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.
Before the
Office of Science and Technology Policy

In the Matter of
Docket No. 2021-21975

Public and Private Sector Uses of
Biometric Technologies

Comments of
COLOR OF CHANGE

Gabrielle M. Rejouis
Color Of Change
Racial Justice Advocacy Group

colorofchange.org

Filed January 14, 2022
Introduction

In its request for information, the Office of Science and Technology Policy (OSTP) seeks input on past deployments, proposals, pilots, and trials, and on current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of individuals’ attributes, including mental and emotional states.\(^1\) Color Of Change urges OSTP to consider how biometric technologies disproportionately impact Black communities by reinforcing biased practices and policies. Biometric technology is often defective, accelerates racist law enforcement, and entrenches bias in employment. For these reasons, we recommend that the federal government ban all use of biometric surveillance technology and prohibit use of other forms of biased biometric technology.

1. **Biometric technology frequently does not work as advertised.**

Biometric technologies often do not identify or recognize Black people and, therefore, cannot do what developers propose they can. Biometric technology developers and vendors often sell promises rather than functional products. Proven inaccuracies and racial biases are built into biometric technologies.\(^2\) If a biometric technology cannot pick up darker skin or respond to an accent, it is defective. Biased technology is not merely an inconvenience; it can potentially interfere with an individual’s livelihood (by locking them out of their jobs) and liberty (by misidentifying them for law enforcement purposes). Congress and the Biden–Harris administration must boost regulations for biometric technologies in the private sector. Technology that shows evidence of bias should be banned.

A. **Biometric technology is not trained to recognize darker skin.**

A 2018 MIT study led by Joy Buolamwini found that when it came to identifying Black women, the error rates for facial recognition technology were up to 35 percent

---


2 Ibid.
while the technology accurately identified White men over 99 percent of the time.\textsuperscript{3} The study also found that the error rate in misidentifying Black women was nearly 49 times that of White men.\textsuperscript{4}

The National Institute of Standards and Technology separately found that facial recognition algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a Black or East Asian individual, compared to identifying a photograph of a White individual.\textsuperscript{5} Such racially biased inaccuracies are found in biometric technologies across the board, including those sold for commercial use. These reports demonstrate that discrimination is a feature of facial recognition technology.

Further, smart watch developers do not properly account for darker skin when developing light-sensing biometric devices. Smart phones and smart watches developed by companies like Apple\textsuperscript{6} and Samsung\textsuperscript{7} use biometric technology to monitor heart rate. These technologies have proven to be inaccurate\textsuperscript{8} and less effective for individuals with darker skin tones.\textsuperscript{9} The technology uses pulses of light to calculate heart rate.\textsuperscript{10} When companies fail to adjust the light for darker skin, they sell ineffective products for Black communities and other people of color. Black communities already face health disparities; it is concerning that ineffective technology builds upon this already biased system.


B. Speech recognition technology struggles to understand people of color and women.

Speech recognition technology has proven to be less effective for people of color and women because developers use databases with majority White male data points to train the technology.\(^{11,12}\) There are major real-world negative implications for these built-in biases. Speech recognition is used to influence immigration decisions, job hiring, and transportation, among many other things.\(^{13}\)

2. Criminal and immigration law enforcement agencies’ use of biometric technologies accelerates the surveillance and racist policing of Black communities.

The use of biometric surveillance by law and immigration enforcement agencies accelerates existing racist policing practices.\(^{14}\) Law enforcement agencies already disproportionately surveil and police Black communities, and biometric surveillance technology threatens to expand those practices.\(^{15}\) The technology gives police an “objective” rationale to continue targeting the Black and Brown communities they have always surveilled.\(^{16,17}\)

Biometric technology can create a vicious cycle, keeping people in constant contact with law enforcement agencies. When police departments use facial recognition

\(^{13}\) Ibid.
technology in connection with mugshot databases to find suspects, they rely on a
dataset that is disproportionately Black, a reflection of the racial bias of the criminal
justice system. In this reinforcement loop, Black people are disproportionately
arrested and therefore overrepresented in these databases. The use of facial
recognition technology to find investigative leads will direct law enforcement agencies to
return to people who have histories with police.

