve as general guidelines for covered entities.

The fundamental principles underlying the recommendations are based on the Fair Information Practice Principles (FIPPs)[1].

It is left to implementers and operators to determine the most appropriate way to implement each of these privacy guidelines. Given the numerous existing uses in widely different applications (such as authentication, social media and physical access control), as well as potential uses, specific /detailed practices are not feasible or practical across this wide spectrum.

These best practices are intended to provide a flexible and evolving approach to the use of facial recognition technology, designed to keep pace with the dynamic marketplace surrounding these technologies. This document is intended to provide a general roadmap to enable entities using facial recognition technologies by recognizing differing objectives, risks and individual expectations associated with various applications of these technologies.

These principles do not apply to the use of a facial recognition for the purpose of aggregate or non-identifying analysis. For example, when facial recognition technology is used only to count the number of unique visitors to a retail establishment or to measure the genders or approximate ages of people who view a store display (for marketing research purposes), those practices are outside the scope of these principles.

These best practices do not apply to security, law enforcement, national security, intelligence or military uses, all of which are beyond the scope of this document.

Definitions

Covered Entity – Any person, including corporate affiliates, that collects, stores, or processes facial template data. Covered entities do not include governments, law enforcement agencies, national security agencies, or intelligence agencies.

[FOR CONSIDERATION: *Unaffiliated Third Party* – Any person other than (1) a user of a covered entity's products or services; (2) a covered entity's employees; or (3) a vendor or supplier to a covered entity when such vendor or supplier is used to provide a product or service related to facial template data.**]**

Facial Template Data – A unique facial attribute or measurement generated by automatic measurements of an individual's facial characteristics, which are used by a covered entity to uniquely identify an individual's identity. Data that has been

[1] FIPPs are a widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. These principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations.

reasonably de-identified[2] and the underlying document from which the data came[3] is not facial template data and therefore is not covered by these best practices.[4]

Facial Recognition Technology – A computer program used to compare the visible physical structure of an individual's face with a stored facial template.

Transparency

- Covered entities are encouraged to make available to consumers, in a reasonable manner and location, privacy policies ~~highlighting~~ describing such entities' ~~policies~~ practices regarding collection, storage, and use of facial template data. Covered entities are encouraged to update their privacy policies when they make material changes to their facial template data management practices. The specifics of such privacy policies will depend on the application, given the widely different uses of the technology. Generally, ~~the policy~~policies should describe, as practicable:
  - the reasonably foreseeable purposes for which the covered entity collects and shares facial template data or uses facial recognition technologies;
  - the covered entity's data retention and de-identification practices;
  - information on how to submit complaints or concerns, and if the entity offers the ability to review, correct, delete, or de-identify facial template data, the procedure to accomplish such actions;
  - how the covered entity responds to requests for facial template data from domestic and foreign law enforcement agencies.
- Where facial recognition technology is used on a physical premises that a covered entity controls, such entity is encouraged to provide concise notice to consumers that facial recognition technology is present, and, if contextually appropriate, where consumers can find more information about the covered entity's use of facial recognition technology~~'s use~~.

- **Developing Good Data Management Practices**
- ~~In drafting notices~~When ~~consider~~ covered entities ~~should consider issues like~~formulate their facial template data management practices, and before covered entities deploy facial recognition technology, they are encouraged to consider the following factors:
  - Voluntary or involuntary enrollment;

[2] De-identification of data—removing information from data that could reasonably be used to identify an individual person—is a subject of intense debate. These best practices do not endorse any particular method of de-identification or set a standard for when data has been adequately de-identified. Instead, ~~commercial~~ covered entities should use their expertise, taking into account the type and use of personal wellness data and using the technical tools available to them, to determine how to de-identify such data.

[3] For example, the photograph or recording of a face is not facial recognition data~~e~~.

[4] For example, when facial recognition technology is used only to count the number of unique visitors to a retail establishment or to measure the genders or approximate ages of people who view a store display (for marketing research purposes), those practices are outside the scope of these principles.

