Facial Recognition: Technology, Trust, and the Path to Ethical Deployment

ACCESS CONTROL JUSTICE & PUBLIC SAFETY TRAVEL IDENTITY – NORTH AMERICA

POSTED ON 06.09.26

Over the past decade, facial recognition has become an increasingly important component of modern identity and security systems. From supporting investigations to streamlining border control and access management, its operational value is well established. Yet its adoption continues to raise legitimate questions around fairness, accountability, and societal acceptance.

Drawing on extensive experience of supporting public safety and identity programs worldwide, IDEMIA Public Security understands performance alone is not enough. Trusted facial recognition must be built on three pillars: accuracy, equitable performance, and governance.

Independent evaluations conducted by national agencies, standards bodies, and scientific institutions have shown modern facial recognition can achieve high levels of accuracy and equitable performance across diverse populations when assessed under clearly defined conditions. These assessments demonstrate that effectiveness depends not only on algorithm design but also on factors such as image quality, threshold configuration, operator procedures, testing methodologies, and ongoing monitoring.

This distinction is critical. Concerns commonly associated with facial recognition—including bias, misidentification, and erosion of public trust—may arise when systems are deployed without appropriate governance, rigorous testing, performance evaluation, and safeguards.

For this reason, responsible deployment must extend beyond algorithmic performance and be anchored in clearly defined principles. The Biometrics Institute articulates this approach through its widely recognized Three Laws of Biometrics:

1. **Policy comes first:** Any use of biometrics is necessary and proportionate, with human rights, ethics, and privacy at its core.
2. **Process follows policy:** Safeguards ensure decisions are rigorously reviewed, operations are fair, equity and inclusion are addressed, and accountability is maintained.
3. **Technology is guided by policy and process:** Organizations must understand their algorithms, systems, data quality, and operating environments to mitigate limitations and risks.

Together, these principles reinforce a fundamental point: Facial recognition must not function as an autonomous decision maker. It is a decision support tool, operating within a human, legal, and institutional framework.

In practice, outcomes depend as much on training, threshold settings, data quality, and governance structures as on the algorithm itself. Human oversight remains essential, particularly in sensitive environments such as law enforcement and border security, where biometric technologies are intended to assist, not replace, professional judgment.

As adoption accelerates globally, the conversation is shifting from whether facial recognition works to how it can be governed and deployed at scale with appropriate oversight. This requires continuous evaluation, clear policies, and precise allocation of responsibility between technology providers and end users.

Facial recognition has reached a level of maturity where its benefits are obvious. The priority now is to ensure its use remains controlled, accountable, and trusted across the communities it serves.

With decades of operational experience across public safety, border management, and identity programs, IDEMIA Public Security supports this approach by combining high-performing and rigorously evaluated biometric algorithms with operational expertise, end-to-end system integration capabilities, and a deep understanding of real-world and regulatory environments. This enables agencies to deploy facial recognition solutions that are not only effective but also transparent, responsible, and aligned with legal and public expectations.