ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

January 14, 2022

Re: RFI Response: Biometric Technologies

Dear Dr. Lander,

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Office of Science and Technology Policy's (OSTP) request for input on the use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.[1]

ITIF is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

SUMMARY

Overall, biometric technologies offer many benefits to society, improving convenience, security and commerce. However, biometric technologies are not a monolith. Within biometric technologies for recognition and inference there are component technologies that not only differ in their application areas, but in the computational processes they employ and the data they are trained on. As such, they present unique considerations, benefits, and potential harms, and require distinct policy approaches. Some nascent technologies that require biometric data to function, such as age estimation and augmented and virtual reality, offer unique benefits to protecting children in online spaces, reducing barriers to opportunity, and enhancing equity and inclusion. Because of the scope and scale of biometric data they need to collect for their core functions, some biometric technologies can also present unique risks, such as autonomy and discrimination risks from inferred data about preferences from involuntary or subconscious movements or reactions. The government can help address and mitigate many of these risks by increasing and expanding independent public testing of these systems (as NIST has done for some technologies); developing performance

[1] "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Federal Register, October 8, 2021, 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.

standards for any systems that use biometric information procured by the federal government; and developing more diverse training and evaluation datasets for recognition and inference.

Sincerely,

Hodan Omaar
Policy Analyst, The Information Technology and Innovation Foundation
homaar@itif.org

Daniel Castro
Vice President, The Information Technology and Innovation Foundation
dcastro@itif.org

(1) PROCEDURES FOR AND RESULTS OF DATA-DRIVEN AND SCIENTIFIC VALIDATION OF BIOMETRIC TECHNOLOGIES.

The RFI broadly refers to any system that uses biometric information for the purpose of recognizing or inferring information about an individual as "biometric technology." Biometric information includes data derived from an individual's physical characteristics (e.g., DNA, face, or fingerprints) or behavioral characteristics (e.g., gestures, gait, voice).

It is important to clarify at the outset that technologies that use biometric information to estimate the similarities between two individuals (what the RFI calls 'recognition') and those that use biometric information to predict attributes about an individual such as age, gender, and emotion (what the RFI calls 'inference') are completely different. They differ in the underlying computational processes they use, the data they are trained on, and the type of information they produce. As a result, characteristics about one technology do not necessarily apply to another.

For example, the accuracy rates of facial recognition are different than those for facial analysis, and the privacy implications of each differ too. Conflating these technologies under one broad umbrella term and seeking to understand the validity, accuracy, and error rates of the whole can create misperceptions about the risks associated with each. Therefore, policymakers should evaluate separately systems that use biometric information for recognition from those that use biometric information for inference.

Looking at systems that use biometric information for recognition first, our 2020 report *The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist* found that the best facial recognition algorithms in the world are highly accurate and have vanishingly small differences in their rates of false-positive or false-negative readings across demographic groups.[2] Taking a close look at data from the National Institute of Standards and Technology (NIST) on the accuracy of facial recognition algorithms across different demographic groups, the report reveals that most accurate identification algorithms have "undetectable" differences between demographic groups; the most accurate verification algorithms have low false positives and false negatives across

[2] Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist,"(Information Technology and Innovation Foundation, January 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

most demographic groups; and algorithms can have different error rates for different demographics but still be highly accurate.[3]

Looking at the validity and accuracy of tools that use biometric information for inference is more complicated because validity and accuracy vary significantly by application and implementation. Some tools may estimate an individual's age, gender, emotional state, or genetic conditions. The accuracy of age estimation algorithms has improved significantly over recent years with leading digital ID company Yoti's technology having a margin of error of 2.79 years across its total 45-year age range.[4] In 2020, an independent nonprofit called Age Check Certification Scheme found Yoti's system to be 98.89 percent reliable when identifying if people are under 25-years-old.[5] On the other hand, the validity of emotion recognition technology has little scientific support.[6] Even within an application area (such as age recognition), the accuracy and validity of different biometric information tools, as well as the methods used, may vary. For example, some systems estimate an individual's age using pictures of their face, while other use pictures of a person's hands or gait or the sound of a person's voice.

