Discussion Draft
Privacy Best Practice Recommendations
For Commercial Biometric Use

These Privacy Best Practice Recommendations for Commercial Biometric Use serve as general guidelines for commercial entities.

The fundamental principles underlying the recommendations are based on the Fair Information Practice Principles (FIPPs)[1], notably transparency and data security.

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 recommendations are intended to provide a roadmap that will enable users and customers to tailor appropriate privacy practices to their specific contexts, taking into consideration the following factors (as well as others noted throughout):

- Application
- Risk and consequence of abuse
- Personal non-biometric data use
- Purpose of the undertaking
- Reasonable expectations of people

Please note these recommendations do not apply to physical security, law enforcement, national security, intelligence or military uses, all of which are beyond the scope of this document.

<u>What are biometrics?</u>

Biometrics are physical or behavioral characteristics which can be used to identify unique individuals. Biometric technologies measure these characteristics electronically and match them against existing records to create a highly accurate identity management system.

[1] FIPPs are the 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.

Facial recognition is one such technology. It uses the layout of facial features and their distance from one another for identification against a "gallery" of faces with similar characteristics.

Transparency

Transparency encompasses two (2) key elements: (i) the existence and availability of privacy policies, and (ii) notice that facial recognition technology is used. The specifics, as noted above, will depend on the application, given the widely different uses of the technology.

General Identity

When biometric technology is deployed but will not be used for individual identification, as for example, when used to just detect and count people or to estimate the gender and age of a person observing a store display (for marketing research purposes), a general notice appropriate to the context is recommended.

Individual Identity

Individual Identity is when a facial recognition system is used to compare the template generated from a face image with a template generated from a previously enrolled face image.

In such applications, Individual Identity enrollment notices are dependent on the application, taking into consideration such issues as:

- Voluntary or involuntary enrollment;
- Type of non-biometric personal data being captured and stored;
- How that data will be stored and used;
- Risks and harms, if any, this process may impose on the enrollee;
- Reasonable expectations with regard to the use of the data.

Collection Limitation Principle

- Identification of the type of biometric that is captured/stored and its relevance to the purpose for which it is being captured/stored;
- Identification of the non-biometric data for that individual that is being associated with the biometric data;
- Description of the period of retention (preferably a defined length) or the policy that determines the period of retention.

Purpose Specification Principle

- Specification of why the information is being captured and limiting its use to those purposes.

Openness Principle

- Providing a mechanism so that users for whom data is collected can request a current record of any data retained on them.

Use Limitation Principle

- Limitation of access to the data to certain specified individuals or applications;
- Restricting third party access unless disclosed and necessary to the original purpose or application as stated in the Purpose Specification or in response to a legal order.

Protection of Data

Security Safeguard Principle

- Protection of any information collected or retained (whether biometric or otherwise) with the implementation of cyber-security best practices;
- Disassociating the data to the extent allowed by the applications to limit exposures if a cyber or other privacy breach does occur;
- Encryption of data at rest and data-in-motion to limit exposures in the event of a breach.

Data Quality Principle

- Maintaining the accuracy and completeness of the data;
- Providing a mechanism for correcting the data, appropriate for the context, for re-enrollment or data removal.

Accountability Principle

- Adhering to these best practices recommendations by maintaining audit logs sufficient to the published purposes;
- Conducting periodic audit reviews by an independent audit.

Problem Resolution and Redress

Make the following available to consumers:

- Description of the process consumers can follow if they believe that the privacy of their personal information has been compromised;
- Contact information for the person or organization to which such concerns could be escalated where that is appropriate;
- Possible redress options, including revocation, deletion, or change of biometrics used for identification purposes.