June 08, 2023

Mr. Gene Sperling
Senior Advisor to the President

The Hon. Arati Prabhakar
Director and Assistant to the President for Science and Technology
Office of Science and Technology Policy

The Hon. Shalanda Young
Director, Office of Management and Budget

Via email

Dear Mr. Sperling, Director Prabhakar, and Director Young,

As the Administration considers its Executive Order on identity management and fraud prevention for government benefits (EO), we write to underscore the risks of promoting or mandating the use of biometric information to enable remote verification of applicant or beneficiary identities. The Administration should instead direct departments and agencies to adopt digital identity solutions that protect and enhance privacy, security, equity, and accessibility.

In particular, the EO should not encourage reliance on facial recognition technology for identity verification. While biometric-based verification can offer benefits, it presents significant risks, as the IRS's ill-fated attempt to use ID.me illustrates.[1] Facial recognition systems exhibit significant bias by race, age, disability, and gender; present accessibility challenges for marginalized and vulnerable populations; and undermine privacy by requiring the collection of deeply sensitive and immutable information. All of these risks jeopardize the critical trust between governments and the communities they aim to serve and will ultimately undermine public agencies' efforts to administer timely and efficient access to benefits while preventing fraud.[2]

NIST's Evaluation of Different Identity Verification Techniques is Still Ongoing

In recognition of these concerns and challenges associated with biometric identification, the Department of Commerce's National Institute of Standards and Technology (NIST), which houses some of the federal government's foremost technical experts, recently solicited comments on its identity management framework, focusing on equity and actively seeking

---

[1] Hannah Quay-de la Vallee, *Combatting Identify Fraud in Government Benefits Programs*, Center for Democracy and Technology (Jan. 7, 2022). https://cdt.org/insights/combatting-identify-fraud-in-government-benefits-programs-government-agencies-tackling-identity-fraud-should-look-to-cybersecurity-methods-avoid-ai-driven-approaches-that-can-penalize-real-applicant/;
Alan Rappeport and Kashmir Hill, *I.R.S. to End Use of Facial Recognition for Identity Verification*, The New York Times (Feb. 7, 2022). https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html

[2] Elizabeth Bynum Sorrell and Ariel Kennan, *Digital Authentication and Identity Proofing in Public Benefits Applications* Digital Benefits Network (May 19, 2023). https://www.digitalbenefitshub.org/digital-authentication-and-identity-proofing-data.

alternatives to facial recognition technology.[3] Given the critical importance of this work, several of the undersigned organizations submitted comments to NIST in response.[4] It would be premature for the Administration to encourage or mandate the use of facial recognition technology in the provision of public benefits before NIST concludes its evaluation. Even following NIST's evaluation, the Administration must prioritize the following considerations in developing the EO.

Facial Recognition Systems Exhibit Bias By Race, Age, Disability, and Gender

Facial recognition systems have historically exhibited significantly biased behavior based on demographic characteristics such as skin tone, age, disability, and gender.[5] In reported tests, these systems were less accurate for people with darker skin tones and women, and those biases were additive, leading to the worst performance for women with dark skin tones.[6] These biases are likely to entrench existing societal biases that harm communities of color and other marginalized populations by delaying their access to benefits, further eroding trust in public agencies' abilities to meet their needs.

While some facial recognition algorithms have made progress on issues of bias, they are not resolved for several reasons. First, facial recognition systems still exhibit varying levels and types of biases along gender and color lines. These systems are often provided by private companies without sufficient transparency and independent research on efficacy to allow public agencies to meaningfully determine whether they have mitigated potential biases. Second, there is a lack of robust research about how well facial recognition systems work for certain populations. For instance, research shows that facial classification systems (which are related to, but distinct from, facial recognition systems) struggle to correctly classify the faces of

---

[3] NIST, SP 800-63-4 (Draft) Digital Identity Guidelines, (Dec. 16, 2022). https://csrc.nist.gov/publications/detail/sp/800-63/4/draft#pubs-documentation.

[4] Hannah Quay-de la Vallee, *CDT Joined by AJL, Researchers in NIST Comments Furthering Equity and Privacy in Digital Identity Guidelines*, Center for Democracy and Technology (April 14, 2023). https://cdt.org/insights/cdt-joined-by-ajl-researchers-in-nist-comments-furthering-equity-and-privacy-in-digital-identity-guidelines/;
EPIC and ACLU Comments on NIST's 2023 Digital Identity Draft Guidelines, Electronic Privacy Information Center and American Civil Liberties Union (April 14, 2023). https://epic.org/documents/epic-and-aclu-comments-on-nists-2023-digital-identity-draft-guidelines/.

[5] Jennifer Mankoff, Devva Kasnitz, Disability Studies, L Jean Camp, Jonathan Lazar, and Harry Hochheiser, *Areas of Strategic Visibility: Disability Bias in Biometrics*, (Jan. 2021). https://arxiv.org/abs/2208.04712.

