

January 12, 2022

Dr. Eric S. Lander
Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Re: RFI Response: Biometric Technologies

Dear Dr. Lander:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the Request for Information (RFI) from the Office of Science and Technology Policy (OSTP) regarding public and private sector uses of biometric technologies, published in the Federal Register on October 8, 2021 (86 Fed. Reg. 56300). The AMA appreciates OSTP's acknowledgement that the use of biometric information has the potential to both help and harm individuals and the public. This letter will focus on three of OSTP's requested topics: (1) descriptions of use of biometric information for recognition and inference; (2) exhibited and potential harms of a particular biometric technology; and (3) exhibited and potential benefits of a particular biometric technology.

Descriptions of use of biometric information for recognition and inference

The AMA is actively monitoring the use of biometric information for recognition and inference in immigration, privacy of genetic information, and use of electronic prescribing of controlled substances (EPCS). Specifically, we have advocated to the Department of Homeland Security (DHS) against the use of facial recognition in the immigration process for reasons that will be outlined below in "Exhibited and potential harms of a particular biometric technology." Also discussed in that section of our response is the AMA's concern around results of mail-order and over-the-counter (OTC) genetic tests. Finally, we summarize our support of the use of biometric technologies for EPCS in "Exhibited and potential benefits of a particular biometric technology." We are also actively monitoring emerging state laws addressing facial recognition. Several laws have been enacted while others are proposed. Some laws address certain contexts (e.g., immigration or law enforcement) while others focus on necessary controls. Several laws require court orders or warrants before facial recognition technology may be used, public notice requirements, and/or explicit statutory authorization for the technology's use.

The AMA's stance on these issues was developed through a balancing of considerations, including potential individual harms resulting from use of the biometric information, envisioned benefits to the users of the technology in question, accuracy of a given technology, equity, and AMA policy. Our overall approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our

policymaking body, the House of Delegates (HOD), which support strong personal privacy protections. AMA policy and ethical opinions on privacy and confidentiality provide that an individual's privacy should be honored unless waived by the person in a meaningful way, is de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of privacy or breaches of confidentiality. When breaches of confidentiality are compelled by concerns for public health and safety, these breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest entities and individuals as possible to achieve the necessary end.

Exhibited and potential harms of a particular biometric technology

Facial recognition

The AMA has significant concerns with the use of facial recognition in certain contexts, including immigration. Facial recognition technology has serious racial, gender, and age biases that lead to considerably decreased accuracy for this technology. Additionally, any entity seeking access to an individual's health information (including biometric information) must pass the stringent test of showing why its professed need should override the individual's most basic right in keeping his or her own information private. Absent such a justification, and because facial recognition has been shown by multiple studies to be inaccurate due to bias, the AMA does not support its use by federal, state, or local governments.

Studies have found that accuracy of facial recognition technology is linked to physical factors, including: pose, illumination or expression of a face, cosmetics, glasses, hair, or other easily changeable characteristics that may cover parts of a face; general image quality; inherent facial characteristics, particularly skin reflectance or underlying facial structure; and aging over time. A study from the National Institute of Standards and Technology (NIST) found that the majority of facial recognition algorithms in the industry possess biases that span race, gender, and age.¹ "While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied," said Patrick Grother, a NIST computer scientist and the report's primary author."²

The NIST study evaluated most of the software algorithms available at the time (nearly 200 algorithms from 99 developers). It focused on each individual algorithm's ability to perform one of two tasks, each of which are among facial recognition's most common uses:

The first task, confirming a photo matches a different photo of the same person in a database, is known as "one-to-one" matching and is commonly used for verification work, such as unlocking a smartphone or checking a passport. The second, determining whether the person in the photo has any match in a database, is known as "one-to-many" matching and can be used for identification of a person of interest.³

To evaluate whether each algorithm can sufficiently complete the "one-to-one" and/or "one-to-many" matching protocols, researchers collected data on the two types of potential software errors: false

¹ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

² *Id.*

³ *Id.*

positives and false negatives. A false positive means that the software wrongly recognized photos of two different individuals as the same person, while a false negative means the software failed to match two photos that show the same person. As such, there are countless factors that can, and do, negatively impact the accuracy of “one-to-one” and “one-to-many” matching.