Law enforcement agencies have demonstrated department policies will not
protect Black communities from abuse. During the summer of 2020 uprisings, New York
City police went to the home of Derrick Ingram, a Black Lives Matter activist, to arrest
him. Police submitted a photo to their facial recognition technology to locate him using
what appeared to be a photo taken from his Instagram account. In doing so, New York
City police violated their own policy, which states that facial recognition technology can
only be used with a still from a surveillance video or an arrest photo. A report from the
Center on Privacy & Technology at Georgetown Law also found the New York Police
Department (NYPD) frequently tampered with photos submitted to their facial recognition
technology. Making changes to a photograph to find an investigative lead could
dramatically alter the results a search will yield. The NYPD also used celebrity lookalikes
to find suspects. For example, detectives used a photo of Woody Harrelson to identify a
suspect from surveillance footage. The department also used a photo of a New York
Knicks player to find another suspect.

---

Technology at Georgetown Law. Retrieved November 24, 2021 from,
https://www.perpetuallineup.org/findings/racial-bias.
19 Kelly, J. (2020, June 10). Analysis of police arrests reveals stark racial disparity in NY, NJ and CT. ABC 7
New York. Retrieved November 24, 2021 from,
20 COC Statement for Facial Recognition Technology: Examining Its Use by Law Enforcement
https://docs.google.com/document/d/1tkaT0r1ZnsXGAjJ0dqUn0PKiDLZtczzzgY0Qm5FNkMoU/edit
21 COC Statement for Facial Recognition Technology: Examining Its Use by Law Enforcement
https://docs.google.com/document/d/1tkaT0r1ZnsXGAjJ0dqUn0PKiDLZtczzzgY0Qm5FNkMoU/edit
22 Joseph, G. and Offenhartz, J. (2020, August 14). NYPD Used Facial Recognition Technology in Siege of
Black Lives Matter Activist’s Apartment. Gothamist. Retrieved November 24, 2021 from,
ent.
23 Vincent, J. (2020, August 18). NYPD used facial recognition to track down Black Lives Matter activist. The
Verge. Retrieved November 24, 2021 from,
gram.
24 Garvie, C. Garbage In, Garbage Out: Face Recognition on Flawed Data. Center on Privacy & Technology
25 Ibid.
26 Ibid.
Due to the past practices of law enforcement agencies, the Biden–Harris administration must ban the use of biometric technology in law enforcement. Existing policies are insufficient to protect Black communities from law enforcement agencies’ misuse of biometric surveillance technologies. Law enforcement agencies will not follow changes in policy to reduce abuse. Biometric technology must be removed from the law enforcement toolbox.

3. **The use of biometric technology in recruitment and employment entrenches bias against Black communities.**

The use of biometric technology in the workplace entrenches discrimination against Black people, including those with disabilities and those who are transgender. Biometric technology is used to evaluate job candidates and current employees. While they are marketed as more equitable than traditional evaluations, these systems can reproduce past patterns of inequity.27

**A. Hiring technology disadvantages Black able-bodied and disabled people.**

Hiring technology that incorporates automated cognitive and emotional state evaluations has the ability to punish Black able-bodied and disabled people for deviating from the White and able-bodied norm.28 Technology developed by HireVue analyzed the language and tone of a candidate’s voice and their facial expressions in job interview recordings.29 The technology was built on a database of about 25,000 pieces of facial and linguistic information compiled by previous interviews of “successful hires.”30 The dataset labeled underrepresented traits as undesired traits, which could disadvantage and systematically exclude Black candidates and candidates with disabilities. The dataset might penalize a job applicant for mannerisms that are acceptable in their culture or that may be indicators of a disability.31 For example, making eye contact may be seen as a

---

30 Ibid.
sign of disrespect or trustworthiness depending on the culture; and some people on the autistic spectrum do not make frequent eye contact when speaking. Hiring software that penalizes job candidates for failing to make eye contact will disproportionately impact people from these backgrounds.

**B. Facial recognition technology disproportionately deactivates trans Uber driver accounts.**

Uber facial recognition technology’s failure to recognize transgender Uber drivers locked them out of their jobs. Transgender Uber drivers have been either temporarily or permanently suspended from their accounts due to an Uber security feature that requires drivers to take a photo of themselves to verify their identity.\(^\text{32}\) If the photo does not come back as a match to other photos on file, the photo will be flagged and the account will be locked. As transgender individuals transition, their faces may change and look different from photos on file. The use of defective facial recognition in employment can result in reduced income for transgender drivers.\(^\text{33}\) When facial recognition technology struggles to identify people with darker skin, this will disproportionately impact Black transgender people. The transgender community already faces barriers to employment. This security feature can exacerbate the economic inequalities they experience.

