INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

IBIA Privacy Best Practice Recommendations
For Commercial Biometric Use

The IBIA's Privacy Best Practice Recommendations for Commercial Biometric Use incorporate general guidelines for commercial use of biometrics, leaving it to implementers and operators to determine what is most appropriate given the application, the risk and consequence of abuse, the personal non-biometric data used, and the purpose of the undertaking.

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

General Notice

General Identity

- A general notice is recommended when biometric technology is deployed but will not be used for individual identification.
- An example is using facial recognition technology to just detect and count people or to estimate the gender and age of a person observing a store display (for marketing research purposes).

Individual Identity – Privacy Opting-In or Out

- Individual enrollment notices are application driven, taking into consideration issues such as:
    - Voluntary or involuntary enrollment;
    - Type of non-biometric personal data being captured and stored;
    - How that data will be used;
    - Extent of notice to individuals that will be provided;
    - Risks and harms, if any, this process may impose on the enrollee.
- To illustrate the differences that are involved, compare:
    - A social media site where one can easily opt-in by clicking a box;
    - An office building where entering amounts to an opt-in (anything else is impractical);

- A retail establishment with a reward program or marketing campaign, where entry alone is a base requirement for its use, or where shoplifting is of concern.

Privacy Policy Notice

We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed below be included.

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 limitation on its use to those purposes.

Data Quality Principle

- Maintaining the accuracy and completeness of the data;
- Providing a mechanism for correcting the data, including a contact point (with human attendant) for re-enrollment or data removal (IBIA believes that self-service systems for initial- or re-enrollment are susceptible to fraud).

User 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.

Security Safeguard Principle

- Protection of any information collected or retained (whether biometric or otherwise) with good cyber-security 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.

Openness Principle

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

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

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

IBIA is a non-profit trade group that advocates and promotes the responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organizations, and governments. www.ibia.org