Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
January 14, 2022

Via Electronic Submission

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

Re:   RF1 Response: Biometric Technologies
86 FR 56300

Dear Dr. Lander:

We, the undersigned Attorneys General of the District of Columbia and the states of Illinois, Maryland, Michigan, Minnesota, New York, North Carolina, Oregon, Vermont, and Washington, submit this letter in response to the Office of Science and Technology Policy’s (OSTP) request for information on Public and Private Sector Uses of Biometric Technologies.¹ As our respective states’ chief law enforcement officers, we are charged with protecting the public interest, particularly against unlawful discrimination and unfair trade practices. We appreciate the opportunity to respond to this request for information and address these issues.

The COVID-19 pandemic has made Americans more reliant on technology than ever. Remote workforces are the new normal, and our children continue to rely on online learning tools. Consumers increasingly use technology for virtual meetings, applying for jobs and credit, to access important records, and to make everyday purchases. The proliferation of artificial intelligence (AI) and advanced biometric technology in our online lives has great potential. These evolving technologies can provide increased accuracy, speed, and convenience for many consumers. But they also come with serious concerns about bias, privacy, and transparency. Our offices have a strong interest in ensuring that AI and biometric technologies do not exacerbate inequalities, are deployed responsibly, and are secure. Across the country, jurisdictions are regulating this evolving

¹ Office of Science and Technology Policy, Request for Information on Public and Private Sector Uses of Biometric Technologies, 86 FR 56300 (Oct. 8, 2021).
industry. We support OSTP’s stated goal of creating a “bill of rights for an AI-powered world” and urge you to mandate strong protections against these vulnerabilities. Importantly, any such federal protections should supplement, not pre-empt, state and local measures (including those discussed below) that we and other States have put into place to protect our residents.

Bias in Biometric Technology Must Be Prevented.

In a perfect world, using AI would eliminate both implicit and explicit human bias, and create more equitable results. But there is no shortage of examples of biometric tools that have significant bias built into them.

For example, the National Institute of Standards and Technology (NIST) has found that facial recognition software misidentifies Native Americans, Asians, and African Americans at significantly higher rates than white people. It also noted increased failures at identifying women, the elderly, and children, noting that “[m]iddle-aged white men generally benefited from the highest accuracy rates.” Facial recognition software has also proven to be less reliable for identifying individuals’ gender when they have a darker skin tone. Voice recognition tools display significant racial bias, as well, particularly in failing to recognize certain accents and African American Vernacular English. Remote testing software that was deployed widely in 2020 to protect against cheating in schools failed to account for disabilities and neurocognitive disorders.

---


5 Id.


As a result, students with movement disorders, ADHD, PTSD, and other conditions or disabilities\(^9\) can be falsely flagged for cheating when their eye, face, and body movement do not match the expected baselines.\(^{10}\) Significantly, the use of flawed biometric technologies has led law enforcement agencies to falsely identify people as a suspect in a crime,\(^{11}\) and it has led to improper denials of employment and credit opportunities with no recourse or explanation.\(^{12}\) Left unchecked, biometric technology bias can have real and devastating impacts on people’s lives.\(^{13}\)

But these problems are not inherent to the technology; the technology is simply reliant on the data (and people) used to build it. In fact, the same NIST study that found high rates of false positive matches in non-white faces found significantly less disparity in technology that was developed in Asian countries.\(^{14}\) This shows that where bias is acknowledged, monitored, and accounted for, it can be prevented.\(^{15}\) The District of Columbia recently introduced legislation

---


\(^{11}\) Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NEW YORK TIMES (Dec. 29, 2020), available at https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html. (“In February 2019, Nijeer Parks was accused of shoplifting candy and trying to hit a police officer with a car at a Hampton Inn in Woodbridge, N.J. The police had identified him using facial recognition software, even though he was 30 miles away at the time of the incident. . . . He is the third person known to be falsely arrested based on a bad facial recognition match. In all three cases, the people mistakenly identified by the technology have been Black men.”); see also Rashawn Ray, *5 questions policymakers should ask about facial recognition, law enforcement, and algorithmic bias*, THE BROOKINGS INSTITUTION (Feb. 20, 2020), available at https://www.brookings.edu/research/5-questions-policymakers-should-ask-about-facial-recognition-law-enforcement-and-algorithmic-bias/.


\(^{13}\) See, e.g., Bolajoko Olusanya et al., *Transcutaneous bilirubin nomograms in African neonates*, PLOS ONE (Feb. 13, 2017), available at https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0172058 (finding that measurement tools that underestimate jaundice risk for darker-skinned patients may lead to delayed interventions in life-threatening neonatal health conditions); Elise Ruter, *Study shows skewed dermatological datasets result in less accurate models*, MEDCITY NEWS (July 20, 2021) (research shows that overrepresentation of lighter skin tones results in disparities in AI model ability to diagnose skin conditions for patients with darker skin).


designed to combat discrimination and biases in algorithms and AI. This legislation will prohibit companies from using discriminatory algorithms in key decision-making processes, and it will require entities to perform annual audits of their technology to identify any disparate impact the technology may have on protected groups. We also support a recent push to require tech companies to make their coding and algorithms more transparent to regulators so there can be independent evaluation of the underlying data. With biometric information being used in new and developing ways, it is critical that we take concrete, aggressive steps now to put a stop to discrimination in these processes, and the OTSP’s bill of rights will be crucial in this endeavor.

