February, 16, 2021

President Joseph Biden
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear President Biden,

We, the undersigned civil rights, civil liberties, immigrants' rights, religious, free speech, technology and privacy organizations and individuals write to ask your Administration to address the use of facial recognition technology (FRT) by the federal government. The use of FRT in policing, public housing, schools, and other areas of public life poses profound and unprecedented threats to core civil rights and civil liberties. For those reasons, we specifically urge you to:

- Take swift executive action to place a moratorium on all federal government use of FRT and other forms of biometric technology so long as bias pervades these systems and Congress has not acted to authorize the use of the technology in specific circumstances and with sufficient safeguards to protect our privacy interests and prevent harms caused by this dangerous, unregulated technology;

- Prevent state and local governments from using federal funds to purchase FRT or access FRT; and

- Support the Facial Recognition and Biometric Technology Moratorium Act, introduced by Senator Markey. This bill would make a federal moratorium law and would place additional limitations on federal funding of these technologies.

FRT is already responsible for multiple false arrests and mistaken incarcerations of Black men. It disproportionately misidentifies and misclassifies people of color, trans people, women, and other marginalized groups, causing harm in our schools, homes, and communities, and it threatens our core constitutional freedoms including freedom of association and speech, due process protections, and privacy rights. When combined with existing networks of surveillance cameras dotting our urban and suburban landscapes, FRT algorithms could enable governments to track the public movements, habits, and associations of all people, at all times—merely with the push of a button. This kind of all-seeing, all-knowing surveillance evokes science fiction dystopias. But in the year 2021, the persistent tracking of all people in America in public spaces with FRT is no longer relegated to the realm of fiction.

Despite this, the law has failed to keep pace with the technology, leaving all people at grave risk of serious harm. Moreover, following the events of January 6th, 2021, when an armed mob stormed the Capitol building disrupting Congress as it was certifying your election to the office of the Presidency, press reports indicated law enforcement turned to FRT to identify those in the crowd. Troublingly, this use of FRT has generated calls to authorize and expand law enforcement use of FRT. As has been demonstrated by the numerous arrests of those who attacked our Capitol building on January 6th using evidence from their own social media feeds and other sources, face recognition technology was simply unnecessary and, expanding government use of FRT is not the solution. As discussed, FRT is dangerous because it exhibits clear racial, gender, and other biases and it's also dangerous when it does work. Even if the technology worked perfectly, it would facilitate the mass tracking of each person's movements in

public space—something intolerable in a free and open society. We cannot allow its normalization.

**Face recognition technology is particularly dangerous to Black and Brown People, LGBTQ People, Women, and Other Marginalized Communities.**

FRT exhibits particularly disturbing accuracy and bias issues against people with darker skin, LGBTQ people, women—especially women of color—and youth. This bias already has caused irreparable harm. Robert Williams, Michael Oliver, and Nijeer Parks are all Black men wrongly arrested and incarcerated after police falsely identified them using a face recognition system.[1]

While disturbing, these wrongful arrests of Black men are not surprising. A few years ago, MIT scholar Joy Buolamwini made a shocking discovery: Commercially available facial recognition systems did not detect her face until she placed a white mask over it. A Black woman and doctoral candidate at the MIT Media Lab, Buolamwini decided to investigate. In her landmark 2018 study, Buolamwini and her colleagues reported alarming racial and gender disparities in a range of facial recognition technologies marketed by some of the most prominent technology companies in the world. While the systems were relatively accurate when analyzing the faces of white men, Buolamwini found, they failed up to 1 in 3 times when classifying the faces of Black women.[2] Subsequent studies, including by the National Institute of Standards and Technology, confirmed Buolamwini's findings.[3] And members of Congress experienced this disproportionate error rate firsthand when an ACLU of Northern California test of FRT falsely matched 28 members with a mug-shot database.[4]

The arrests of Williams, Oliver, Parks, and others illustrate that these concerns are far from academic. Due to a near complete lack of necessary transparency, we do not know how many times FBI officials have wrongfully arrested or accused someone on the basis of errors in facial recognition systems. In fact, it appears to be the agency's general practice to shield information about the use of FRT from criminal defendants, depriving these individuals of their due process rights.[5] That is unacceptable.

Government agencies should never use technologies that harbor racial, gender, or age bias, let alone use them without providing notice to those who stand accused. Yet, despite these glaring

---

[1] Kashmir Hill, *Another Arrest and Jail Time Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, Detroit Free Press (Jul. 20, 2020), ttps://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

[2] Joy Buolamwini et al., "Gender Shades," MIT Media Lab, available at https://www.media.mit.edu/projects/gender- shades/overview/

[3] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[4] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers*, N.Y. Times (Jul. 26, 2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

[5] Neema Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (Jun. 7, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through.

bias problems, police departments and federal agencies have been using the technology for nearly two decades—in secret and absent any regulation or oversight.

**Face Recognition Technology threatens core constitutional freedoms**

FRT is extraordinarily dangerous to core freedoms even when it works exactly as advertised. Never before has the government possessed a technology that purportedly enables it to keep a running record of every person's every public movement, habit, and association—until now.

