January 14, 2022

Dr. Eric Lander
Director
Office of Science and Technology Policy
1600 Pennsylvania Ave, NW
Washington, DC 20500

Re: **Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies**

Dear Director Lander:

Consumer Reports (CR) writes today in response to the Request for Information on Public and Private Sector Uses of Biometric Technologies. Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace with and for all consumers and to empower consumers to protect themselves.[1]

Biometrics and biometric processing using artificial intelligence can have many positive applications. Diagnostics is an area where, if used appropriately, AI can perhaps help identify disease from medical scans before doctors are able to.[2] Gait analysis can be used to assist in physical therapy rehabilitation.[3] Using biometric processing like monitoring whether a driver is paying attention to the road can help improve public safety.[4] However, some companies

---

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] Denise Grady, "A.I. is Learning to Read Mammograms," *The New York Times,* January 1, 2020. https://www.nytimes.com/2020/01/01/health/breast-cancer-mammogram-artificial-intelligence.html.
[3] ProtoKinetics, "Measuring Gait Function," https://www.protokinetics.com.
[4] Kate Kaye, "The infrastructure law just gave a boost to controversial driver-monitoring AI tech companies," *Protocol*, November 23, 2021, https://www.protocol.com/enterprise/driver-monitoring-ai-infrastructure-bill

developing products that deploy biometric processing techniques are engaging with pseudoscientific claims that could lead to massive consumer harms. Certain companies are using biometric technologies to attempt to infer individuals' behavioral, cognitive, or emotional states. Often, however, these technologies use underlying methods and processes that are not based in science and can therefore have discriminatory or otherwise harmful impacts on individuals being analyzed.[5] At worst, some of these technologies are reviving pseudoscientific racism which has been debunked many times over.[6] Companies designing these algorithms can exploit biometric features including faceprints, retina/eye scans, or an individual's gait or gestures in order to attempt to predict certain characteristics about the individual. These technologies can exclude people from opportunities or mark them as a threat or "high-risk" in a particular situation based on little or fraudulent evidence.[7] In this comment, we will expand on the different types of biometric processing, the concerning claims companies make about their products, and how individuals can be impacted by these technologies. We will then discuss how existing legislation applies to these technologies and propose best practices and policy recommendations to mitigate harm.

We have several recommendations to mitigate the harm that can occur due to algorithms used to make subjective predictions or classifications about individuals. Specifically:

- **Companies should be prohibited from developing and selling algorithms to make predictions about people's behavioral, emotional, and cognitive states without robust evidence to substantiate any claims.**

- **Companies should not be using algorithms to make predictions about people's behavioral, emotional, and cognitive states, particularly in sectors where limited contestability of these decisions could endanger the individual or deprive them of life opportunities.**

- **Biometric processing, including emotion, cognitive, and behavior predictions, should be significantly curtailed in public spaces.**

---

[5] Arvind Narayan, "How to Recognize AI Snake Oil," *Princeton University*, https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf

[6] Catherine Stinson, "Resurrection of phrenology? AI's quest to link facial features and criminality has a shady Victorian legacy," *Genetic Literacy Project,* September 9, 2020, https://geneticliteracyproject.org/2020/09/09/resurrection-of-phrenology-ais-quest-to-link-facial-features-and-criminality-has-a-shady-victorian-legacy/.

[7] Seth Colaner, "AI phrenology is racist nonsense, so of course it doesn't work," *VentureBeat,* June 12, 2020, https://venturebeat.com/2020/06/12/ai-weekly-ai-phrenology-is-racist-nonsense-so-of-course-it-doesnt-work/

- **Increased funding and resources for agencies that enforce antidiscrimination law, as well as the FTC, to go after and identify companies that are engaging with biometric-related pseudoscientific claims in the AI space. Agencies enforcing antidiscrimination law should also clarify that these technologies fall under their jurisdiction, and Congress may need to update laws to fill in gaps concerning new biometric technology.**

