February 14, 2022

A Call To Federal and State Agencies To End the Use of ID.me and Other Facial Recognition Identity Verification Services

We, the undersigned organizations, applaud the IRS and Treasury for the decision to end the use of ID.me in response to concerns raised by privacy experts, lawmakers, and the public. We call on other federal and state government agencies using or considering use of ID.me to follow suit and cancel the use of ID.me and other facial verification tools. Facial recognition technology has been found to be biased, have a disproportionate impact on people of color and other marginalized communities, and the use of the technology has serious implications for privacy and civil liberties. This third-party technology should not be forced upon individuals by government agencies.

Several federal agencies and states are already using ID.me's face verification service. According to reports, 27 states have contracted with ID.me as well as federal agencies like the Department of Labor, the Department of Veteran Affairs, and the Social Security Administration.[1] This recent pivot by federal agencies and states towards the use of facial recognition technology is troubling for several reasons.

Facial recognition technology has been shown to have a racial bias and disproportionate impact on people of color. For example, facial recognition has led to the wrongful arrest of Black men in at least three documented incidents.[2] A National Institute of Standards and Technology ("NIST") study found "for one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm."[3] False positives will only become a bigger issue as fraudsters increasingly seek ways to trick face verification systems.[4]

Although disparate rates of false negatives were less of a problem in the NIST study, the absence of data about ID.me's actual performance in real-world applications means that the public lacks information about ID.me's face verification   failure rate, including whether the system disproportionately fails to verify the identities of people of color. We remind federal agencies using ID.me and other face verification services that they have an affirmative legal obligation under Title VI of the Civil Rights Act to ensure that recipients of federal funds are not engaging in practices that discriminate on the basis of race. This obligation under Title VI also extends to state agencies receiving federal funds.

---

[1] Shawn Donnan and Dina Bass, *How Did ID.me Get Between You and Your Identity*, Bloomberg Businessweek (Jan. 20, 2022), https://www.bloomberg.com/news/features/2022-01-20/cybersecurity-company-id-me-is-becoming-government-s-digital-gatekeeper.

[2] 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.

[3] National Institute of Standards and Technology, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[4] Parmy Olsen, *Faces Are The Next Target For Fraudsters*, WSJ (July 7, 2021), https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828.

There is no indication that the federal and state entities using ID.me performed any type of meaningful assessment that considered whether ID.me's facial recognition identity verification will have a disproportionate impact on people of color or other marginalized groups.[5] And make no mistake, ID.me's problems will not be confined to people of color.[6] Identity verification by facial recognition may be inaccessible for individuals with certain disabilities, including blindness.[7] Additionally, the issues with implementing such a system go beyond questions of accuracy as we've seen with the use of ID.me for access to unemployment benefits.[8] Requiring access to reliable internet service and a quality webcam or smartphone camera will undoubtedly exclude numerous older Americans as well as people from low income and other marginalized communities.

The use of ID.me by federal and state entities is also problematic in light of ID.me's use of 1:many facial recognition. 1:many searches present even greater bias risks and risks to privacy and civil liberties. We do not know which agencies contracting with ID.me simply ignored this use or were unaware of it. Either scenario is disturbing. What is clear is that ID.me misled the public. The company initially claimed it only used 1:1 facial recognition only to later backtrack and admit it does also use 1:many facial recognition.[9] The about-face by ID.me calls into question how the company is using the data, particularly the face prints, it collects from members of the public forced to use its service. ID.me's descriptions of its use of facial recognition tend to be overly favorable if not misleading.[10]

---

[5] *See, e.g.*, IRS Privacy Impact Assessment for ID.me (June 15, 2021), https://www.irs.gov/pub/irs-pia/id-me-pia.pdf.

[6] Andrew Kenney, *No Internet, No Unemployment: Solving This ID.me Glitch Took Two Months And A Journey Across The Rural Front Range*, CPR News (July 7, 2021), https://www.cpr.org/2021/07/07/colorado-unemployment-idme-glitch-internet-access/.

[7] Jonathan Keane, *Facial Recognition Apps Are Leaving Blind People Behind*, VICE (March 22, 2016), https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind; Alexandra Mateescu, Data & Society, *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care* 54 (2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf.

[8] Monica Williams and Joe Ducey, *ID.me says unemployment delays are not their fault; AZ system had problems from the start*, ABC15 Arizona (Mar. 18, 2021), https://www.abc15.com/news/let-joe-know/id-me-says-unemployment-delays-are-not-their-fault-az-system-had-problems-from-the-start; David Hodges and Emery Eisner, *ID.me delays leave Carolinians without unemployment money for weeks*, WBTV (May 3, 2021), https://www.wbtv.com/2021/05/03/idme-delays-leave-carolinians-without-unemployment-money-weeks/; Josh Lyle, *EDD verification delayed by long waits for ID.me*, abc10 (Jan. 15, 2021), https://www.abc10.com/article/money/edd-verification-id-me-delay/103-b3a5de8e-9150-464f-9020-7fff939b9b17; Jennifer Lewke, *News10NBC Investigates: Many struggle to get through ID.me process*, News10NBC (Sept. 16, 2021), https://www.whec.com/news/many-struggle-to-get-through-idme-process/6240392/.

