Chamber Technology Engagement Center (C_TEC)

FACIAL RECOGNITION POLICY PRINCIPLES

Facial recognition technology has an enormous potential to enhance security and safety, and enable innovation across a wide variety of sectors including transportation, retail, hospitality, and financial services. Already, the technology can be used in applications including airline passenger facilitation, criminal investigations, theft prevention, and fraud detection. However, facial recognition technology has received heightened attention by policymakers and the public, and there is an ongoing national dialogue as to whether to place a moratorium or a ban on the technology.

The business community recognizes that we have a responsibility to ensure the safe development and deployment of facial recognition technology. To address this challenge, the U.S. Chamber of Commerce's Technology Engagement Center (C_TEC) convened its diverse membership that spans facial recognition vendors, developers, users, and other stakeholders to draft a set of policy principles to guide policymakers as they consider proposals pertaining to facial recognition technology. These policy principles seek to appropriately mitigate any risks associated with facial recognition technology with the benefits the technology provides to consumers and the public.

PRIORITIZE TRANSPARENT USE OF FACIAL RECOGNITION TECHNOLOGY

Transparency should be the cornerstone that governs the use of facial recognition technology. Commercial and government users should be transparent about when and under what circumstances the technology is used as well as the processes and procedures governing the collection, processing, storage, use, and transfer of facial recognition data.

PROTECT PRIVACY AND PERSONAL DATA

Facial recognition technology involves the collection, processing, possible storage, and use of sensitive facial biometric data. Consequently, C_TEC believes that clear and consistent privacy protections are required to ensure that all facial recognition technology users handle the data carefully, securely, and in a manner that protects individual privacy. Policymakers should look to the U.S. Chamber of Commerce's Privacy Principles as a guide for pursuing privacy rules that fosters innovation while protecting human rights and civil liberties. In addition, C_TEC supports a risk-based approach to managing the cybersecurity of facial recognition technology, such as encrypting face templates and transmitted images. Policymakers should also promote cyber hygiene for individuals involved with handling data associated with facial recognition technology.

DEVELOP AN APPROPRIATE REGULATORY FRAMEWORK THAT PROMOTES INNOVATION, CIVIL LIBERTIES, AND HUMAN RIGHTS

PROMOTE BENEFICIAL USES OF FACIAL RECOGNITION TECHNOLOGY WHILE MITIGATING RISKS

Facial recognition technology has numerous beneficial functional applications in commercial, government, and law enforcement settings. Policymakers should recognize and acknowledge these numerous and diverse uses, ensure that public policies are narrowly tailored to both foster innovation and beneficial deployment of facial recognition technology, and prevent misuse of facial recognition technology. Policymakers should not support overly burdensome regulatory regimes, such as moratoriums or blanket prohibitions.

PURSUE A RISK-BASED AND USE-CASE SPECIFIC REGULATORY APPROACH

Facial recognition technology has innovative and a diverse range of use cases. Accordingly, any regulation of facial recognition technology should be risk and performance-based and take into account specific use-cases rather than establishing blanket, one-size-fits-all, prescriptive regulations. Policymakers should also consider the application of existing regulations and laws to prevent conflicting requirements that would thwart innovation.

ESTABLISH A SINGLE NATIONAL GOVERNANCE AND REGULATORY FRAMEWORK

As the deployment of facial recognition technology becomes more ubiquitous, it is critical that Congress ensure a clear and consistent approach to the regulation and governance of facial recognition technology. A patchwork of conflicting state and locals will hinder innovation, inhibit public safety, and create confusion for consumers. To address this patchwork, any national framework should preempt all state and local laws governing the use of facial recognition technology.

PROMOTE ACCOUNTABILITY AND CONSISTENCY THROUGH APPROPRIATE STANDARDS AND TESTING

SUPPORT THE DEVELOPMENT OF RISK-BASED PERFORMANCE STANDARDS

Common, nationwide standards are important to ensure the trustworthiness and accuracy of facial recognition technology, promote data quality, and drive consistent use-case based performance across all demographics. In accordance with existing law, the establishment of standards should be voluntary, industry-driven and consensus-based and should be undertaken by existing, independent standard-setting bodies, such as the National Institute for Standards and Technology (NIST). Also, considering the unique technical and probabilistic attributes of facial recognition technology, standards should be flexible, use-case and performance-based, and non-prescriptive.

ENSURE FEDERAL INVESTMENTS IN TESTING AND BENCHMARKING

Building public and consumer trust in the accuracy of facial recognition technology is essential. To further this objective, policymakers should prioritize standardized testing and benchmarking of facial recognition technology through existing independent entities, like NIST. To strengthen these important efforts, policymakers should ensure NIST is provided with sufficient and modern resources to support testing and benchmarking efforts. Because performance is tightly coupled with the use-case, it is essential that the benchmarks follow suit.

For more information, please contact:

Matt Furlow
Director of Policy
Chamber Technology Engagement Center (C_TEC)
Mfurlow@uschamber.com