Comment [A1]: CTA: It may be sufficient to add a footnote to the first sentence that clarifies that we are discussing data *derived from* an image rather than the image itself. The existing language of the definition already has words, like "generated by automatic measurements," that imply that we are not talking about images themselves.

Comment [A2]: Because Transparency is such a widely accepted principle, and privacy policies are common, it may be worth using "should" for this bullet only.

Comment [A3]: CTA: Recommend deleting this sentence; some of its ideas are reflected in the preamble, and we already couch the transparency principle in terms of reasonableness and "as practicable".

Formatted

Formatted: Font: Bold

Formatted: Normal, Indent: Left: 0.25", No bullets or numbering

Comment [A4]: CTA: Created a new section for this bullet because it seemed incongruous with the Transparency principle. I think it is better articulated as a set of factors covered entities should consider, whether covered entities discuss them in the privacy policy or not. I welcome feedback.

- Type of non-facial recognition sensitive data being captured and stored;
- How that data will be stored and used;
- Whether facial template data may be used to determine a person's eligibility for, or access to, employment, healthcare, financial products or services, credit, housing, or insurance;
- Risks and harms, if any, this process may impose on the enrollee;
- Reasonable consumer expectations with regard to the use of the data.

Data Minimization

- Covered entities are encouraged to only collect and retain facial template data that is reasonably necessary to provide their services or otherwise meet legitimate business objectives.

Purpose Specification

- Covered entities are encouraged to specify for what purpose(s) their facial recognition technologies are being used.

Openness

- Covered entities are encouraged to provide a mechanism so that users for whom data is collected can request information about data retained on them.

Use Limitation

- When appropriate, covered entities are encouraged to limit access to facial template data to certain specified individuals or applications.
- Covered entities that use facial recognition technologies to determine an individual's identity are encouraged to provide the individual the opportunity to control the sharing of their facial template data with an unaffiliated third party that does not already have this information.

Security Safeguards

- Covered entities are encouraged to take reasonable steps to secure facial template data.
- Covered entities are encouraged to take reasonable steps to periodically assess their facial template data protection measures ~~(~~consistent with the sensitivity of the use of the data~~)~~.

Data Quality

- Covered entities are encouraged to take reasonable steps to maintain the accuracy and completeness of the facial template data they collect.
- Covered entities are encouraged to provide a mechanism for correcting facial template data, and if appropriate given context, facilitate re-enrollment or data removal appropriate for the context.

Problem Resolution and Redress

- Covered ~~Commercial~~ entities are encouraged to provide a description of the process consumers can follow to contact the entity regarding its use of facial template data.

Comment [A5]: Addressed in the Transparency principle.

CTA: In general, we prefer not to place restrictions on data itself, but on uses, so we would prefer to delete this section entirely.

Comment [A6]: Addressed in the Transparency principle.

CTA: If we keep this section, we suggest tying it back to the privacy policy. Also, we suggest replacing "specify" with "describe" to be consistent with the updated Transparency principle.

Comment [A7]: Addressed in the Transparency principle.

Comment [A8]: CTA: This looks like a statement about data security. Is it redundant with the Security Safeguards principle?

Comment [A9]: CTA: "Control" seems vague. Suggest we use "consent to".

Comment [A10]: CTA: suggest deleting this phrase because it's redundant – there's no reason for a covered entity to transfer information to a third party that already has it, and therefore no reason to obtain consent.

Comment [A11]: CTA: For consistency, it may be worth writing something closer to the FTC's formulation of this: "Covered entities should take measures to protect covered data by implementing a program that contains reasonable administrative, technical, and physical safeguards appropriate to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the facial template data."

Comment [A12]: CTA: We're not sure what this principle means as a practical matter. Are we encouraging covered entities to affirmatively test the validity of the data they hold? Or does this mean that companies should keep their databases "clean" by removing incomplete data? We're not sure either requirement would make ...

Comment [A13]: Addressed in the Transparency principle.

CTA: "Context" is used twice here. Also, we may need to reconcile this language with t ...

Comment [A14]: Addressed in the Transparency principle.

- Covered ~~Commercial~~ entities are encouraged to publish whether they permit requests for revocation, deletion, or change of facial template data used for identification purposes.