Therefore, policymakers should not draw broad conclusions about biometric technologies based on a single application or even a sample of the technology, but rather judge the potential of the technology based on the best-in-class implementations. This is important, because assessing a technology based on the average-in-class will lead to a very different result than assessing only best-in-class. Moreover, the level of accuracy necessary for various commercial and government uses cases will depend on the context in which it is deployed and the controls in place to mitigate potential errors.

(2) EXHIBITED AND POTENTIAL BENEFITS OF A PARTICULAR BIOMETRIC TECHNOLOGY.

Public understanding and appreciation of the benefits of systems that use biometric information for recognition continue to grow because this technology has multiple applications and is increasingly commonplace. For instance, authorities use facial recognition to help find and rescue human

[3] Ibid.
[4] Matt Burgess, "This AI Predicts How Old Children Are. Can It Keep Them Safe?" *Wired*, October 26, 2021, https://www.wired.co.uk/article/age-estimation-ai-yoti.
[5] Ibid.
[6] Lisa Feldman Barrett, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," *Association for Psychological Science,* Vol 20, Issue 1, 2019 https://doi.org/10.1177/1529100619832930.

trafficking victims, and identify individuals committing crimes ranging from shoplifting and check forgery to armed robbery and murder.[7] Businesses also use facial recognition to improve security and facilitate convenience for consumers. Several credit card companies such as Visa and Mastercard have launched services that allow customers to use selfies to verify the authenticity of online purchases and many airports use the technology to reduce the time it takes passengers to board their flights. Businesses can also use the technology to improve the accessibility of online services and help visually impaired individuals better understand their surroundings. Apps like Uber and Lyft use face recognition to verify identity documents for drivers and prevent unauthorized drivers from using an approved account, while these apps also use facial analysis to confirm they are wearing a face covering.

The benefits of systems that use biometric information for inference are less known because the technology itself is still nascent and its applications are less interwoven into society. However, two application areas are gaining increasing traction and offer significant value to consumers and businesses: age estimation and augmented and virtual reality. Given the many potential benefits of biometric technology, the primary purpose of policy should be to guide its development and deployment to ensure appropriate use, rather than impose strict limits or bans on the technology.

Age Estimation

Traditional age verification mechanisms are often trivial to circumvent. For example, a website or mobile app may use a form that asks users to submit their age or year of birth that younger children can easily bypass by giving false information. There have been multiple reports that document the routine nature by which children circumvent current age verification technologies to use websites and online services like Facebook and Instagram which are officially only available for individuals age 13 and over.[8] Systems that use biometric information to estimate age can be a valuable solution to better protect children from accessing potentially harmful content and services without strictly limiting them from having access to many types of online services.

This technology offers unique benefits in this context because most children in the United States do not have government-issued forms of ID, which means systems that use recognition cannot verify

[7] "ITIF Technology Explainer: What Is Facial Recognition?" ITIF website, April 8, 2020, https://itif.org/publications/2020/04/08/itif-technology-explainer-what-facial-recognition.
[8] Daniel Castro and Alan McQuinn, "Comments to the Federal Trade Commission on Implementation of the Children's Online Privacy Protection Act," (Information Technology and Innovation Foundation, October 2019), https://www2.itif.org/2019-ftc-coppa-comments.pdf.

their age against a reference ID. Given recent legislation such as the United Kingdom's Age Appropriate Design Code that requires social media companies, video streaming sites, and gaming platforms to verify the age of users that visit their websites, many companies are increasingly turning toward age estimation solutions. Members of the U.S. Senate and Congress have called on large U.S. technology and gaming companies to voluntarily adopt the UK's rules for American children as well.[9]

Augmented and Virtual Reality

Augmented and virtual reality (AR/VR)—immersive technologies that enable users to experience digitally rendered content in both physical and virtual space—can collect extensive biometric data. By collecting detailed biometric information from individuals, AR/VR systems can get a more complete picture of an individual and create immersive experiences for them. For example, hand-tracking technologies estimates important information such as the size, shape, and positioning of users' hands and fingers.[10] AR/VR devices may also use eye tracking sensors to determine where users are looking (to improve how they interact with the technology, to enhance graphics rendering, and to track user behavior) and to uniquely identify users.[11]

