International Biometrics+Identity Association

IDENTIFICATION TECHNOLOGY & PRIVACY POLICY PRINCIPLES

The International Biometrics + Identity Association is a strong advocate for ethical uses of technology, particularly related to identity technology. These Privacy Policy Principles provide general guidelines for commercial use of biometric technologies and data, while allowing implementers and operators to customize their approaches based on the biometric technology application(s) used and the potential risks and benefits associated with the given use-case.

IBIA recommends implementers and operators of commercial biometric technology develop and publish privacy policies incorporating the following principles:

Collection Limitation Principle

- Identifying the type of biometric data captured or stored and the purpose for which it is captured or stored;
- Identifying the non-biometric data for that individual that is being associated with the biometric data;
- Describing the retention period and, if applicable, the policy that determines the retention period.

Purpose Specification Principle

- Specifying why the information is being captured and whether that information will be used for other purposes.

Data Quality Principle

- Maintaining the accuracy and completeness of the data;
- Providing a mechanism for correcting identified errors in the data, including a point of contact with human attendant for re-enrollment or data removal.

User Limitation Principle

- Only permitting authorized individuals, entities, and technological applications to access biometric data;

Security Safeguard Principle

- Protecting any information collected or retained with robust cybersecurity and data protection practices, such as:
    - Anonymizing and/or aggregating the data to the extent allowed by the applications, in order to limit exposures if a data breach does occur.
    - Encrypting data-at-rest and data-in-motion to limit exposures in the event of a breach.

Openness Principle

- Providing a mechanism so that individuals whose data is collected can request a current of record of their data.

Accountability Principle

- Maintaining audit logs sufficient to the published purposes;
- Conducting periodic audit log reviews by an independent audit.

Problem Resolution and Redress Principle

- Describing the process consumers can follow if they believe the privacy of their personal information has been compromised and publishing the contact information for the individual or organization to which such concerns should be addressed;
- Publishing possible redress options, such as revocation, deletion, or change of biometrics used for identification purposes.

IBIA is dedicated to the ethical use of biometrics and welcomes opportunities to participate in multi-stakeholder dialogues and to serve as a resource to policymakers and media outlets interested in discussing and working to address these important topics.