**C. Emotion recognition can encode microaggressions against Black women.**

Emotion recognition technology in customer service industries forces employees to strictly adhere to a narrow and sometimes inappropriate set of cultural norms. Companies are using biometric technologies to surveil employees and evaluate their work performance.\(^\text{34}\) Call centers use voice analysis technology—like Voci and Cogito—to

---


assess the emotion of call center employees. This technology will reprimand employees for indicators of negative emotions, such as the tone of their voice or long pauses. The dataset also rewards a narrowly defined set of behaviors, which might not be appropriate for the context of the call. For example, a call center employee repeated “I’m sorry” on a call where a customer joyfully shared about the birth of a baby, aware that the emotion recognition software would register this as empathy.

Biometric technology may provide justification for otherwise biased reviews from their managers. Black women in particular are often judged more harshly for the tone of their voice. Other industries already use biometric surveillance as a pretext to fire Black workers. Amazon monitors the rate at which employees work using a measure called “time off task.” If a worker is assigned to assembling orders, time off task (TOT) will track every moment they are not scanning an item. Farhiyo Warsame led worker organizing at the Amazon Shakopee warehouse. After being transferred to a new department, Amazon reported that Warsame was violating the TOT policy. When Black workers are more likely to be fired for raising concerns about workplace conditions, biometric surveillance technology should not provide cover for employers’ biased decisions and retaliation.

D. Without regulation and enforcement, private actors will continue to use discriminatory biometric technology.

Regulation is needed because employers will continue to use biometric technology despite these risks. Following the Electronic Privacy Information Center’s

---

36 Ibid.
complaint before the Federal Trade Commission, HireVue conducted a third-party audit of its algorithms and released the results.\textsuperscript{41} The audit identified several areas where the company could do more to address racial bias in its algorithms. The audit recommended that HireVue look into potential bias for job candidates with different accents.\textsuperscript{42} It also found that candidates of color were more likely to give shorter answers to questions, resulting in these interviews being disproportionately flagged for human reviewers, which might harm candidates’ chances to advance to the next phase.\textsuperscript{43} Despite these proven concerns of bias, HireVue says that about 700 companies, including GE, Unilever, Delta, and Hilton, have used or continue to use its technology.\textsuperscript{44} It is vital that biometric technology developers are given standards to prevent products with bias from going to market.

4. The Biden–Harris administration must protect Black communities by regulating and banning certain biometric technologies.

Law enforcement agencies’ use of biometric technologies must be suspended and banned. Addressing the use of this technology is an urgent racial justice issue. A law enforcement agency biometric technology moratorium is vital to protect Black communities. Facial recognition technology increases the surveillance of Black people both in the criminal justice system and in our everyday lives. Law enforcement agencies have proven that they are unlikely to follow changes in policy or regulation. The only way to protect Black communities is to prevent law enforcement from using the technology. Color Of Change supports the Facial Recognition and Biometric Technology Moratorium Act of 2021. The bill would prohibit the use of facial recognition technology by federal entities as well as the use of federal dollars for biometric surveillance systems.

Private actors must adhere to civil rights laws when developing and using biometric technology. They must avoid using technology that advances discrimination and should not be able to pass blame for bias onto the systems they use. Regulation is necessary to create assessment and testing requirements to proactively detect and correct bias in biometric technology. Employers must also be banned from using


\textsuperscript{43} \textit{Ibid}.

biometric surveillance technology. The federal government must provide obligations to suspend all use of biometric technology that has discriminatory impact.

**Conclusion**

Biometric technologies have not delivered the promises of their developers and vendors. These technologies threaten to entrench discrimination in areas such as law enforcement and employment. Improving the accuracy of biometric surveillance technology will not prevent it from enhancing discrimination. Flawed technology should not invite repair but discontinued use. It is paramount for algorithmic accountability regulation to protect Black communities by incentivizing proactive testing and swift termination of technologies that discriminate.