July 1, 2020

The Honorable Mitch McConnell
Majority Leader
U.S. Senate
Washington D.C., 20510

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington D.C., 20515

The Honorable Chuck Schumer
Minority Leader
U.S. Senate
Washington D.C., 20510

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
Washington D.C., 20515

Dear Leaders McConnell and Schumer, Speaker Pelosi and Leader McCarthy:

The undersigned privacy, civil liberties, civil rights, and investor and faith groups write to urge you to take action to prevent the continued use and investment in face recognition technology, including by (1) passing legislation, like the *Facial Recognition and Biometric Technology Moratorium Act of 2020*, which would halt the use of face recognition and prevent federal funds from being used to purchase such technology, (2) stop continued federal funding of invasive and discriminatory technologies by police, including face recognition; and (3) ensure that any policing reform bill that funds body or dash cameras prohibits the use of face recognition used in conjunction with these accountability tools.

Efforts to reform policing must address the bloated and discriminatory surveillance architecture that has contributed to police abuses. As thousands gather to demonstrate and demand justice for George Floyd, Tony McDade, Breonna Taylor and countless other Black people who have been killed by police, it is time Congress responds to these demands and eradicates systemic racism and tools that facilitate discriminatory policing – including face recognition technology. Indeed, the case of Robert Williams, disclosed just this week, underscores how technologies like face recognition can exacerbate existing police abuses and result in improper arrest, detention, or even worse.

On January 9, 2020, Robert Williams was wrongfully arrested by the Detroit Police Department (DPD) due to an erroneous face recognition match from a blurry surveillance photo. Mr. Williams, a Black man, was falsely matched with an image of a shoplifting suspect captured on a store's surveillance video and then scanned through face recognition software operated by the Michigan State Police. As a result of that false match, Mr. Williams was arrested in broad daylight on his front lawn, in front of his wife and two young daughters, and in plain sight of his neighbors. He was held for nearly 30 hours in a crowded and dirty cell. Since the arrest, the DPD and Wayne County have continued their efforts to cover up what happened, including by ignoring both court orders and FOIA requests for records relating to this case.[1]

[1] Victoria Burton-Harris and Philip Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020) *available at* https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/.

As Mr. Williams case demonstrates, face recognition technology is dangerous when wrong. But, it would be dangerous even if it was accurate. Face recognition poses a particular threat in our communities for several reasons.

One, it gives government agencies the unprecedented power to track who we are, where we go, and who we know. Companies marketing this technology to the government boast that it can be used to track people in real-time, reconstruct past movements from video footage, or identify a hundred individuals from a single photo. This capability threatens to create a world where people are watched and identified as they attend a protest, congregate outside a place of worship, visit a medical provider, or simply go about their daily lives. In the U.S., this technology has already been used to identify people protesting police brutality; abroad, it has been deployed to systematically control a religious minority group.

Two, as we have already seen, the harms associated with this technology will likely fall disproportionately on communities of color. Numerous studies, including the most recent report from the National Institute of Standards and Technology, have found that leading face recognition algorithms are less accurate on certain groups, including women and people with darker skin.[2]

But, even if the technology were accurate, it cannot be dissociated from the racist policies that are embedded in policing. Today, police surveillance cameras are disproportionately installed in communities of color, keeping a constant watch. Across the U.S., communities of color face arrest for a variety of crimes at far higher rates than white people, and suffer overwhelming disparities at every single stage of the criminal punishment system – from street-level surveillance and profiling all the way through to sentencing and conditions of confinement.[3] Face recognition will not fix these problems; it is likely to make them worse by providing another flawed tool that will be disproportionately targeted at communities of color.

Three, this technology has been deployed largely in secret, undermining principles of democratic governance. Congress has not passed a law explicitly authorizing face recognition for law enforcement use that clearly dictates what safeguards must be in place. Yet, federal agencies, including the FBI, have continued to expand the use of face recognition without safeguards. The FBI has access to over 640 million photos for face matching, including the driver's license databases of 20 states and passport application photos,[4] has performed hundreds of thousands of face recognition searches, and is now reportedly piloting new uses of the technology. Despite this, the agency appears to be skirting even its most basic obligation to provide notice to individuals who have this technology used against them. Congress must take action to prevent

---

[2] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (Dec. 2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. *Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies,* Association for Computing Machinery US Technology Policy Committee (June 30, 2020), available at https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf.

[3] Megan Stevenson and Sandra Mayson, *The Scale of Misdemeanor Justice*, 98 Boston University Law Review 731 (2018).

[4] U.S. Gov't Accountability Office, GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS (June 2019), *available at* https://www.gao.gov/assets/700/699489.pdf.

the harms associated with face recognition and other invasive and discriminatory surveillance technologies. Thus, it should pass legislation like the *Facial Recognition and Biometric Technology Moratorium Act of 2020* that will halt the use of face recognition technology and prohibit use of funding for such technology. In addition, it should stop continued investment and funding in discriminatory and invasive technologies, like face recognition.

Sincerely,

Algorithmic Justice League
American Civil Liberties Union
Amnesty International - USA
Arab American Institute
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center on Privacy & Technology at Georgetown Law
CenterLink: The Community of LGBT Centers
Charles Hamilton Houston Institute for Race and Justice
Chula Vista Partners in Courage
Congregation of Sisters of St. Agnes
Council on American-Islamic Relations (CAIR)
Defending Rights & Dissent
Demand Progress
Dominican Sisters ~ Grand Rapids
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
Equality North Carolina
Fight for the Future
Free Press Action
The Greenlining Institute
Harrington Investments, Inc.
Indivisible SF
LGBT Technology Partnership & Institute
Liberty Coalition
MediaJustice
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Project On Government Oversight
Racial Justice Committee of the San Francisco Public Defender
Region VI Coalition for Responsible Investment
Restore The Fourth
S.T.O.P. - The Surveillance Technology Oversight Project
Sisters of St. Dominic of Caldwell
South Bay People Power
Starting Over, Inc
TRANScending Barriers
Ursuline Sisters of Louisville