One of the benefits of AR/VR devices is that they can make several important contributions to equity and inclusion by reducing opportunity gaps, especially among members of underserved and disadvantaged communities.[12] First, AR/VR devices use a diverse set of sensors and inputs as well as digital outputs, which means they present potential workarounds for audiovisual barriers that users with vision or auditory impairments might encounter—without minimizing the user experience. For instance, immersive 3D audio that mimics 360-degree sound in physical space can provide a sense of spatial awareness for users with visual impairments: a musician performing in front of them, a friend

[9] Letter from Congressman Edward J. Markey, Congresswoman Kathy Castor, and Congresswoman Lori Trahan of the United States, June 30, 3031, https://www.markey.senate.gov/imo/media/doc/letter_-_age_appropriate_design_code.pdf.
[10] Shangchen Han et al., "Using Deep Neural Networks for Accurate Hand-Tracking on Oculus Quest," Facebook AI, September 25, 2019, https://ai.facebook.com/blog/hand-tracking-deep-neural-networks.
[11] Ellysse Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality," (Information Technology and Innovation Foundation, March 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality.
[12] Ellysse Dick, "Current and Potential Uses of AR/VR for Equity and Inclusion," (Information Technology and Innovation Foundation, June 2021), https://itif.org/publications/2021/06/01/current-and-potential-uses-arvr-equity-and-inclusion.

calling out from behind, an object appearing on their left, etc.[13] Second, because immersive experiences place the user in partially or fully virtual environments, they can manipulate and tailor these to their individual needs, making these technologies more inclusive for a wider set of users. For example, Microsoft's social VR platform AltspaceVR includes public channels such as "LGBTQ+ and Friends Meetup," "Autism VR," "ADHD and Neurodiversity," and "Indigenous Peoples in XR."[14] Finally, immersive experiences offer more engaging and realistic interpersonal and sensory experiences than their two-dimensional counterparts, creating new opportunities for digital communication and allowing virtual experiences to mirror the physical world. For example, AARP Innovation Labs developed a "virtual living room" program called Alcove aimed at families or other intergenerational groups, and offers virtual spaces for users to communicate, play games, and engage in a number of immersive experiences and activities together.[15] It is easy to imagine similar applications and activities being used to engage other communities who face distance or mobility barriers. Unnecessarily restricting the collection and use of biometric data could negatively affect the deployment of AR/VR technologies.

(3) EXHIBITED AND POTENTIAL HARMS OF A PARTICULAR BIOMETRIC TECHNOLOGY.

Systems that collect and use biometric information can reveal or enable one to infer biographical and demographic information, even if a user has not elected to provide these details. For instance, motion and eye tracking can capture a user's subconscious reactions, such as pupil dilation, which can in turn reveal inferred information about their interests and preferences—from favorite foods to sexual orientation.[16]

Bias and discrimination can occur when inferred personal information from biometrics such as details on race, gender, sexual orientation are used to deny a person access to something, such as employment, housing, loans, or basic goods and services. Consider an employer that uses an AI system with eye-tracking technologies to monitor how safely its employees drive when out on

[13] Mona Lalwani, "Surrounded by Sound: How 3D Audio Hacks Your Brain," The Verge, February 12, 2015, https://www.theverge.com/2015/2/12/8021733/3d-audio-3dio-binaural-immersive-vr-sound-times-square-new-york.
[14] From a review of the top 50 listings of "popular" channels on AltSpace VR as of April 16, 2021. See "Channels," AltspaceVR, https://account.altvr.com/channels/popular.
[15] "About Alcove," accessed January 11, 2022, https://alcovevr.com.
[16] Avi Bar-Zeev, "The Eyes Are the Prize: Eye-Tracking Technology is Advertising's Holy Grail," *VICE*, May 28, 2019, https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-trackingtechnology-is-advertisings-holy-grail.

delivery, as Amazon does.[17] The tool collects information about where a user is looking, changes in their pupil size, and whether their eyes are open or closed. If it identifies dangerous behavior such as distracted driving, it suggests actions to the driver, such as taking a break. However, many studies have found that people with autism react differently to stimuli when driving.[18] The employer may be able to infer from the eye-tracking AI software which drivers have autism, even though employees may want to keep this information private, exacerbating the risk of bias and discrimination. Similar risks could arise in other critical areas such as education, healthcare, and government services. But at the same time, the overall benefit to such a technology should not be underestimated —in this case, safer driving of delivery vehicles.