[6] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Fairness, Accountability and Transparency, Proceedings of Machine Learning Research (2018). http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf;
Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute Of Science and Technology, (Dec. 2019). https://doi.org/10.6028/NIST.IR.8280;
Nicol Turner Lee. *Mitigating Bias and Equity in Use of facial recognition technology by the U.S. Customs and Border Protection*, The Brookings Institution (July 27, 2022). https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/.

transgender and gender non-conforming people.[7] While little direct research has been done about the performance of facial *recognition* systems for these populations, the failings of related systems is cause for doubt.[8] Additionally, there is concern that facial recognition systems will struggle to identify faces of individuals with disabilities that affect their facial morphology, but little research has been done on how facial recognition systems fare when attempting to identify these individuals.[9]

Facial Recognition Systems Compound Accessibility Challenges

Even if the biases in facial recognition were mitigated, lack of accessibility in facial recognition systems will impede efforts to provide timely and accurate access to public benefits. Facial recognition systems for identity verification typically require users to upload a selfie, either as a photo or short video, which introduces numerous avenues for disproportionate failures to seep into the administration of public benefits, particularly for vulnerable populations who are most likely to rely on benefits:

- *Limited technology access:* Not all individuals have access to the necessary technology to support identity verification protocols. Facial recognition systems typically rely on a high-quality camera, either through a cellphone or webcam, and sufficiently high-speed internet. The absence of either of these components can lead to higher failure rates.[10] Many people lack the necessary access. For example, roughly a quarter of people in the U.S. lack broadband internet access at home, a figure that is even higher for Black and Hispanic households.[11] Additionally, individuals with disabilities are more likely to have limited technology access than the general population.[12]

---

[7] Morgan Klaus Scheuerman, Jacob M. Paul, and Jed R. Brubaker, *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, PACM HCI, CSCW (Nov. 2019). https://dl.acm.org/doi/10.1145/3359246.

[8] Jim Nash, *Can Facial Recognition Do Right by Trans, Non-Binary Subjects? There is Doubt*, Biometric Update (Jun. 8, 2022). https://www.biometricupdate.com/202206/can-facial-recognition-do-right-by-trans-non-binary-subjects-there-is-doubt

[9] Sheri Byrne-Haber, *Disability and AI Bias* (July 11, 2019). https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533;
Jiaqi Qiang, Danning Wu, Hanze Du, Huijuan Zhu, Shi Chen, and Hui Pan, *Review on Facial-Recognition-Based Applications in Disease Diagnosis*, Bioengineering (Basel) (June 23, 2022). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9311612/;
Cuiting Xu, Chunchuan Yan, Mingzhe Jiang, Fayadh Alenezi, Adi Alhudhaif, Norah Alnaim, Kemal Polat, and Wanqing Wu, *A Novel Facial Emotion Recognition Method for Stress Inference of Facial Nerve Paralysis Patients*, Expert Systems (July 1, 2022). https://doi.org/10.1016/j.eswa.2022.116705;
Vera Lúcia Raposo, *When Facial Recognition Does Not 'Recognise': Erroneous Identifications and Resulting Liabilities*, AI & Society (Feb. 8 2023). https://doi.org/10.1007/s00146-023-01634-z.

[10] Shahina Anwarul and Susheela Dahiya, *A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy*, Proceedings of ICRIC (Nov. 22, 2019). https://link.springer.com/chapter/10.1007/978-3-030-29407-6_36.

[11] *Internet Broadband Fact Sheet*. Pew Research Center (April 7, 2021) https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

[12] Barbara A. Butrica, and Jonathan Schwabish, *Technology and Disability: The Relationship Between Broadband Access and Disability Insurance Awards*, Center for Retirement Research at Boston College (Oct. 24, 2022). https://crr.bc.edu/working-papers/technology-and-disability-the-relationship-between-broadband-access-and-disability-insurance-awards/.

- *Lack of comfort and familiarity with technology:* Users who are unfamiliar with technology may struggle to take a sufficiently high-quality selfie, leading them to fail the verification check. This issue is likely to disproportionately affect older, poorer applicants.[13]
- *Physical inability to use technology:* Other populations, such as blind users and those with movement disorders, may also fail the identity check due to the challenges they face when trying to take an effective selfie.[14]

Biometric Systems Collect Sensitive and Immutable Information

Mandating the use of facial recognition and other biometric identifiers raises significant privacy issues because biometric data is, by its nature, incredibly sensitive. While there are more and less privacy-preserving architectures for biometric systems, they all require some amount of collection of biometric data, making them inherently invasive. A person's biometric data can never be changed, even if it falls into unauthorized hands. In the event of a data breach, the harms are enormous because individuals are subject to an unending risk of identity theft in connection with any service that uses the breached biometric data for authentication.[15] Moreover, individuals who suffer from identity theft can face significant obstacles in regaining access to government services when agencies put a red flag on legitimate identities that were misappropriated for fraud.[16] It would be irresponsible for the government to mandate or preference collection of such data, especially when other rigorous avenues of verification and fraud prevention exist.[17] This is particularly true when the collection is part of an application for necessary and sustaining benefits, as applicants for such benefits are exceptionally vulnerable and have no choice but to comply with the requirements. The goal of public benefits is to protect and support people who would benefit from government assistance, and the application process should not run counter to that aim.

