International Biometrics+Identity Association

ETHICAL USE OF BIOMETRIC TECHNOLOGY

In 2019, IBIA published our Principles for Biometric Data Security and Privacy, which aim to provide useful guidelines to biometric technology developers and users that would help build public trust. We remain committed to upholding these principles, and we apply them when considering important questions about how to ethically and effectively use biometric technologies. Below, we explain that, to us, using biometric technologies ethically means:

1. **Respecting the person and related data;**

Work to use biometric technologies in a way that protects privacy and minimizes bias. Despite the major strides the industry has made in improving biometric technologies' overall accuracy and accuracy across demographic groups, concerns about privacy and promoting racial and broader social justice remain vital to address. At a minimum, developers and users should work to mitigate the risk of using biometric technologies in a way that perpetuates or exacerbates systemic bias in societal institutions and structures. Ideally, developers and users should work to use biometric technologies in a way that actively reduces that bias and enhances the privacy of marginalized communities. Combatting systemic biases is a multifaceted, complex challenge that biometric technology developers and users certainly cannot overcome on their own. But, developers and users can work to ensure their biometric technologies are accurate across demographic groups and are not used for discriminatory purposes or with discriminatory intent.

Procure and deploy only biometric technologies that are sufficiently accurate for the given use case. In law enforcement and national security settings, use only the most accurate biometric technologies according to established, third-party evaluations, such as NIST and DHS S&T tests, that measure overall accuracy and accuracy across demographic groups.

2. **Upholding a commitment to transparency;**

Communicate with data subjects about 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. Biometric technology users should provide notice and obtain consent for all but a narrowly defined set of national security and public safety situations, and communications should be in plain language accessible and understandable to the average person.

Provide the public with an opportunity to provide input on public-sector biometric technology programs. Public-sector biometric technology users should notify the public of planned biometric technology procurements and deployments, provide the public with an opportunity to comment on and ask questions about the planned procurements and deployments, and respond to public comments and questions.

3. **Working to secure biometric data;**

Minimize data. Biometric technology developers and users should not collect and retain more data than they need to achieve the purpose for which they collected the data. They should examine data quality to assess compliance with data quality standards, and they should delete data that is of insufficient quality.

Store data in the lowest-risk appropriate format. Biometric technology developers and users should encrypt data in transfer and at rest and, when appropriate, should anonymize and aggregate data, rather than retaining individual data points with personally identifiable information.

Limit which individuals can access and use biometric systems. Biometric technology developers and users should employ physical and digital access control measures that aim to ensure that only trained and authorized persons can use the biometric systems.

Monitor and only allow authorized transfers of biometric data from one system to another. Because data breaches often occur when data is transferred to an unsecure system, device, or network, we recommend that biometric technology developers and users keep track of data flows and restrict data flows to third-party systems and users.

4. **Promoting accountability; and**

Facilitate both internal and external oversight of biometric technology deployments. Biometric technology users should publish publicly available privacy policies and should complete and publish Privacy Impact Assessments (PIAs) existing and new biometric programs. Biometric technology developers should internally test their algorithms' and full solutions' performance, and they should also submit their algorithms and systems to established third-party evaluators, such as NIST and DHS S&T, for testing.

Adhere to industry standards. Biometric technology developers and users should work to ensure that biometric systems and inputs adhere to applicable standards, such as those governing image quality for facial recognition systems.

Require biometric system operators to complete training on proper use. Biometric technology developers and users should work together to develop and provide training to individuals operating biometric systems. The training should aim to ensure that everyone operating biometric systems is capable of doing so effectively and responsibly.

Work with policymakers to develop biometric legislation that facilitates appropriate reporting, oversight, and other accountability measures. Promoting accountability through voluntary actions and disclosures is helpful and important, but IBIA also supports efforts to further strengthen accountability through legislative and regulatory frameworks for biometric technologies. To help ensure that such frameworks reflect a nuanced and comprehensive understanding of biometric technologies and the risks and benefits that the technologies can produce in different settings, biometric technology users and developers should make themselves available to work with policymakers.

5. **Resolving and redressing any problems that arise.**

Conduct operational performance assessments when deploying biometric technologies and on a regular basis thereafter. Monitoring the system's performance in operational conditions is important to detecting and rectifying any issues that may arise. Developers and users should work together to proactively address performance challenges when deploying and operating biometric technologies.

Regularly upgrade biometric systems to ensure use of the most accurate, secure, and privacy-protective technologies available. As recent NIST and GAO reports have demonstrated, the biometrics industry has made rapid technological advances and has grown tremendously in recent years. To resolve and reduce problems related to inaccurate match results, biometric technology users should make every effort to use the most up-to-date technologies, and biometric technology developers should aim to communicate about upgrades as soon as they are available.

Communicate with biometric technology operators and data subjects about data protection and cybersecurity issues, data protection best practices, and what to do in the event of a data breach. Users should provide clear, accessible information to individuals operating biometric technologies and data subjects about recommended practices to safeguard biometric data and what to do if they think that biometric data has been compromised.

Have humans review the biometric system's match results when making important decisions. We recommend keeping a human in the loop to help rectify any inaccurate match results and help prevent any system performance issues from negatively impacting data subjects.

Accept personal responsibility. Ultimately, people are responsible for how we use biometric technologies. When biometric technologies are involved in a problematic situation, solely blaming the technologies can harmfully and counterproductively distract attention from the deeper societal issues affecting the situation.

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.