IDEMIA'S Principles for the Responsible Use of Facial Recognition Technologies

The maturation and convergence of a group of key technologies has made the need for trusted digital identification critically important.

Digital identification improves security, protects our personal devices, ensures a seamless travel experience, generates leads for solving crimes, and helps identify individuals' intent on doing harm. Identity is a vital enabler for commerce, as well as for the law enforcement, homeland, and national security communities that investigate crime, secure our communities and protect our nation.

That is why IDEMIA—one of the leading providers of facial recognition solutions—has committed to principles that guide our deployment of this vital technology in our customer engagements. We believe that that these principles should apply to any implementation of facial recognition tools, in both commercial and governmental settings, and that the federal government should put strong rules in place to set clear national standards governing its use.

This will help ensure that this technology is used in a responsible manner and aid public officials in securing the public interest.

IDEMIA believes that to ensure accuracy and fairness, a human-driven verification process is necessary to assess potential matches discovered by facial recognition solutions. While tests conducted by the National Institute for Standards and Technology (NIST) and at the Department of Homeland Security's Biometric Rally show that IDEMIA's algorithms return highly accurate results, we recommend that our customers use a proven process to ensure that the technology produces accurate leads and recognize that those leads are just one element of the investigative process. This process includes a software-based algorithm *and* human-driven assessment that relies upon traditional investigatory procedures and corroborating documents. With regard to law enforcement, facial recognition matches are leads only—*investigators and analysts must be the ones to determine viability of a lead*.

IDEMIA believes that training is the foundation of the match process. We believe everyone involved in the matching process should undergo a rigorous training program that incorporates human physiology and the latest investigatory techniques. IDEMIA offers training to our customers on a regular basis and believes that responsible vendors should do the same to ensure that usage and adoption adheres to the highest standards.

IDEMIA believes that bias has no place in facial recognition, or any other, identification solutions. We understand that there are legitimate concerns that facial recognition could disproportionately impact minority communities, and we work to continually improve the precision of our solutions to eliminate bias. We believe that investigators and analysts should undergo rigorous training to reduce implicit bias. The goal of our solutions is to help our customers make an accurate match—*bias in any form makes it harder to achieve that goal.*

IDEMIA believes that data storage should be optimized to ensure privacy and security. IDEMIA's solutions seek to limit data stored in central repositories and that templates—rather than original imagery—should be used whenever possible. This distributed data approach helps improve privacy and data security over the long term. IDEMIA believes that our customers' data is precisely that. IDEMIA engages with this data only with the explicit permission of our customers to troubleshoot system performance.

IDEMIA believes in transparency. IDEMIA believes that its customers should develop and publish explicit policies that describe how facial recognition data is obtained, used and secured. We believe proper training and re-assessment of the policy is vital for compliance purposes and to ensure that the technology is used for expressly stated purposes. For law enforcement, we believe the US Department of Justice's Face Recognition Policy Development template offers a comprehensive inventory of good policy practices including the following areas:

- **Administration and Compliance** – Facial recognition policies should be written in a clear and understandable manner, and there should be a point of contact for inquiries, errors and complaints. The policy should describe who it covers, how often it is updated, and the procedures for ensuring compliance.

- **Search procedures** – The policy should lay out appropriate search procedures, how facial recognition images are obtained, how image quality is ensured, whether the system covers live *and* recorded images, how the image repositories are used, and procedures for mobile searches and sharing with other agencies. Importantly, the policy should make clear that potential matches do not represent positive identification, but should serve as investigative leads only. Some customers set their systems to never return a single candidate match to ensure it is not used for positive identification. This policy makes sense in many cases.

- **Public access** – The policy should delineate whether facial recognition data is a public record subject to the US Department of Justice's Freedom of Information Act or other public records act requests under applicable law.

- **Data security** – The policy should describe the physical, procedural, and technical safeguards for ensuring the security and privacy of all personally identifiable information, including facial recognition information, as well as procedures in the event of a breach of systems housing such data. It also should detail the requirements for ensuring that personally identifiable information be stored in a secure format and secure environment, as well as document which personnel are authorized to access data.

- **Retention** – There should be a clear retention policy for files contained in the image repository, as well as search images, consistent with traditional investigatory practices. Data should be retained only so long as it has demonstrable, practical value.

- **Training** – Training on the appropriate use of the technology should be conducted for all personnel who interface with facial recognition systems. Regular assessment of compliance with policies based on this training, consistent with the published policy, should be conducted.

IDEMIA recognizes that we have a duty to ensure that our technologies are used in a responsible manner and consistent with our values. We will continue to engage with government leaders about appropriate and effective use of the technology aligned with these values.