Emotion/Affect Recognition

Some companies are using certain biometric features of people to predict their emotional states. Most frequently, an algorithm can use an individual's faceprint (capture of a person's face) to attempt to predict real-time emotions — also called "affect recognition."[8] However, there is no reliable public evidence to suggest that people reliably feel what is expressed on their faces. According to one study, while people sometimes express on their face the way they feel (a frown for sadness, a scowl for anger or frustration, etc.), the way people express emotions on their face can vary "substantially across cultures, situations, and even across people within a single situation."[9] Other biometric processes companies are exploiting to infer emotion include but are not limited to voice analysis, gait analysis, and even eye tracking.[10] We will discuss which sectors these technologies are prevalent in and for what applications these biometric tech companies are marketing their products.

Employment

Some AI companies are developing algorithms that are intended to help HR departments narrow down job applicants or monitor/encourage productivity in the workplace. Companies like HireVue have been criticized for incorporating facial and other analysis into their video interviewing software which monitors the applicant's expressions, their tone of voice, perceived traits like "enthusiasm," eye contact, and their word choice. After much pushback from civil rights groups including an official complaint to the FTC from the Electronic Privacy Information Center, the company discontinued their facial analysis component of their software. They claimed that due to their improvements in natural language processing technology, "visual

---

[8] Kate Crawford, "Artificial Intelligence is Misreading Human Emotion," *The Atlantic,* April 27, 2021, https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/
[9] Lisa Feldman Barrett, et. al., "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements," *Psychological Science in the Public Interest,* July 17, 2019, https://journals.sagepub.com/doi/10.1177/1529100619832930.
[10] Lydia Belkadi, "The Proposed Artificial Intelligence Act and Biometric Systems: A Peek into the Maze," *Centre for IT and IP Law*, October 26, 2021, https://www.law.kuleuven.be/citip/blog/the-proposed-artificial-intelligence-act-and-biometric-systems-part-i/

analysis no longer significantly added value to the assessments."[11] While the company's decision to stop their visual analysis is an improvement, vocal analysis can still lead to various biases, especially against those who are nonnative speakers, those who have certain disabilities, or even those the software decides are speaking "too casually," for example, or are not using certain words that the algorithm values more highly. HireVue is not the only company using biometrics to assess job applicants — other companies like Interviewer.AI and MyInterview assess candidates' faces, body language, and/or voices and rank candidates perceived characteristics like "sociability," "humility," and "positive attitude."[12] Not only is the perception of these traits subjective, but they are often not related to someone's ability to do a job well.

Other Examples of Emotion Recognition

Other companies are using biometrics for marketing purposes. Some companies are trying to classify people's emotions to see how they respond to advertisements.[13] While using people's perceived emotions (even if perceived inaccurately by the algorithm) to determine how they respond to an advertisement may not contribute overtly to exclusion from a life opportunity, there could be some substantiation issues with the technology if the product is being sold to advertisers. There could also be some privacy issues with these processes depending on how collected data is handled. People's faces are integral to who they are as a person, and companies collecting data like their faceprints or expressions could exploit that data by selling it or using it for other purposes. There are massive privacy and dignity concerns when collecting biometrics about an individual, and it is important that even if there is a good business reason to collect biometrics that they not be used for other purposes beyond what is conveyed to the consumer. While processing of biometric data for research may be reasonable in certain controlled settings with clear user understanding and institutional safeguards, biometric data collection in public spaces should be significantly constrained.

Particularly in the employment context, it is unlikely (or at least lacking evidence) that the way a person talks, their tone of voice, or their facial "microexpressions" have much to do with their

---

[11] Roy Maurer, "HireVue Discontinues Facial Analysis Screening," *SHRM*, February 3, 2021, https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/hirevue-discontinues-facial-analysis-screening.aspx; Lindsey Zualoga, "Industry leadership: New audit results and decision on virtual analysis," HireVue blog, January 11, 2021, https://www.hirevue.com/blog/hiring/industry-leadership-new-audit-results-and-decision-on-visual-analysis.