Although any system that collects biometric data raises autonomy and discrimination risks, AR/VR poses new potential risks because of the scope of information AR/VR devices gather and the potential for additional information to be inferred. Researchers at the Stanford Virtual Human Interaction Lab have estimated users generate "just under 2 million unique recordings of body language" in one 20-minute session in VR.[19] Immersive experiences require users to share—and allow devices to gather, track, and process—much more information than they would with other digital media platforms that simply transmit audiovisual information. The subtle, subconscious movements sensors can detect, which is called "nonverbal data," is virtually impossible for users to consciously control.[20]

(3) GOVERNANCE PROGRAMS, PRACTICES OR PROCEDURES APPLICABLE TO THE CONTEXT, SCOPE, AND DATA USE OF A SPECIFIC USE CASE.

To accelerate improvements in existing systems that use biometric information for recognition and inference, the government should increase and expand independent public testing of these systems. Despite the growing use and policy importance of age estimation, NIST has not performed a large-scale empirical evaluation of facial age estimation algorithms since 2014. And its evaluations of

[17] James Vincent, "Amazon delivery drivers have to consent to AI surveillance in their vans or lose their jobs," *Verge*, March 24, 2021, https://www.theverge.com/2021/3/24/22347945/amazon-deliverydrivers-ai-surveillance-cameras-vans-consent-form.
[18] Joshua Wade et al., "A Pilot Study Assessing Performance and Visual Attention of Teenagers with ASD in a Novel Adaptive Driving Simulator" (NCBI, November 1, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5693648/pdf/nihms896479.pdf.
[19] Jeremy Bailenson, "Protecting Nonverbal Data Tracked in Virtual Reality," JAMA Pediatrics, August 6, 2018, https://vhil.stanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf.
[20] Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

commercial facial recognition systems do not require cloud providers to participate.[21] Expanding and increasing testing would be useful as many commercial systems are using these services. These tests should include race, gender, and age diversity metrics as part of the testing protocol.

There should also be performance standards for any systems that use biometric information procured by the federal government, including for accuracy and error rates by age, race, and gender. These standards will ensure federal agencies do not waste tax dollars on ineffective systems or ones with significant performance disparities. NIST and the General Services Administration (GSA) would be best placed to develop such standards. Since the federal government and the private sector use the same technology, setting a performance standard for the federal government can promote better accuracy rates across all sectors of the economy, and greatly reduce the risk of systems with unacceptable accuracy rates.

To address the unique risks presented by the extent of biometric data collected and used in AR/VR, government agencies and industry should develop voluntary guidelines for AR/VR developers to secure users' privacy through transparency and disclosure practices. This could parallel the digital signage industry, which in 2011 adopted a set of voluntary privacy and transparency guidelines for the use of facial recognition and facial analysis.[22] This standard offers detailed guidance for how to provide clear and meaningful notice to consumers and under which conditions consumers should be able to opt in or opt out of data collection. A voluntary framework for AR/VR should include transparency and disclosure standards and mechanisms for immersive experiences, including clear disclosure of how sensitive biometric data is collected and used as ITIF explains in its 2021 report, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*.[23]

Finally, the government should fund the creation of additional and more diverse training and evaluation datasets for recognition and inference. For instance, the MORPH dataset is a widely used database for gender and race classification, as well as age estimation. By funding the creation of

[21]Hearings on "Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy," Before the House Committee on Oversight and Reform, January 15, 2020, Statement of Daniel Castro, Vice President of ITIF, https://www2.itif.org/2020-commercial-use-facial-recognition.pdf.
[22] "Digital Signage Privacy Standards," Digital Signage Federation, February 2011, https://www.digitalsignagefederation.org/wp-content/uploads/2017/02/DSF-Digital-Signage-Privacy-Standards-02-2011-3.pdf.
[23] Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

additional and more diverse datasets, the government can spur developers to further reduce any differences in accuracy across different demographics and reduce concerns about bias.