



January 14, 2022

Office of Science and Technology Policy
1650 Pennsylvania Avenue NW
Washington, DC 20502

Re: Request for Information on Public and Private Sector Uses of Biometric Technologies [Docket Number 2021-21975]; 86 FR 56300

To Whom It May Concern:

The U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC") appreciates the opportunity to submit feedback to the Office of Science and Technology Policy (OSTP) in response to its request for information ("RFI") on "Public and Private Sector Uses of Biometric Technologies." C_TEC appreciates OSTP's efforts to "understand the extent and variety of biometric technologies in past, current or planned use."¹ Biometric technologies are not new. Their origins can be traced back to the 1960s. However, since that time, technology has steadily improved. Notably, the recent enhancements in underlying artificial intelligence ("AI") and computing power have advanced the technology. Biometric technology has multiple beneficial functional applications in both the public and private sectors. We believe it has enormous potential to enhance security and safety and enable innovation across various industries.

The Chamber has long been a fierce advocate for "promoting accountability and consistency²," which looks to elevate any "unanticipated misuse or harms³" around the use of artificial intelligence and biometric technology. Therefore, the Chamber has developed principles around the use of "artificial intelligence⁴" and "facial recognition⁵," which highlight the need for transparency. Furthermore, the Chamber stands committed to working with the Office of Science Technology Policy

¹ <https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies>

² <https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies>

³ <https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies>

⁴ <https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles>

⁵ <https://www.uschamber.com/technology/us-chamber-of-commerce-releases-facial-recognition-policy-principles>

around its work to develop an AI Bill of Rights that allows for the "equitable harnessing⁶" of the benefits of AI and Biometrics technology.

Many of the questions posed within the RFI are directed towards how organizations and businesses develop their products. Because C_TEC is comprised of companies from a wide array of sectors who use biometric technology and AI in many different ways, we will focus our feedback on topics five and six, which look to address the specific benefits of biometric technology as well as governing principles.

Topic five: Exhibited and potential benefits of a particular biometric technology

C_TEC is exceptionally excited about the past, current, and future uses of biometric technology, which will provide ample benefits to society. Some of the biometric modalities producing the most exciting benefits include voice, facial, fingerprint, palm, and iris. However, vendors and end-users are increasingly leveraging a wide variety of other biometric technologies in diverse public-sector and private-sector applications.

While C_TEC will highlight many of the great uses of biometric technology, we would like to highlight a concern that "biometric technologies" are not fully defined within the RFI, which does not allow us to address the question regarding the "scope." C_TEC believes there is a need to thoughtfully define the term "biometric technology" to reduce any misinterpretations of the scope of the RFI and the work of the Office of Science Technology Policy.

Voice:

Regarding voice technology and biomarkers, there is already excellent utilization of this technology within the healthcare sector. Current examples of the use of this technology include Cedar-Sinai, and Boston Children's use to keep in touch with their families, connect with care team members, easily access news and information and play music. Additionally, artificial intelligence to interpret patient intent enables the message to be sent to the appropriate care team member using existing hospital communication systems. This technology utilization will allow for better and more streamlined care for patients.

Furthermore, vocal biomarkers can be used for health tracking, triage, risk prediction, and detecting emergencies. C_TEC is also excited about using "voice technology" for healthcare as a remote patient monitoring tool. This includes uses within one's home to help patients adhere to post-discharge instructions or a

⁶ <https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies>

diagnostic tool. This technology is currently being used for things such as reminding patients to take their medications and to be able to share post-surgical recovery data between a patient's home and the hospital. This technology can significantly reduce pressure placed on the medical system and staff by enabling real-time engagement and remote care of certain situations.

C_TEC sees the use of voice biomarkers to further improve human-to-human interaction, such as through in-person health visits, by capturing notes to support care teams. Combined with AI, voice technology may be able to leverage data from visits to expedite fact discovery and diagnoses, assist providers in developing care recommendations, and potentially support claims processing.

Fingerprint & Palm:

Fingerprint technologies are the oldest biometric technologies, and the FBI has been using fingerprint technologies to support law enforcement and forensics since the 1960s⁷. Today, biometric technology vendors produce fingerprint, latent print, ten print, and palm print technologies for use not only in law enforcement settings but also in a wide variety of public and private sector settings. These technologies not only help generate leads in criminal investigations, but they also help secure our borders, conduct background checks, and facilitate access control to various facilities and devices.