Any federal policy suggesting the use of facial recognition technology must demonstrate that it is accurate and unbiased. Race and ethnicity are fundamental demographics to consider when determining the quality and accuracy of facial recognition technology. This is especially relevant considering that the algorithms designed to pilot these facial recognition technologies are not objective in nature but fluctuate widely depending on the demographic of the creator themselves. As an illustration of these algorithmic biases, NIST’s test revealed that facial recognition algorithms that were developed in China showed low false positive rates on East Asian faces.⁴ On the other hand, facial recognition algorithms that were developed in the U.S. and Western Europe were 10 to 100 times more likely to inaccurately identify a photograph of a Black or East Asian face, compared with a White one.⁵ With such a wide variation across algorithm development, this produces significant discrepancies in the false non-match rate, which has been found to be between 0.1 percent and 10 percent.⁶ This variation is unacceptable in a technology policy that will impact individuals from all races and ethnicities.

Additionally, a July 2020 Government Accountability Office (GAO) report analyzing DHS’ pilot facial recognition program noted that DHS’ facial recognition technology is still struggling with algorithmic biases.⁷ GAO officials stated that DHS’ analysis of its pilot facial recognition programs is limited due to lack of data on age, gender, and ethnicity for travelers entering and exiting the country. The report also notes that verification algorithm performance was lowest on women, Black people, and very young or very old people in comparison to performance on middle-age [W]hite men. Put differently, “[i]n verification algorithms, false positive rates for [W]hite males and [B]lack females varied by factors of 10 to more than 100, meaning the lowest-performing algorithm could be over 100 times more accurate on [W]hite male faces than on [B]lack female faces. Additionally, for verification and identification vendor tests, false positives were higher for women than men.”⁸ These differences are very likely to result in more frequent misidentification for the individuals who would be subject to use of facial recognition technology.

Moreover, additional studies found constant biases in favor of White men with error rates never worse than 0.8 percent when determining the gender of light-skinned men. However, women in the studies were more often inaccurately identified with a correlation between darker skin tone and a higher error rate.⁹ For medium skinned women the error rates were between 20.8 and 34.7 percent. But, for the darkest-skinned women in the data set the error rates increased to between 46.5 and 46.8 percent.¹⁰ For those women, the technology was doing little more than guessing their gender at random. The U.S. companies that owned this facial recognition algorithm claimed an accuracy rate of more than 97 percent. However, the data sets used to assess this performance were more than 77 percent male and more than 83 percent White.¹¹ As such, this technology not only had biased results, but the proprietors of these technologies claimed a

⁴ <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

⁵ *Id.*

⁶ <https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/>

⁷ <https://www.gao.gov/assets/gao-20-522.pdf>

⁸ *Id.*

⁹ <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212?s=09>

¹⁰ *Id.*

¹¹ *Id.*

greater accuracy than warranted based on the limited data set on which the algorithm was trained. These studies underscore our concerns with the federal government using a technology to identify individuals when such technology is unable to distinguish gender and race accurately and consistently.

Genetic information

The AMA has had significant involvement in policy and clinical discussions concerning the quality and accuracy of genetic testing over the past decade. An individual's genetic information (i.e., DNA) is the biological element responsible for determining one's identity. Accordingly, DNA is inherently identifying; genetic data cannot be de-identified. Use of direct-to-consumer (DTC) genetic tests has grown exponentially over the past decade, with an estimated 100 million individuals expected to have undergone the testing by the end of 2021.¹² The U.S. Food and Drug Administration classifies these tests as medical devices, but they also are a mechanism for massive information-gathering whereby personal, self-disclosed information, including a person's genome, can be used by the company or third parties to sell products and services. However, unbeknownst to most customers, this information can be used against them. While federal law—the Genetic Information Nondiscrimination Act (GINA)—prevents health insurance companies and employers from discriminating based on genetic information, these restrictions do not apply to life, disability, or long-term care insurance companies, which can result in insurance application rejections not only for the applicant but for their family members who may not have consented to use of DTC genetic data.¹³ Users of consumer genetic testing should be advised of the potential risks of their participation. To address these concerns, the AMA urges the federal government to advance the following policies:

- Prevent genetic testing entities without explicit, informed, and noncoerced user consent from transferring information about a user such as birthdates and state of residence to third parties which may result in the re-identification of the user based on surname inference;
- Prohibit pharmaceutical companies, biotechnology companies, universities, and all other entities with financial ties to genetic testing companies from sharing identifiable information, including DNA, with other parties without informed consent of the user;
- If a data security or privacy breach occurs with a DTC genetic company or its collaborators, require the company to inform all users and relevant regulatory bodies of the breach and the impact of the unprotected private data on those individuals.
- Ensure that research using consumer genomic data derived from saliva or cheek swabs or other human samples is treated as research on human subjects requiring informed consent with, or similar to, those required by the Department of Health and Human Services Office for Human Research Protection, using an “opt in” option to allow more consumer choice in the consent process; and
- Add long-term care, disability insurance, and life insurance consumer protections to GINA.

