The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036

202.466.3311 voice
202.466.3435 fax
www.civilrights.org

The Leadership Conference
on Civil and Human Rights

December 21, 2020

Michael Hardin
Director, Entry/Exit Policy and Planning
Office of Field Operations
U.S. Customs and Border Protection, 5th Floor
1300 Pennsylvania Avenue NW
Washington, DC 20229

Submitted via regulations.gov

Re: Docket No. USCBP-2020-0062; 85 FR 74162; RIN: 1651-AB12; FRN: 2020-24707; 8 CFR Parts 215 and 235; Comments in Opposition to Proposed Rulemaking: Collection of Biometric Data from Aliens upon Entry to and Departure from the United States

Dear Mr. Hardin,

On behalf of The Leadership Conference on Civil and Human Rights (The Leadership Conference), a coalition charged by its diverse membership of more than 220 national organizations to promote and protect the civil and human rights of all persons in the United States, we write to express our strong opposition to the above-referenced proposed rule USCBP-2020-0062 relating to the Department of Homeland Security, Customs and Border Protection (DHS or CBP) collection and use of biometrics, which was published in the Federal Register on November 19, 2020. This rule threatens the privacy interests of millions of immigrants and visitors to the United States and would enable the government's surveillance and tracking of people on a massive scale, with the harm disproportionately affecting immigrants and communities of color. Moreover, the rule ignores the fact that facial recognition technology is prone to error, and disproportionately leads to the over-criminalization of people of color, immigrants, LGBTQ people, and other marginalized communities.

The proposed new rule represents a radical departure from today's practices and would authorize DHS to photograph all non-citizens upon entry and departure from the United States. DHS also intends to categorically collect, store, and share "faceprints," or facial recognition scans, which would represent the unique facial geometric measurements of each non-citizen traveler in an untransparent DHS database for up to *75 years*. The rule explicitly allows DHS to share this sensitive biometric data with foreign governments, and federal, state, and local law enforcement to identify individuals for a variety of purposes unrelated to border security. Finally, the NPRM notes that CBP also intends to apply a face-matching algorithm to non-U.S. citizen travelers, which will compare a traveler's faceprint to a gallery of other images of the traveler in the government's possession.

The proposed rule does not address serious civil rights and civil liberties issues that are brought about by DHS's expanded use of facial recognition. Earlier this year, The Leadership Conference was pleased to join with a broad national coalition of civil rights, technology policy, and media justice organizations in endorsing Civil Rights Principles for the Era of Big Data.[1] These principles build on principles that these same groups published in 2014, which included a related report which offers key examples of the ways big data can impact civil rights.[2] We believe the proposed rule violates the Civil Rights Principles for the Era of Big Data, which call for the following to be upheld:

1. **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.

2. **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.

3. **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.

4. **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.

[1] https://www.civilrightstable.org/principles/
[2] https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/; https://bigdata.fairness.io

5. **Defining Responsible Use of Personal Information and Enhance 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.

6. **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.

Through these principles, we and the other signatory organizations highlight the growing need to protect and strengthen key civil rights protections in the face of technological change. As discussed below, because the proposed rule violates these principles, it should be rejected.

First, the proposed rule would enable the government's surveillance and tracking of non-citizen people on a massive scale, facilitating the high-tech profiling of Black, Indigenous and Asian non-citizens. Because the NPRM authorizes CBP to retain, store, and even share the sensitive personal information of millions of non-citizens without safeguards, or proper oversight mechanisms, the likelihood for abuse is high. Additionally, the rules lay out a categorical data-retention policy, which would allow the agency to store the immutable biometric information of millions of non-citizens without meaningful oversight of up to 75 years without providing notice to the person about the ways in which that unique information was shared with a foreign government or domestic officials.

The proposed rule does not do enough to ensure that people historically subject to discrimination are served through the expanded use of facial recognition technologies. Under the proposed rule, DHS would be able to target non-citizens, including those who happen to belong to marginalized communities, without putting in place measures to curtail the algorithmic bias that often results from broad data-collection policies.

Nor will the proposed rule ensure justice in automated decisionmaking. Specifically, a close reading of the proposed rule shows that DHS contradicts the government's own findings on the accuracy of facial recognition technology. While the proposed rule references the second of the National Institute of Science and Technology's (NIST) reports on facial recognition, it fails to recognize the *third and most relevant* *report*, which focused on bias in facial recognition tools.[3] That report found that there was "empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms [NIST] studied."[4] NIST's analysis also found that there were high rates of false positives for Black, Asian, and Indigenous people as well (which include Native American, American Indian, Alaskan Indian and Pacific Island communities).[5] NIST's findings are also consistent with scholarship that has found similar discrepancies based on race, and for Black women in particular.[6] DHS acknowledges these arguments in the proposed rule as it relates to race, gender, and age. Yet, DHS incorrectly asserts that these concerns will be alleviated by putting in place more policies that include more facial recognition, without attacking the central issue of algorithmic bias.

DHS's flawed argument—namely that that expanding the government's use of facial recognition tools will make those tools less biased—cannot lead to an equitable or just solution. Instead, this proposed rule threatens to over-criminalize non-citizens who are already disproportionately targeted by the criminal legal system and immigration enforcement apparatus in part due to other flawed programs that use similar biased algorithms. This is particularly true near the border where we have seen law enforcement agencies act with impunity in using cutting-edge technology to unlawfully target vulnerable migrants. We are also deeply concerned about extending the over-criminalization of non-citizens to public-private partnerships that are not fully disclosed to the public, as these partnerships lack the requisite public transparency and oversight.

The proposed rule does not have a clear definition of responsible use of personal information nor does the proposed rule enhance individual rights. As written, the proposed rule does the exact opposite: nowhere in the rule does it state that the personally identifiable information will not be shared across agencies or used in a manner inconsistent with upholding civil rights and civil liberties. Rather, the proposed rule looks to use public private partnerships to help collect facial recognition data on non-citizens. The proposed rule has no meaningful checks or balances for cases in which the private corporation misuses the personal data of those required to have their faces scanned, photographed, or recorded.

Finally, the proposed rule does not have any meaningful transparency or accountability, which is particularly troubling with facial recognition technology. The proposed rule looks to expand facial recognition use in ports of entry when these tools, as stated previously, are inaccurate for Black, Asian, and Indigenous people, and in particular women belonging to those groups. The proposed rule does not include any accountability or transparency measures that take these inaccuracies into account. Moreover,

[3] Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Standards and Technology NISTIR 8280 (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[4] Id.
[5] Id.
[6] Inioluwa Deborah Raji and Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Massachusetts Institute of Technology Media Lab (January, 24, 2019) https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/; *See also* Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (October 18, 2016) https://www.perpetuallineup.org.

there is no system in place for individuals to challenge facial recognition technology nor are there any meaningful checks to CBP's use of these tools.

For the above stated reasons, we urge you to rescind this proposed rule, and instead adopt policies that conform to these above principles. Thank you for your consideration of our views. If you have any question about these comments, please contact Iman Boukadoum at boukadoum@civilrights.org and Bertram Lee at lee@civilrights.org.

Sincerely,

Vanita Gupta
President and CEO