Facial Recognition:

C_TEC also would like to highlight the benefits facial recognition technologies, which analyze facial features, generate biometric templates of these features, and compare the template generated from a probe image to one (in the case of facial verification) or many (in the case of template and the gallery template(s)). Facial recognition technologies, when used effectively and appropriately, can help expedite and improve the accuracy and security of authentication and access control. For instance, because of the uniqueness of and security protections built into biometric templates, leveraging facial recognition technology, alongside user consent to use and transparency around such applications, has become an increasingly popular way to log into phones and devices to securely access information and programs.

C_TEC member companies also provide facial recognition technologies for a variety of commercial applications that include theft prevention in the retail industry, fraud detection, ticketless entry to event venues, keyless and cashless resort experience, and face pay services to secure and enhance customer experience in

⁷ <https://www.nist.gov/programs-projects/biometrics>

financial transactions. This includes applications such as "identity check mobile," which uses facial recognition to verify a cardholder's identity for payment. This use has been found to be secure and provide ease of access to an individual's financial data.

C_TEC also sees a bright future for the use of biometric technology in everyday commerce. One of the exciting and innovative uses is opt-in frictionless retail, which allows customers to quickly maneuver throughout a retail store and pick up merchandise that is being tracked through sensors and checkout remotely. The technology provides customers with a more streamlined shopping experience. Furthermore, the use of this technology will help reduce unnecessary contact with store surfaces, which will help reduce transmission of germs onto store goers.

We also see great value in using facial recognition technology for remote virtual proctoring. This technology provides students and work professionals the ability to take exams in remote locations while at the same time maintaining the integrity of the exam. The technology further allows students to continue studies at times that are more convenient for their schedules, allowing students obtain a better work/school balance.

C_TEC would also like to highlight further government applications of facial recognition technology, which include improving border security at airports and other points of entry, detecting and combatting (attempted) identity theft, and helping to generate leads in criminal investigations. An example includes the federal governments use of facial recognition to help solve a case which a man was stalking 30 high school women through various social media outlets. Federal law enforcement obtained a warrant and used facial recognition technology through the Mississippi Fusion Center to identify and arrest the suspect.⁸

Top-performing face recognition technologies are highly accurate overall⁹ and across demographic groups¹⁰, and when used properly by trained operators, is much more accurate than the average human's facial recognition capabilities. Given the potentially serious consequences of misidentifying individuals in situations involving international air travel, obtaining government-issued identity documents, and criminal investigations, using face recognition technologies to improve the accuracy of identifications can be especially beneficial in these settings.

⁸ <https://www.justice.gov/usao-sdin/pr/mississippi-man-faces-interstate-stalking-charges-five-year-long-crime-against>

⁹ <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing>;
<https://mdtf.org/Downloads/MatchingSystemResults.pdf>.

¹⁰ NIST has found that top-performing algorithms have "undetectable" false positive error rate differences across demographic groups based on race and sex. <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

Any broad sweeping effort to limit biometric facial recognition technology within the federal government has the potential to harm innovation throughout the facial recognition ecosystem. Furthermore, it would undermine the implementation of a long-standing, bipartisan congressional mandate to apply one of the 9/11 Commission Report recommendations, namely, a biometrically enabled immigration exit system. Given the diverse uses and benefits of facial recognition technology, C_TEC believes that facial recognition regulation frameworks should calibrate any restrictions or limitations that they impose to address the risk of a specific facial recognition directly.

Iris Biomarkers:

Additionally, C_TEC would like to highlight the benefits of iris recognition technologies. Because these technologies can achieve accuracy rates of over 99%¹¹ and have become more commercially available, passengers around the world are choosing to participate in opt-in programs that leverage iris recognition technologies (in conjunction with face recognition technologies) to securely and accurately verify their identities and expedite their passage through airports.

Behavioral Biometrics:

Finally, C_TEC would like to highlight the opportunities related to “behavioral biometrics”. The financial industry is gradually moving towards the use of authentication solutions that rely upon behavioral biometric data; i.e., characteristics about an individual's interaction with their computer or smartphone device, including the use of their keyboard, mouse and/or the way in which they hold and interact with their device.