[12] Interviewer.AI, "What's the technology behind it?" https://interviewer.ai/explainable-ai/; Sheridan Wall and Hilke Schellmann, "We tested AI Interview Tools. Here's what we found," *MIT Technology Review,* July 7, 2021, https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/.

[13] "Facial recognition advertising: the future is here," Alfi, https://www.getalfi.com/advertising/facial-recognition-advertising-future-is-here/; Peter Adams, "How Mars measures the emotional impact of video ads using AI tech," *Marketing Dive,* September 1, 2021, https://www.marketingdive.com/news/how-mars-measures-the-emotional-impact-of-video-ads-using-ai-tech/605882/.

ability to do their jobs in most cases. While these factors do affect how a hiring manager might view an applicant, it is unclear whether these algorithms are picking up on similar or relevant factors. These algorithms can rank individuals against preferred characteristics, but these characteristics can be chosen arbitrarily, likely biased against those with differences due to culture or disability, and perhaps unrelated to the individual's job performance. And, as mentioned, there is little evidence that an algorithm can accurately predict someone's emotions. **We recommend against companies using an individual's biometrics in order to evaluate them as a job applicant as well as in other contexts/sectors that could deprive an individual of life opportunities.**

Behavioral Inferences

Some AI companies that use biometrics also claim they are able to identify behavioral aspects of people — such as whether someone is lying, is a criminal or a threat in some way, or even someone's sexuality. One company, EyeDetect, claims to be able to detect whether someone is telling the truth or not based on pupil dilation and the rapidity of eye movements. Critics of the technology claim that human truth-telling is too subtle to accurately detect, which is similar to the criticism of polygraph tests.[14] This type of algorithm could be particularly harmful if used by law enforcement or other security-clearance agencies, for example. Similar to the issues of validity with polygraph tests,[15] individuals would have few ways to push back against false or wrong decisions made by the algorithms which could seriously jeopardize their rights or freedoms.

Similarly, other companies claim that their algorithms can analyze people's faces to determine their jobs, intelligence, or even if they are a criminal. One company in Israel called Faception claims it can determine whether someone has a "High IQ," is an academic researcher, professional poker player, bingo player, white-collar offender, terrorist, or even pedophile.[16] A research group at Harrisburg University claimed in 2020 that they developed an algorithm that could "predict if someone is a criminal, based solely on the picture of their face."[17] Another research group at Stanford University developed an algorithm they claimed could determine someone's sexual orientation based on a photo of their face.[18] These companies and research groups are playing into the debunked concepts of physiognomy and phrenology, which are

[14] https://www.washingtonpost.com/technology/2021/11/15/lie-detector-eye-movements-converus/
[15] "The Truth About Lie Detectors (aka Polygraph Tests)," American Psychological Association, https://www.apa.org/research/action/polygraph.
[16] Faception, "Our Technology," https://www.faception.com/our-technology
[17] "Facial recognition to 'predict criminals' sparks row over AI bias," *BBC News*, June 24, 2020, https://www.bbc.com/news/technology-53165286.
[18] Sam Levin, "LGBT groups denounce 'dangerous' AI that uses your face to guess sexuality," *The Guardian*, September 8, 2017, https://www.theguardian.com/world/2017/sep/08/ai-gay-gaydar-algorithm-facial-recognition-criticism-stanford.

pseudoscientific notions that an individual's personality or character can be determined from their appearance.[19]

Cognitive Inferences

Companies like Affectiva (now part of HireVue) claim their technology can tell whether a driver is distracted or drowsy while driving a car.[20] While improving road safety is critical, companies must prove that their biometric technology works for a variety of people, circumstances, appearances, clothing/accessory types, etc. If a car detects driver distraction and uses that information to sound an alert or limit the misuse of an active driving assistance system, for example, this could be a positive use case with significant safety benefits. However, the privacy and autonomy implications of this technology could be severe if irresponsibly combined with law enforcement or other external monitoring — such as if a car is programmed to automatically summon police when it (potentially falsely) detects its driver is not capable of being behind the wheel. Biometric applications can have many positive use cases but necessary guardrails need to be put in place to minimize infringement on consumers' privacy and legal rights.

