Principles for Biometric Data Security and Privacy

Principles for Biometric Data Security and Privacy: Landscape

IBIA's Principles for Biometric Data Security and Privacy are intended to be useful guidelines to biometric system developers and users of the technologies. The purposes are to assure the public that their sensitive biometric information will be handled transparently and respectfully to help rebuild trust and allay concerns about the collection and use of this personal information.

Data Vulnerability

Vulnerability of data has become an unwelcome part of everyday life. The rise of the digital age, with the emergence of big data, has both defined the security and privacy challenges of protecting personal data and constrained our ability to respond to those challenges. Abundant troves of sensitive personal data are available online at no, or low, cost. Public records, no longer protected by obscurity and the cost of finding and copying them, are readily available online with a few clicks. We regularly post and communicate personal information online.

Breakdown of Trust in Stewards of our Information

We have been conditioned by an endless series of breaches by government, banks, and virtually everyone else to neither trust nor have comfort in the stewards of our information. A May 2019 consumer survey by F-Secure found that 71% "feel that they will become a victim of cybercrime or identity theft" and that 51% of consumers have had a family member "affected by some form of cybercrime."

This new environment has given rise to calls, on a scale not previously seen, to protect the security and privacy of our personal data. Sometimes, even calls to not collect it at all, ignoring the benefits of the new systems that enable the collection of data.

Biometric Data in Society Today

Biometric data is a form of personal data that is increasingly used throughout society. There are differing perspectives as to whether biometric data is less or more sensitive than other personal data. Technologists are often more sanguine about use of biometrics than the public who have generally had far less exposure to biometrics (although the use of biometrics for our mobile devices is changing that).

Biometric technologies are increasingly used throughout society by government, the military, law enforcement, commercial, and consumer sectors. All indications are the use of biometrics will significantly increase. The need to know the identity of people with whom we interact continues to grow -- for example, in aviation, access to buildings and critical infrastructure, digital and mobile devices, in banking, healthcare, schools and countless other daily transactions etc. The accuracy continues to improve and cost continues to decline.

Restoring Trust by Protecting Personal Data

All personal data, including biometric, is deserving of protection. The principles outlined below will aid in providing that protection for biometric data. Trust, once lost, is at best difficult to regain and IBIA hopes these principles will help restore that trust.

As systems incorporate biometric technologies, careful attention must be paid to respecting the individual and data, including notice and consent. It is unproductive to address protection of biometric information without acknowledging that notice and consent are important issues. A full treatment of notice and consent is beyond the scope of this paper, however, and IBIA is preparing a separate paper on these fundamental issues.

There are numerous and diverse applications of the biometric technologies, and many more will emerge over time. For that reason, it must be left to the implementer of a specific application to evaluate how to appropriately apply these general principles, taking into consideration the:

- Application
- Purpose of the application
- Risks and consequences of abuse
- Personal non-biometric data used

Principles for Biometric Data Security and Privacy[1]

Respect the Person and Related Data:

- Personal data, including biometrics, should not be collected without the subject's knowledge. There will sometimes be exceptions for national security and public safety.
- In the absence of a legal mandate, identifying personal biometrics should not be collected and retained without the individual's consent to the collection (the kind of consent may vary depending on the application and factors noted above), the authorized use, and any further dissemination.
- Effective notice and consent is to be conveyed with brief written statements, in ordinary language, readily comprehended by the notified or consenting person. Lengthy fine print pro-forma statements, such as most software license agreements, real estate documents, and loan documents do not meet this principle.

1 These principles can easily become applicable to all forms of personal data.

Transparency:

- Prepare and make readily available a written statement of what biometric information is being collected, what it will be used for, with whom it will be shared, and for how long it will be retained.
- The information should be brief, easy to read and understand, and easily accessible.
- If there is concern over potential embarrassment from sharing such information revise the policy to eliminate the concern.
- Enforce the policy.
- Consider incorporating mechanisms for individuals to redress their collected information and potentially request for deletion/ destruction of their biometric data.

Data Quality:

- Ensure the quality, accuracy and completeness of the data.
- Provide mechanisms for correcting data, including a human contact point for re-enrollment or data removal (self-service systems for initial / re-enrollment are at risk of fraud).

Data Retention:

- Only retain data genuinely needed for the stated application.
- Retain data in compliance with a formal published schedule.
- Limit retention to a period essential to the purpose for which retained.
- For all commercial and civil government applications, protect the biometric data retained by using biometric one-way template transformation.
- Encrypt any raw data collected, at rest or in motion. Delete raw biometric data following template transformation (this may vary depending on the application and factors noted above).

User Limitation:

- Limit the access of data to specified individuals, or applications, which require the information to perform their functions.
- Restrict third-party access unless explicitly disclosed and necessary to the original purpose/ application as stated in the System's Purpose Specifications or in response to legal orders.
- Notify the individuals who may have their data breached in the event of unauthorized access.

Security Safeguard:

- Protect all collected/ retained personal data, whether biometric or biographic, with adequate methods of cyber-security tailored to the type of data, particularly encryption of the data at rest and in transit.
- Disassociate/anonymize all data to the highest extent allowed by the application to limit data exposure in the event of a security breach.

Accountability:

- Maintain audit logs sufficient to the published purposes.
- Conduct adequate numbers of periodic independent audit reviews, not less than annually.

Problem Resolution and Redress:

- Describe all processes in terms that consumers can follow in the event they believe that their personal information has been compromised.
- Publish all contact information for the person/ organization to which consumer concerns should be addressed.
- Publish all possible redress options, including revocation, deletion, or change of biometric modalities used for identification purposes.

About IBIA: IBIA is the leading voice for the biometrics and identity technology industry. It advances the transparent and secure use of these technologies to confirm human identity in our physical and digital worlds. #identity matters

#identitymatters

International
Biometrics+Identity
Association

1325 G Street, NW, Suite 500
Washington, DC 20005

202.888.0456 | **IBIA.ORG**