
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

Suresh Venkatasubramanian
Office of Science and Technology Policy
Executive Office of the President
The White House
Washington, DC 20500

Re: RFI Response-Biometric Technologies, Document Number: 2021-21975

Dear Dr. Venkatasubramanian,

On behalf of The Leadership Conference on Civil and Human Rights, a coalition charged by its diverse membership of more than 230 national organizations to promote and protect the civil and human rights of all persons in the United States, we write in response to the Request for Information published in the Federal Register on October 8, 2021, titled Request for Information on Public and Private Sector Uses of Biometric Technologies. Specifically, these comments will focus on the need to ensure that biometric technologies protect civil rights, prevent unlawful discrimination, and advance equal opportunity.

Technological progress should promote equity and justice as it enhances safety, economic opportunity, and convenience for everyone. In 2014, a coalition of civil rights and media justice groups released “Civil Rights Principles for the Era of Big Data,” calling on the U.S. government and businesses to respect and promote equal opportunity and equal justice in the development and use of data-driven technologies. These principles, along with the Obama White House’s subsequent reports on big data, highlighted the need for rules of the road for the private and public institutions whose decisions can ultimately protect or deny civil and human rights.

Today, while the terminology has shifted from “big data” to “AI” and “biometrics,” the issues remain the same and the threats technology can pose to civil rights have only grown. Recognizing this increased urgency, in 2020, The Leadership Conference, along with a number of advocacy and civil rights organizations, released updated Civil Rights Principles. Of relevance to this inquiry, the Civil Rights Principles propose a set of civil rights protections, including:

Ending High-Tech Profiling. Surveillance technologies are empowering governments and companies to collect and analyze vast amounts of information about people. Too often, these tools are deployed without proper safeguards, or are themselves biased. In some cases, surveillance technologies should simply never be deployed. In other cases, clear limitations and robust auditing mechanisms are needed to ensure that these tools are used in a
responsible and equitable way. Law should hold both the government and private actors accountable for abuses.

**Ensuring Justice in Automated Decisions.** Statistical technologies, including machine learning, are informing important decisions in areas such as employment, health, education, lending, housing, immigration, and the criminal legal system. Decision-making technologies too often replicate and amplify patterns of discrimination in society. These tools must be judged not only by their design but also, even primarily, by their impacts — especially on communities that have been historically marginalized. Transparency and oversight are imperative to ensuring that these systems promote just and equitable outcomes, and in many cases the best outcome is to not use automated tools in high-stakes decisions at all.

**Preserving Constitutional Principles.** Enforcement of constitutional principles such as equal protection and due process must keep pace with government use of technology. Search warrant requirements and other limitations on surveillance and policing are critical to protecting fundamental civil rights and civil liberties, especially for communities who have been historically marginalized and subject to disproportionate government surveillance. Moreover, governments should not compel companies to build technologies that undermine basic rights, including freedom of expression, privacy and freedom of association.

**Ensuring that Technology Serves People Historically Subject to Discrimination** Technology should not merely avoid harm, but actively make people’s lives better. Governments, companies, and individuals who design and deploy technology should strive to mitigate societal inequities. This includes improving access to the internet and addressing biases in data and decision-making. Technologies should be deployed in close consultation with the most affected communities, especially those who have historically suffered the harms of discrimination.

**Defining Responsible Use of Personal Information and Enhancing Individual Rights.** Corporations have pervasive access to people’s personal data, which can lead to discriminatory, predatory, and unsafe practices. Personal data collected by companies also often end up in the hands of the government, either through the direct sale of personal data or through data-driven systems purpose-built for the government. Clear baseline protections for data collection, including both primary and secondary uses of data, should be enacted to help prevent these harms.

**Making Systems Transparent and Accountable.** Governments and corporations must provide people with clear, concise, and easily accessible information on what data they collect and how it is used. This information can help equip advocates and individuals with the information to ensure that technologies are used in equitable and just ways. Any technology that has a consequential impact on people’s lives should be deployed with a comprehensive, accessible, and fair appeals process with robust mechanisms for enforcement, and governments and corporations must be accountable for any misuse of technology or data. When careful examination reveals that a new, invasive technology poses threats to civil rights and civil liberties, such technology should not be used under any circumstance.
Evidence that facial recognition technology can impede civil and human rights has never been clearer. With respect to law enforcement use of one specific type of biometrics technology—facial recognition—the evidence of impact on civil and human rights has never been clearer. The Leadership Conference has spoken out against law enforcement use of facial recognition since 2016, highlighting the inherent bias of these tools and their disparate impact on marginalized communities that were already over-policed.iii

In June 2021, The Leadership Conference, along with Upturn and New America’s Open Technology Institute, released “Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology,” which was signed by 40 advocacy organizations.iv Additionally, The Leadership Conference, the ACLU, and more than 45 advocacy organizations wrote a letter to the Biden administration calling for a moratorium on the government use of facial recognition technology.v

Most recently, in July 2021 testimonyvi before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, The Leadership Conference highlighted six of the most pressing civil rights concerns that advocacy organizations have with law enforcement use of facial recognition technology:

1. Regardless of technical accuracy, law enforcement use of face recognition systems could exacerbate the harms of policing in communities that are already targeted by the police.
2. Law enforcement use of face recognition threatens individual and community privacy by allowing invasive and persistent tracking and targeting.
3. Law enforcement use of face recognition can chill First Amendment-protected activities.
4. Law enforcement use of face recognition can easily violate due process rights and otherwise infringe upon procedural justice.
5. Face recognition systems used by law enforcement often rely on faceprints that have been obtained without consent.
6. In addition to racial bias in how law enforcement use face recognition, the technology itself poses disproportionate risks of misidentification for Black, Asian, and Indigenous people.

The Obama administration’s big data reports provided important next steps for future administrations, Congress, and regulators to ensure that technology is used to enhance equal opportunity, not undermine it. And they acknowledged the important role that the civil rights community, and specifically, the Civil Rights Principles, played in informing this critical work. The Biden administration has a critical opportunity to continue this work and to ensure that biometric technologies serve the best interests of each of us. To accomplish this goal, civil rights must be a key part of any public policy framework. We urge you to ensure that the voices of the civil and human rights community are heard in this important, ongoing national conversation.

Thank you for your consideration of these views. If you have any questions, please contact Anita Banerji, Senior Program Director, Media and Tech, at
Sincerely,

Wade Henderson  
Interim President and CEO

Jesselyn McCurdy  
Executive Vice President of Government Affairs

---

1 https://www.civilrightstable.org/civil-rights-principles-for-the-era-of-big-data/
2 https://www.civilrightstable.org/principles/