Further privacy harms can result from secondary uses of biometric data originally collected for verification. Absent strict regulation, vendors providing digital verification services may resell data to other businesses or back to the government itself.[18] Even strict regulation may not be

---

[13] Andrew Kenny, *System for Unemployment Benefits Exposes Digital Divide*, AP News (May 2, 2021). https://apnews.com/article/digital-divide-technology-business-health-coronavirus-429ca0ef19108f2a6c99c4d812abe10b.

[14] Jonathan Keane, *Facial Recognition Apps Are Leaving Blind People Behind*, Motherboard (March 22, 2016). https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind.

[15] Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023). https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice.

[16] Cezary Podkul, *How Unemployment Insurance Fraud Exploded During the Pandemic*, ProPublica (July 26, 2021). https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

[17] Hannah Quay-de la Vallee, *CDT Joined by AJL, Researchers in NIST Comments Furthering Equity and Privacy in Digital Identity Guidelines*, Center for Democracy and Technology (April 14, 2023). https://cdt.org/insights/cdt-joined-by-ajl-researchers-in-nist-comments-furthering-equity-and-privacy-in-digital-identity-guidelines/;
Michael Yang, *Digital Identity Verification: Best Practices for Public Agencies*, Center for Democracy and Technology (Oct. 24, 2022). https://cdt.org/insights/digital-identity-verification-best-practices-for-public-agencies/.

[18] Joseph Cox, *LexisNexis to Pay $5 Million Class Action Settlement for Selling DMV Data*, Motherboard (Nov. 5, 2020). https://www.vice.com/en/article/epddy4/lexisnexis-dmv-data-class-action-settlement;

enough to limit the harms of secondary uses, as companies often have difficulty governing their data collection, use, and disclosure.[19] Critically, government-managed databases initially created for benefits may be repurposed for use by law enforcement or immigration authorities, placing benefits recipients at disproportionate risk of legal action and entrenching historical disparities in the criminal justice system.[20] Fear of what the government will do with their data may cause individuals not to apply for benefits in the first place, particularly individuals from marginalized communities that have historic reasons for distrust of law enforcement or immigration agencies, such as immigrant communities.[21] These challenges are exacerbated with biometric data since, as noted above, it cannot be changed or divorced from the person it belongs to, leaving benefits seekers at disproportionate risk of over-policing for as long as the data exists.

Conclusion

Any Executive Order on identity verification and preventing benefits fraud should promote equity, accessibility, and privacy. Requiring or preferencing collection and use of biometric data, such as through facial recognition, risks undermining those values by further marginalizing already disadvantaged communities and placing vulnerable applicants at risk of harm at precisely the moment when they most need protection and support. Although preventing fraud is a legitimate and important goal, the Administration can and should pursue that goal through alternative identity verification measures that do not present the risks inherent in the use of biometric data.

If you have any questions about the issues raised in this letter, please contact Hannah Quay-de la Vallee, Senior Technologist, Center for Democracy & Technology at hannah@cdt.org.

Sincerely,

Algorithmic Justice League
American Civil Liberties Union
Center for Democracy & Technology
Data & Society Research Institute
Fight For the Future
Lawyers' Committee for Civil Rights Under Law
The Leadership Conference on Civil and Human Rights

Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It*, The Washington Post (April 26, 2021). https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.

[19] Geoffrey A. Fowler, *Google Promised to Delete Sensitive Data. It Logged my Abortion Clinic Visit*, The Washington Post (May 9, 2023). https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data/; Jacob Seitz, *Facebook Engineers Admit There's No Way to Track All the Data it Collects on You*, Daily Dot (Sep. 7, 2022). https://www.dailydot.com/debug/facebook-data-engineers-lawsuit/.

[20] *Deferred Action for Childhood Arrivals ("DACA")*, Electronic Privacy Information Center (Accessed June 5, 2023). https://archive.epic.org/privacy/daca/;
Spencer Woodman, *States Move to Protect Their Immigration Data From the Trump Administration*, The Verge (Feb. 2, 2017). https://www.theverge.com/us-world/2017/2/2/14483888/trump-immigration-ban-washington-state-immigrant-data-registry.

[21] Michael Wines, *Critics Say Questions About Citizenship Could Wreck Chances for an Accurate Census*, The New York Times (Jan. 2, 2018) https://www.nytimes.com/2018/01/02/us/census-citizenship-status-immigrants.html.