**Biometric Information Must be Protected, and Consumers Must Be Fully Informed.**

The brief history of public and private use of biometric information has shown it to be a minefield for mishandling and misuse. The same technological advances that have increased the available uses of biometrics have also resulted in new ways for hackers and bad actors to use this information to gain access to sensitive information. For example, artificial fingerprint databases have been created capable of “spoofing” a fingerprint access scanner, and Apple recently had to upgrade its Face ID technology because a “3D model constructed to look like the enrolled user may be able to authenticate via Face ID.”

Moreover, unlike traditional passwords or pin codes, biometric data cannot simply be changed when a database is breached. Therefore, it must be held with the highest security, and people must know how that information is being used. Unfortunately, we have already seen how

---


17 Id.


21 Lenildo Morais, *Biometric Data: Increased Security and Risks*, SECURITY MAGAZINE (May 6, 2020), available at [https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks](https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks). (“The security of biometric authentication data is of vital importance, even more than the security of passwords, as passwords can be easily changed if exposed. A fingerprint or retinal scan, however, is immutable. Disclosure of this or other biometric information can put users at permanent risk and create significant legal exposure for the company that loses the data. In the event of a breach, it creates an enormous challenge because physical assignments, such as fingerprints, cannot be replaced. Biometric data in the hands of a corrupt entity also has very frightening but real implications.”)
vulnerable some biometric information can be. The privacy risks are significant and are growing with the technology. It is vital that real, enforceable security protocols are developed and implemented across the industries utilizing biometric data.

The security and privacy risks discussed above are often exacerbated by a lack of transparency by entities using biometric data. Without clear information about when, why, and how biometric information is collected, used, bought, and sold by a company, consumers cannot make informed decisions about their biometric information or take steps to protect themselves when there is a security issue.

Just this past summer, the popular social media app TikTok changed its privacy policy to include a new section notifying users that the app was collecting biometric data, including “faceprints and voiceprints.” This change was automatic within the application, and users do not have an ability to grant or deny permissions. This came even after TikTok agreed to a $92 million settlement in a lawsuit that alleged it illegally collected and sold biometric data from U.S. users. This is just one example of ways in which everyday technology can collect and distribute biometric information from unsuspecting individuals, potentially putting their identity and security at risk.

Additionally, several lawsuits filed against Clearview AI, Inc. (Clearview) highlight the extent to which businesses are capitalizing on people’s biometric information without the individual ever transacting or interacting with them in the first place. Clearview has been accused of collecting images found online to create a database of billions of faceprints without the knowledge or consent of any of those contained in the database. Clearview then sold access to that database to many third parties. None of the individuals included had consented or were aware that their images had been collected or sold.

---

22 Chris Baraniuk, *Biostar security software 'leaked a million fingerprints,‘* BBC NEWS (August 14, 2019), available at https://www.bbc.com/news/technology-49343774. (“More than a million fingerprints and other sensitive data have been exposed online by a biometric security firm, researchers say. ... As well as fingerprint records, the researchers say they found photographs of people, facial recognition data, names, addresses, passwords, employment history and records of when they had accessed secure areas.”)


24 Id.


27 Id.
States and local jurisdictions are increasingly undertaking regulatory efforts to protect the privacy of their residents. Illinois, with its Biometric Information Privacy Act, was the first state to enact a comprehensive law governing the collection and use of biometric information. Since then, the states of California, New York, and Washington, and the cities of Berkeley, New York, Oakland, Portland, and San Francisco, have enacted laws specifically prohibiting the use of biometric information in certain circumstances, such as to clock-in to a job or to identify suspects in a crime. Additionally, the District of Columbia and several other states have passed legislation to address biometric privacy concerns. In these jurisdictions, although the collection and use of biometric data may not be regulated, the information is protected as personal identifiable information (PII), mandating a certain level of security and requiring entities to provide notice when the information has been compromised. These statutes are responsive to the harm consumers face from companies that otherwise have little incentive to prioritize cybersecurity. While the District and states should and will continue to take action to protect their residents, all Americans should have these protections, and this patchwork effort would be greatly assisted by a national effort.

We strongly urge OSTP to incorporate robust and measurable security and transparency protocols into the technology bill of rights. This should include, but not be limited to (1) a requirement that biometric data be maintained at least as securely as other protected personal identifiable information (as is already required by many state laws); (2) a prohibition on the sale or transfer of biometric data to third parties; (3) clear and conspicuous disclosures to users of when biometric data is being collected and its intended use; (4) a requirement that users affirmatively opt-in to biometric data collection, rather than opt-out; (5) a simple mechanism for consumers to delete biometric data collected by companies; and (6) a ban on the use of discriminatory algorithms.


29 Biometric Information Privacy Act, 740 I.L.C.S. 14/1, et seq.


32 Id.

33 As mentioned above, if OSTP or other federal agencies take action in this space, they should be explicit that such measures do not pre-empt state and local standards.

coupled with a requirement that companies perform an annual audit to monitor for discrimination and immediately take action to rectify any discrimination revealed by such audit.

We appreciate the opportunity to comment on these important issues, and we applaud the OSTP for its thorough consideration of our concerns.

Sincerely,

KARL RACINE
Attorney General for the District of Columbia

KWAME RAOUl
Illinois Attorney General

BRIAN E. FROSH
Maryland Attorney General

DANA NESSEL
Michigan Attorney General

KEITH ELLISON
Minnesota Attorney General

LETITIA JAMES
New York Attorney General

JOSH STEIN
North Carolina Attorney General

ELLEN F. ROSENBLUM
Oregon Attorney General

THOMAS J. DONOVAN, JR.
Vermont Attorney General

BOB FERGUSON
Washington State Attorney General