[9] Tonya Riley, *ID.me CEO backtracks on claims company doesn't use powerful facial recognition tech*, Cyberscoop (Jan. 26, 2022), https://www.cyberscoop.com/id-me-ceo-backtracks-on-claims-company-doesnt-use-powerful-facial-recognition-tech/; Ina Fried, *ID.me CEO apologies for misstatements on IRS facial recognition*, Axios (Jan. 27, 2022), https://www.axios.com/idme-ceo-apologizes-misstatements-irs-facial-recognition-88ce2ee2-9ae9-426c-b69e-c0b42ad82f61.html.

[10] Dr. Joy Buolamwini, *The IRS Should Stop Using Facial Recognition*, op-ed The Atlantic (Jan. 27, 2022), https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386/.

The use of a third-party face verification service also creates needless security issues facilitated by government agencies forcing individuals to hand over biometric data to a private company.[11] Biometric data, particularly faceprints, are increasingly becoming targets for fraudulent activity.[12] The likely result of federal and state agencies using faces as a credential to access sensitive information will be large-scale data breaches of a credential that cannot easily be changed.[13]

The issues described above are all exacerbated by one simple fact: There is no comprehensive law regulating the collection, use, disclosure, and retention of biometric data. This alone should have stopped any government agency in its track when it considered the use of facial verification. Facial recognition is a powerful technology that has serious potential for bias as well as significant implications for our privacy and civil liberties.[14]

The recent announcement by ID.me to offer identity verification without facial recognition and to allow users to delete their photos does not solve the issues described above and raises additional questions. The option is not automatically granted to users of ID.me. It is only an option that government agencies can implement if they choose and only if the agency has "procured [ID.me's] offline option."[15] Furthermore, the vast majority of people are not aware of the risks associated with handing over their sensitive biometric information and making this tech "optional" puts the onus on the individual to have the right information about those risks.

Additionally, users of ID.me that needed to verify their identity with a human operator have faced significant obstacles, wait times lasting hours, and delays lasting days or weeks.[16] Forcing individuals to choose between submitting to facial recognition scans and these burdens would be no choice at all. Any alternative to facial recognition must be an equally accessible option, and we are concerned ID.me will be unable to provide that based upon its history of user interaction.

Also, the mere fact that individuals will be directed to ID.me's face verification through the government may give a false sense of security in using the technology. Many individuals may still either be forced to submit to face verification or assume it is safe unless federal and state agencies cease the use of face verification all together. Sensitive biometric data should not be used to access government services.

---

[11] *See* Joseph Marks, *IRS dodged a cyber minefield by ditching facial recognition*, Washington Post (Feb. 8, 2022), https://www.washingtonpost.com/politics/2022/02/08/irs-dodged-cyber-minefield-by-ditching-facial-recognition/.
[12] Parmy Olsen, *Faces Are The Next Target For Fraudsters*, WSJ (July 7, 2021), https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828.
[13] *See* Andy Greeberg, *OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers*, Wired (Sept. 23, 2015), https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/.
[14] Even a 100% accurate facial recognition system poses risk and arguably poses more risks to privacy and civil liberties given its potential for mass, indiscriminate surveillance.
[15] ID.me, *ID.me Announces Options for Selfie Deletion and Identity Verification without Automated Facial Recognition* (Feb. 8, 2022), https://insights.id.me/press-releases/id-me-announces-options-for-selfie-deletion-and-identity-verification-without-automated-facial-recognition/.
[16] *See, e.g.*, Todd Feathers, *Facial Recognition Failures Are Locking People Out of Unemployment Systems*, Vice (June 18, 2021), https://www.vice.com/en/article/5dbywn/facial-recognition-failures-are-locking-people-out-of-unemployment-systems.

It's not clear how meaningful ID.me's option is for users to delete photos. ID.me's current policy states that personal information is kept for "the duration of your relationship with ID.me plus seven and a half years."[17] Does ID.me keep photos for seven and a half years after a deletion request? Does ID.me use these photos as part of their 1:many facial recognition searches?

The safest and best "option" is for federal and state government agencies to end their use of this perilous technology on the public – through ID.me or any other vendor.

Signatories:

Access Now
ACLU
Advocacy For Principled Action In Government
Algorithmic Justice League
Amnesty International USA
Asian Americans Advancing Justice – AAJC
Brooklyn Defender Services
Center for Law and Social Policy (CLASP)
Center on Privacy & Technology at Georgetown Law
Consumer Action
Consumer Federation of America
Constitutional Alliance
Council on American-Islamic Relations, Washington Chapter (CAIR-WA)
Data & Society Research Institute
Defending Rights & Dissent
Demand Progress Education Fund
Densho
Distributed AI Research Institute (DAIR)
Due Process Institute
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Government Information Watch
Indivisible Plus Washington
Japanese American Citizens League
Jobs with Justice
Just Futures Law
Kairos
Massachusetts Jobs with Justice
Media Alliance
Muslim Justice League
NAACP LEGAL DEFENSE AND EDUCATIONAL FUND, INC (LDF)
National Immigration Law Center
National Workrights Institute

---

[17] ID.me, *Privacy Policy* (Last updated Feb. 4, 2022), https://www.id.me/privacy.

New America's Open Technology Institute
Open Mic
Organization for Identity and Cultural Development
PolicyLink
Privacy Rights Clearinghouse
The Project for Privacy and Surveillance Accountability
Project On Government Oversight
Public Citizen
Real Change
Restore The Fourth
Secure Justice
Surveillance Technology Oversight Project
X-Lab