If the government can track everyone who goes to a place of worship, attends a political rally, or seeks healthcare for reproductive health or substance use, we lose our freedom to speak our minds, freely criticize the government, pray to the god we want, and access healthcare in private. Americans should feel free to worship their religion, express their right to assemble and protest, and seek substance use treatment or reproductive care without fear that government officials are secretly tracking and cataloging their every move.

These are not hypothetical dangers: FRT is currently being used to conduct precisely this kind of dystopian monitoring. For example, the authoritarian government in China is deploying FRT to control and oppress the religious minority Uighur population, to devastating effect. The technology is so invasive that Chinese authorities use it to track how many times and where individual people pray, whether they enter their homes through the front or back door, and their social and professional associations and contacts.[6]

Closer to home, the Detroit Police Department has purchased FRT to integrate with its networked public surveillance camera system. The system was acquired in secret, without public debate, legislative authorization, or regulations to protect civil rights and liberties.[7]

**Government FRT Use Goes Far Beyond Law Enforcement**

The FBI and other federal law enforcement agencies have been using FRT for years and without explicit authorization or guidance from Congress. That must be corrected, but law enforcement use is not the only concern. FRT is being deployed in schools, workplaces, public housing developments, and healthcare facilities, in many cases to devastating effect. For instance, in schools, Black and brown children are disproportionately disciplined compared to their white counterparts, for the same behavior. Introducing FRT into that already discriminatory environment compounds the negative and discriminatory impacts on Black and brown children, increasing their negative interactions with school officials and greasing the school-to-prison pipeline.

Under no circumstances should these technologies be used to monitor school children, workers, residents, or patients. If it's ever to be used for any purpose in schools, health facilities, or elsewhere, there must be an act of Congress outlining needed standards and safeguards

---

[6] Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, NY. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[7] Clare Garvey & Laura Moy, "America Under Watch," Georgetown University, 2019. https://www .americaunderwatch.com/; Sidney Fussel, *Did a University Use Facial Recognition to ID Student Protesters?*, Wired (Nov. 18, 2020), https://www.wired.com/story/did-university-use-facial-recognition-id-student-protesters/.

protecting people from abuse. Your administration should take any action necessary to pause these uses pending the creation of standards and safeguards to protect against the harms FRT causes.

**The United States should lead the world by placing a moratorium on government use of facial recognition technology**

Over the past two years, activists and local leaders have passed local bans on government use of FRT in at least fifteen municipalities across the country, including Boston, MA, San Francisco, CA, and Jackson, MS. States including Vermont, California, and New York have passed legislation halting some government use of the technology, in light of the substantial racial justice and constitutional concerns detailed above.

But local and state governments are largely powerless to control the way the FBI and other federal agencies use this technology in our communities.

At present, decisions about how to use this dangerous technology are being made by unelected officials, behind closed doors. We respectfully urge you to bring democratic control over this dangerous, biased technology by swiftly signing an executive order that halts the federal government's use of FRT so long as bias pervades these systems and as long as Congress has not acted to authorize the use of the technology in specific circumstances and with sufficient safeguards to protect our privacy and the public interest, and prevent harm. We ask you to limit the ability of state and local governments to use federal money to purchase FRT. We also ask your administration to support the Facial Recognition and Biometric Technology Moratorium Act, introduced by Senator Markey. This bill would make a federal moratorium law, until Congress acts to authorize its use, and would place additional limitations on federal funding of these technologies.

Thank you for your consideration of this urgent matter. If you have any questions, please contact Kate Ruane, American Civil Liberties Union, kruane@aclu.org.

Sincerely,

Organizations:

Access Now
Advocacy for Principled Action in Government
AFT Massachusetts
American Civil Liberties Union
American Library Association
American Muslim Empowerment Network (AMEN)
Amnesty International - USA
Asian Americans Advancing Justice | AAJC
Boston Public Library Professional Staff Association, Local 4928 MLSA-AFT
Boston Teachers Union
Campaign for a Commercial-Free Childhood
CAIR Washington
Center for Constitutional Rights
Center on Privacy and Technology at Georgetown Law
CertNexus
Charles Hamilton Houston Institute for Race and Justice at Harvard Law School

Civil Liberties Defense Center
Climate Defense Project
Council on American-Islamic Relations, MA
Defending Rights & Dissent
Densho
DesigniIT International aka KnowledgeHouseAfrica
Earthworks
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Encode Justice
Fight for the Future
Free Press Action
Freedom House
Indivisible Plus Washington
John T. Williams Organizing Committee
Library Freedom Project
Massachusetts Pirate Party
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
New England Library Association
OCA - Asian Pacific American Advocates
Open The Government
Palestine Legal
Poligon Education Fund
Project On Government Oversight
Restore The Fourth
S.T.O.P. - The Surveillance Technology Oversight Project
South Asian Americans Leading Together (SAALT)
The Freedom to Read Foundation
The Leadership Conference on Civil and Human Rights
Welcome Project, Inc.

Individuals:

Professor Elsa Auerbach, University of Massachusetts
Joy Buolamwini, Founder of the Algorithmic Justice League
Isaac Kamola, Trinity College, Hartford CT