

United States Senate

WASHINGTON, DC 20510

May 18, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan:

We write to urge the Federal Trade Commission (FTC) to investigate evidence of deceptive statements made by ID.me — a provider of identity verification services widely used by federal and state government agencies — about its use of facial recognition.

Federal and state government agencies have turned to ID.me, a commercial digital identity provider, to verify online applicants for government services. In January, the Internal Revenue Service's (IRS) use of ID.me set off a long-overdue public debate about the appropriateness of requiring facial recognition technology as a condition of accessing government services. To the IRS' credit, after the public outcry, the agency quickly changed course and announced on February 7, 2022, that it would no longer require the use of facial recognition. However, dozens of other federal and state agencies continue to require applicants to submit to facial recognition scanning by ID.me in order to access essential services like state Unemployment Insurance.

In public statements and blog posts, ID.me has frequently emphasized the difference between two types of facial recognition: one-to-one versus one-to-many. In one-to-one facial recognition, one photo is compared to a single other photo to confirm that both are of the same person. ID.me uses one-to-one facial recognition to compare an applicant's submitted selfie against a photo the applicant provides of their driver's license or passport. In contrast, one-to-many facial recognition involves comparing a face against a database of other faces to find any potential matches.

Americans have particular reason to be concerned about the difference between these two types of facial recognition. While one-to-one recognition involves a one-time comparison of two images in order to confirm an applicant's identity, the use of one-to-many recognition means that millions of innocent people will have their photographs endlessly queried as part of a digital "line up." Not only does this violate individuals' privacy, but the inevitable false matches associated with one-to-many recognition can result in applicants being wrongly denied desperately-needed services for weeks or even months as they try to get their case reviewed. This risk is especially acute for people of color: NIST's Facial Recognition Vendor Test found that many facial recognition algorithms have rates of false matches that are as much as 100 times higher for individuals from countries in West Africa, East Africa and East Asia than for individuals from Eastern European countries. This means Black and Asian Americans could be

disproportionately likely to be denied benefits due to a false match in a one-to-many facial recognition system.

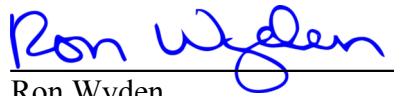
Since at least June of 2021, ID.me published blog posts and white papers on its website that claimed, unambiguously, that it did not use one-to-many facial recognition. In these materials, the company repeatedly emphasized that one-to-one facial recognition was more accurate and less biased than one-to-many – distancing its system from criticisms of facial recognition raised by experts, such as the evidence that many systems are less accurate at identifying people of color. On January 24, 2022, after the backlash against the IRS’ announcement about ID.me, the company’s Chief Executive Officer Blake Hall published a statement in which he emphasized once again that ID.me “does not use 1:many [one-to-many] facial recognition,” calling it “problematic” and “tied to surveillance applications.”

Just two days after this unqualified public denial, Mr. Hall reversed course, in a LinkedIn post in which he admitted that ID.me does use one-to-many facial recognition. Within days, the company edited the numerous blog posts and white papers on its website that previously stated the company did not use one-to-many to reflect the truth. According to media reports, the company’s decision to correct its prior misleading statements came after mounting internal pressure from its employees. CyberScoop obtained and published internal ID.me corporate chats from the days before Mr. Hall’s LinkedIn post in which multiple employees expressed concerns about the company’s deceptive public statements about one-to-many facial recognition. One employee ended their message about the company’s statements by saying, “doing one thing and saying another [is] bound to land us in hot water.”

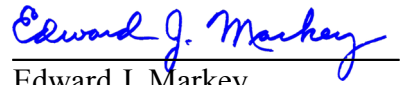
ID.me’s statements, therefore, appear deceptive, and were harmful in two ways. First, they likely misled consumers about how the company was using their sensitive biometric data, including that it would be stored in a database and cross-referenced using facial recognition whenever new accounts were created in the future. Second, the statements may have influenced officials at state and federal agencies as they chose an identity verification provider for government services. These officials had the right to know that selecting ID.me would force millions of Americans – many of them in desperate circumstances – to submit to scanning using a facial recognition technique that ID.me itself acknowledged was problematic. We therefore request that you investigate evidence of ID.me’s deceptive public statements to determine whether they constitute deceptive and unfair business practices under the Section 5 of the FTC Act.

Thank you for your attention to this urgent matter.

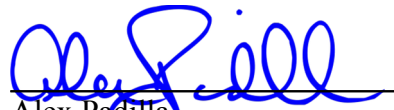
Sincerely,



Ron Wyden
United States Senator



Edward J. Markey
United States Senator



Alex Padilla
United States Senator



Cory A. Booker
United States Senator