Additionally, while the AMA strongly supports the quality of such testing where health care professionals are extensively trained and have established protocols for the collection of specimens, the performance of tests, and returning results (including identifying the limitations of the testing), we have strong concerns when DNA collection, testing, and return of results are not undertaken by trained health care professionals under the rigorous protocols of the Clinical Laboratory Improvement Amendments. This is

¹² <https://www.pewtrusts.org/en/research-and-analysis/reports/2021/10/the-role-of-lab-developed-tests-in-the-in-vitro-diagnostics-market>.

¹³ <https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008>.

because errors (including contamination, incorrect procedures, and misinterpretation) undermine the quality and accuracy of the DNA testing and, if inappropriately performed, could have disastrous consequences for individuals and their families.

To authenticate identifiable biological evidence, those who are responsible for managing this process must be carefully trained in the handling and collection of samples. The biometric samples are extremely susceptible to contamination; thus, the quality and usability of the specimen will be lost with exposure to even miniscule amounts of DNA from others than the applicant. Such contamination may occur if multiple samples are handled at one time or if the handler touches a non-sterile surface while in possession of the DNA specimen. To appropriately analyze the collected samples, a polymerase chain reaction (PCR) process is performed. If the specimen is contaminated by another person's DNA, the PCR process will copy the DNA that is present within the specimen, including the impurity, and there will be no ability to distinguish between the DNA of the person of interest and the DNA of the contaminant. In addition, these biometric samples are highly sensitive to environmental factors.¹⁴ Introduction of moisture, sunlight, or narrow temperature changes, factors that are easily overlooked and underestimated, also destroy the integrity of the DNA specimen.¹⁵ Sample quality and meticulous conservation of the procedures required for biometric data analysis determine accuracy and usability of DNA evidence.

Exhibited and potential benefits of a particular biometric technology

EPCS is important to support high-quality patient care and to reduce fraud, tampering, and diversion of prescriptions for controlled substances. EPCS utilizes multifactor authentication, including biometric authentication as one of the acceptable methods. A well-designed electronic prescription system adds value to physicians' practice of medicine and supports better patient care. Yet, to accomplish greater uptake of EPCS across the nation, the Administration must update its regulations around the use of biometric authentication in EPCS.

The SUPPORT for Patients and Communities Act (SUPPORT Act) included a requirement that Medicare Part D prescriptions for controlled substances be electronically prescribed. The SUPPORT Act also directed the U.S. Drug Enforcement Administration (DEA) to update its EPCS regulations pertaining to the biometric component of multifactor authentication. It is critically important for the DEA to modernize its EPCS rules to increase the number of DEA registered physicians utilizing EPCS. By significantly reducing drug diversion and fraudulent prescriptions for opioid analgesics and other controlled substances, increased adoption of EPCS by physicians could contribute to ending the nationwide epidemic of opioid-related deaths. Physicians want to adopt EPCS, utilize biometric authentication, and have it integrated into their practice workflows. However, physicians have expressed great frustration that they are hampered by the limited selection of biometric products required by the DEA for EPCS, which are high-cost and poorly integrated. The current DEA requirements for multifactor authentication have been a significant hurdle in adoption of EPCS. In particular, the rigid and burdensome requirements for biometrics included in the DEA's 2010 interim final rule preclude physicians from deploying user-friendly biometric devices already found in their practices.

The AMA continues to urge the DEA to reexamine the scope of technology that is compliant with EPCS requirements and allow for lower-cost, high-performing biometric devices (e.g., fingerprint readers on laptop computers and mobile phones) to be leveraged in multifactor authentication. Additional information can be found in the [AMA's June 22, 2020, letter to the DEA](#).

¹⁴https://www.nist.gov/system/files/documents/2019/08/19/standards_for_prevention_monitoring_and_mitigation_of_dna_contamination_draft.pdf.

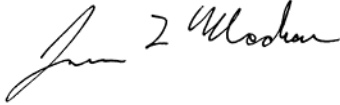
¹⁵<https://www.ncjrs.gov/nij/DNAbro/evi.html>.

Dr. Eric S. Lander
January 12, 2022
Page 6

Conclusion

We appreciate the opportunity to respond to this RFI and welcome the opportunity to discuss our views further with OSTP. If you have any questions, please contact Laura Hoffman, Assistant Director, Federal Affairs, at laura.hoffman@ama-assn.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim L Madara". The signature is written in a cursive, flowing style.

James L. Madara, MD