Behavioral biometric data has several advantages over knowledge-based (i.e., PIN or passwords) authentication solutions. These include reduced risk of social engineering and fraud given behavioral biometrics are difficult to copy and/or replicate. Use of behavioral biometrics also leads to reduced transaction failure and abandonment rates, and consequently reduced harm to consumers, as they cannot be forgotten like passwords or PINs.

Topic six: Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case.

C_TEC firmly believes that safe, ethical, and effective use of AI-enabled biometric technology can provide tremendous benefits to society. However, we

¹¹ <https://pages.nist.gov/IREX10/>

understand that biometrics technologies are increasingly being developed and deployed within critical processes (e.g., healthcare, employment, judicial, policing, etc.) where there is a concern that such systems could pose a risk to safety, privacy, and human rights if not appropriately vetted. In particular, C_TEC recognizes that inaccurate biometric technologies can contribute to misidentifications that, if not subject to effective human review and oversight, could result in delays in accessing a workplace or an essential service and/or unnecessary contact with law enforcement.

C_TEC also realizes that even highly accurate biometric technologies in conjunction with surveillance cameras could lead to tracking individuals in a way that infringes on individual privacy. C_TEC encourages U.S. policymakers to develop use-case-specific governance frameworks that aim to mitigate the risks that biometric technologies can pose in specific settings without unduly limiting the public's ability to reap the multitude of benefits that biometric technologies can produce. In addition to domestic biometric technology governance framework, international governance frameworks that the United States develops in coordination with allied partner nations that have a shared commitment to human rights and democratic freedoms can serve an important role in promoting the ethical and appropriate use of these valuable technologies abroad, while also strengthening international partnerships that help advance global economic efficiency and innovation.

C_TEC believes that the following principles around the use of facial recognition are the appropriate framework for any specific governance structure around the use of facial recognition technology and may be useful starting point for developing broader biometric technology governance frameworks as well.

1. PRIORITIZE TRANSPARENT 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, testing, processing, storage, use, and transfer of facial recognition data.

2. PROTECT PRIVACY AND PERSONAL DATA: 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.

3. PROMOTE BENEFICIAL USES OF FACIAL RECOGNITION TECHNOLOGY WHILE MITIGATING RISKS: Policymakers should acknowledge the benefits of facial recognition technology and not support overly burdensome regulatory regimes, such as moratoriums or blanket prohibitions.

4. PURSUE A RISK-BASED AND USE-CASE SPECIFIC REGULATORY APPROACH: Regulation of facial recognition technology should be risk and

performance-based, take into account specific use-cases, and consider the application of existing regulations and laws.

5. ESTABLISH A SINGLE NATIONAL GOVERNANCE AND REGULATORY FRAMEWORK: Congress should ensure a clear and consistent approach to the regulation and governance of facial recognition technology by developing a national framework governing the use of facial recognition technology.

6. SUPPORT THE DEVELOPMENT OF RISK-BASED PERFORMANCE STANDARDS: 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). Standards should be flexible, use-case and performance-based, and non-prescriptive.

7. ENSURE FEDERAL INVESTMENTS IN TESTING AND BENCHMARKING: To build public and consumer trust, policymakers should prioritize standardized testing and benchmark through existing independent entities, like NIST. Policymakers should ensure NIST is provided with sufficient and modern resources to support testing and benchmarking efforts.

Conclusion:

In conclusion, C_TEC believes that AI-enabled biometric technology has enormous potential to transform entire industries, providing innovative benefits to consumers and enhancing personal safety, security and privacy for all Americans. While there may be risks associated with these technologies, it is important to evaluate the level of risk posed by technologies and their intended applications to determine an appropriate course of action for mitigating risks. It is also important to work alongside industry stakeholders to determine appropriate applications and considerations for various biometric use cases. We firmly believe that biometric technology has a critical role in the advancement of our society. C_TEC looks forward to continuing to collaborate with OSTP on this important matter and encourage OSTP to continue to engage stakeholders on all matters that address biometric and artificial intelligence technology.

Sincerely,



Michael Richards
Policy Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce