



SIX PRINCIPLES FOR DEVELOPING AND DEPLOYING FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is defined for the purpose of these principles as technology that can be used for the personal identification of individuals in images, both still and video. We distinguish the use of technology for personal identification from related computer vision technologies that estimate gender or age, for example, but do not lend themselves to personal identification. We believe that the personal identification capabilities of facial recognition technology have unique attributes that require special consideration. These attributes include the ability to capture facial images remotely, without knowledge or consent, and the technology's emerging capability to eliminate practical personal obscurity at a scale not previously achievable.

1. **FAIRNESS:** We will work to develop and deploy facial recognition technology in a manner that strives to treat all people fairly.

We seek to develop and deploy facial recognition technology in ways that minimize and mitigate unfair bias against any individual or group, while recognizing that it is not possible to guarantee that any technology is completely bias free. We aim to employ diverse teams in the design, development and testing of our facial recognition technology, to help ensure the technology reflects the diversity of the world in which we live. We will develop processes and tools to systematically assess the data we use for training, testing and benchmarking our facial recognition technology to help ensure it has appropriate representativeness and quality. We will create appropriate bias assessment tools to analyze the operation of our facial recognition technology, and we will use the output of those tools to improve our models over time. For customers using our facial recognition technology, we will publish guidelines and best practices to help them deploy the technology in scenarios and ways that minimize the potential for unfair bias. We will also encourage our customers to undertake their own rigorous testing of the technology in the scenario in which they intend to use it, to assess the potential for bias that may arise in that specific scenario.

2. **TRANSPARENCY:** We will document and clearly communicate the capabilities and limitations of facial recognition technology.

We will provide documentation for our customers to help them understand the capabilities and limitations of facial recognition technology, so they can make informed choices about deployment. We will provide illustrative examples of what we believe are appropriate as well as inappropriate or premature uses of the technology, given the current state of the technology and the broader ecosystem. We also commit to ensuring that where we make our facial recognition technology available as an online service for customers to use in their own scenarios, we will include an application programming interface or other technical capability to enable third parties that are legitimately engaged in independent testing to conduct reasonable tests of our facial recognition technology for accuracy and unfair bias.

3. **ACCOUNTABILITY:** We will encourage and help our customers to deploy facial recognition technology in a manner that ensures an appropriate level of human control for uses that may affect people in consequential ways.

Consequential uses of facial recognition technology are use cases where the technology is deployed in ways that may have a significant impact on individuals or society. They include use cases that involve the risk of bodily or emotional harm to an individual, where an individual's employment prospects or ability to access financial services may be adversely affected, where there may be implications on human rights, or where an individual's personal freedom may be impinged. In such cases, we believe the potential risk of harm or adverse consequences associated with errors are sufficiently high that there must be a qualified human appropriately involved in the decision-making process (sometimes referred to as human-in-the-loop or meaningful human review). When we work with customers to deploy our facial recognition technology, we will ensure that the solution is designed to incorporate an appropriate level of human control. In addition, we recommend that customers establish a communication and remediation channel to ensure that individuals impacted by the technology can surface their concerns and have them addressed (for example, in cases of misidentification in high stakes areas).

4. **NON-DISCRIMINATION:** We will prohibit in our terms of service the use of facial recognition technology to engage in unlawful discrimination.

We will prohibit the use of our facial recognition technology, by any customer, to unlawfully discriminate against individuals based on their actual or perceived race, ethnicity, religion, political views, national origin, disability, gender, gender identity, sexual orientation or any other characteristic protected by applicable anti-discrimination laws.

5. **NOTICE AND CONSENT:** We will encourage private sector customers to provide notice and secure consent for the deployment of facial recognition technology.

The private sector today uses facial recognition technology to identify individuals on private premises or online. For example, retailers may use the technology in their stores to improve a customer's in-store experience, employers may use the technology as a second factor to facilitate secure access to office buildings, and stadium operators may use the technology to protect the safety of their customers. In these scenarios and others, we recommend that, at a minimum, our private sector customers provide conspicuous notice to, and secure consent from, an individual before capturing their image for use with facial recognition technology. In some jurisdictions, data protection laws impose explicit consent requirements that go beyond notice and consent, e.g., the European Union's General Data Protection Regulation (GDPR). Pursuant to our Online Services Terms, our customers must comply with all laws applicable to their use of our online services, including those that relate to privacy, biometric data and data protection.

6. **LAWFUL SURVEILLANCE:** We will advocate for safeguards for people’s democratic freedoms in law enforcement surveillance scenarios, and will not deploy facial recognition technology in scenarios that we believe will put these freedoms at risk.

We believe law enforcement should be prohibited from using facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces, except in the following scenarios that seek to strike an appropriate balance between the legitimate interests of government to protect public safety, and the preservation of important individual civil liberties and privacy rights: first, if there are laws that have been enacted in jurisdictions that respect the rule of law and specifically regulate and define the parameters for the use of facial recognition technology in public spaces; second, if a court order is issued in a jurisdiction that maintains a fair and independent judiciary that authorizes the use of facial recognition technology by law enforcement for ongoing surveillance of a specified individual in a public space; and finally, in an emergency involving imminent danger or risk of death or serious physical injury to a person.

We have made, and will continue to make, strong calls for legislation of this kind. In our deployment work, we will work closely with our law enforcement customers to understand their proposed scenarios. We will not deploy our facial recognition technology in those surveillance scenarios where we believe there are inadequate safeguards to protect democratic freedoms and human rights.

We recognize this a fast paced and evolving area implicating novel and complex issues that come together at the intersection of law, policy, human rights, technology and human experience. We know that we do not have all the answers and we have much to learn. We fully expect to be revising and supplementing these principles over time as we listen and learn from our own experience, the experience of others, and the insights gained from internal and external input that we will proactively solicit. We anticipate that, over time, some of these principles may reveal themselves to be applicable to other AI technologies as well.