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 applications, 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.

Unaffiliated Third Party – Any person other than (1) a user of a covered entity's products or services; (2) a covered entity's employees; (3) an entity under common control or ownership with a covered entity; or (4) 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 or authenticate an

[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.

individual when the individual accesses a system or account. Data that has been 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 to confirm an individual's claimed identity or to uniquely identify an individual.

Security Applications- Loss prevention and other applications intended to detect or prevent shoplifting, fraud, misappropriations or other malicious and criminal activities.

Transparency

- Covered entities are encouraged to make available to consumers, in a reasonable manner and location, policies or disclosures describing such entities' practices regarding collection, storage, and use of facial template data. Covered entities are encouraged to update their policies or disclosures when they make material changes to their facial template data management practices. Generally, policies or disclosures should describe, if applicable, and/or in the appropriate context:
    - the reasonably foreseeable purposes, or examples, 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;
    - and, if the covered entity offers the ability to review, correct, or delete facial template data, the process to accomplish such actions.
- 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.

Developing Good Data Management Practices

- When covered entities formulate their facial template data management practices, and before covered entities deploy facial recognition technology, they are encouraged to consider the following factors:

[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, 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.

[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.

- Voluntary or involuntary enrollment;
- 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.

Use Limitation

- 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 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." 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.
- When appropriate, covered entities are encouraged to consider whether these measures should include limiting the individuals or applications that may access facial template data.

Data Quality

- Covered entities are encouraged to take reasonable steps to maintain the integrity[5] of the facial template data they collect.

Problem Resolution and Redress

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

[5] In this context, integrity refers to the assurance that the covered entity that create the facial template data is trusted.