Governance

There are several laws and regulations that can likely apply to biometric processing with regards to predicting emotional, cognitive, and behavioral states. However, due to the black box nature of many algorithms, enforcement of these rules may be difficult. We will outline the main relevant laws and potential limitations to enforcement, as well as provide some policy recommendations for mitigating harm these types of algorithms can cause.

Section 5 of the FTC Act

Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts and practices in or affecting commerce." The FTC has a long history of bringing cases against companies who lack scientific substantiation for their claims, and it has said that statements about the efficacy of AI and algorithms must be backed up by scientific evidence.[21] Of course, the FTC may not have the resources to investigate every single company making these claims about their products — it could be helpful for the **FTC or Congress to pass regulations prohibiting the use of algorithms predicting individuals' emotional, cognitive, and behavioral states for particular**

---

[19] "Face to Face: Physiognomy and Phrenology," The Shelf: Harvard Blog, September 24, 2012https://blogs.harvard.edu/preserving/2012/09/24/face-to-face-physiognomy-phrenology/.

[20] Affectiva Automotive Ai for Driving Systems, Affectiva, https://www.affectiva.com/product/affectiva-automotive-ai-for-driver-monitoring-solutions/.

[21] Elisa, Jillson, "Aiming for truth, fairness, and equity in your company's use of AI, *Federal Trade Commission Business Blog*, April 19, 2021, https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

applications, and furthermore make explicit that companies making biometric technologies need to back up their claims under advertising substantiation law. This would make the dangers of these algorithms more explicit and hopefully disincentivize companies from working on them at all.

Federal/State Antidiscrimination Law

Many federal and state laws prohibit discrimination based on protected classes like race, gender, skin color, disability, etc. in areas like housing, credit/lending, and employment. At the federal level, these laws include the Fair Housing Act, the Equal Credit Opportunity Act, and Title VII of the Civil Rights Act; at the state level, antidiscrimination laws can be even more restrictive. If these products lead to disparate impacts against protected classes in regulated sectors, this is prohibited under antidiscrimination law. However, the various agencies that enforce these laws may not have the resources to go after all companies making these kinds of products. **We recommend increased funding and resources for agencies that enforce antidiscrimination law, as well as the FTC, to identify and take action against companies that are engaging with biometric-related pseudoscientific claims in the AI space; furthermore agencies enforcing antidiscrimination law should clarify that these technologies fall under their jurisdiction, and federal and state legislatures may need to update antidiscrimination law to fill in gaps regarding emerging biometric processing technology.**

Biometric data laws

While there are some laws that require consent for biometric data collection (such as the Biometric Information Privacy Act in Illinois),[22] virtually none explicitly prohibit data collection for the purposes of emotion/cognitive/behavior prediction. Some cities like San Francisco have banned the use of facial recognition software by law enforcement and other government agencies, but these laws are not specific enough to capture the harm done by other types of biometric data collection and processing.[23]

Conclusion

Ultimately, the types of decisions algorithms are being designed to make about people's emotional, behavioral, and cognitive states are largely based on unfounded claims and debunked pseudoscience. Depending on the application, their usage could lead to serious harm to individuals and consumers including loss of liberties and basic rights. While we have laws that prohibit many of these technologies in theory, we should make more explicit the particular kinds

---

[22] "Biometric Information Privacy Act (BIPA)," ACLU Illinois, https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.
[23] Kate Conger, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

of algorithms that should be banned, especially for applications with significant legal effects. Our recommendations will help ensure that biometric data collection will be limited only to use cases that can be beneficial to consumers (such as diagnostics) and prohibit the use of pseudoscience that can cause massive harm. We urge the Office to set clear guidelines and work with other agencies to establish thoughtful guardrails for how these technologies should be used.

Sincerely,
Nandita Sampath
Policy Analyst