



CYBERSCOOP

CLOSE AD X

PRIVACY

ID.me CEO backs powerful facial

The company had said it did

BY TONYA RILEY • JANUARY 26, 2025

ny doesn't use



Continue to CyberScoop



Get our latest cybersecurity news first on Google.

CLICK HERE!



SHARE



I dentity verification company ID.me uses a type of powerful facial recognition that searches for individuals within mass databases of photos, CEO Blake Hall explained in a LinkedIn post on Wednesday.

CYBERSCOOP

The post follows a news release from the company last week stating directly that: “Our 1:1 face match is comparable to taking a selfie to unlock a smartphone. ID.me does not use 1:many facial recognition, which is more complex and problematic.” Hall’s [post on Wednesday](#) confirms that ID.me does indeed use 1:many technology.

Privacy advocates say that both versions of facial recognition pose a threat to consumers. In addition to numerous studies demonstrating the technology is less accurate on non-White skin tones, amassing biometric data can prove a huge security risk.

“Governments and companies are amassing these databases of your personal biometric information, which unlike databases, of credit cards, cannot be replaced,” explained Caitlin Seeley-George, campaign director at nonprofit Fight for the Future. “And these are databases that are highly targeted by hackers and information that can absolutely be used in ways that are harmful to people.”

In the Wednesday LinkedIn post Hall said that 1:many verification is used “once during enrollment” and “is not tied to identity verification.”

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)

“We avoid disclosing methods we use to stop identity theft and organized crime as it jeopardizes their effectiveness,” Hall writes. He pointed to a recent [indictment of a New Jersey man last week by the FBI](#) after the man bypassed ID.me’s verification system and stole nearly a million dollars in unemployment benefits.

The LinkedIn post follows internal discussions expressing concerns that the company’s public statements had been inaccurate.

“We could disable the 1:many face search, but then lose a valuable fraud-fighting tool. Or we could change our public stance on using 1:many face search,” an engineer wrote in a message posted to a company Slack channel on Tuesday. “But it seems we can’t keep doing one thing and saying another as that’s bound to land us in hot water.”

CYBERSCOOP

The internal messages, obtained by CyberScoop, also imply that the company discussed the use of 1:many with the IRS in a meeting.

“I was in a conversation with the IRS on 1/19 where we explicitly discussed using AWS Recognition for 1:many face search,” the engineer wrote. “This seems like it could be troublesome so I wanted to post this here to discuss next steps.”

While [ID.me](#) lists Paravision and iProov as biometric technology partners, it does not appear to disclose its relationship with Amazon’s facial recognition product. Amazon isn’t mentioned in a recently released white paper explaining ID.me’s technology.

ID.me confirmed Thursday in an email to CyberScoop that the company uses Amazon’s Rekognition facial recognition product.

ID.me’s database consists of images uploaded directly to ID.me and not external sources, a company spokesperson told CyberScoop in an email. ID.me retains selfies uploaded during the verification process for seven and a half years after an account is closed, per federal guidelines. Biometric information is shared with a government agency “when there is apparent fraud and identity theft tied to the account associated with the agency,” according to the company’s

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)

Seeley-George says the fact that ID.me mislead the public about the type of technology it is using raises serious concerns about government agencies using facial recognition technology.

“This is just another example where ID.me is falsely portraying its tool and how it will be used on millions of people,” said Seeley-George. “This is not the type of product that we should be asking millions of people to be using if they have to lie about what it’s doing.”

Jay Stanley, senior policy analyst with the American Civil Liberties Union’s Speech, Privacy and Technology Project said that the use of 1:many raises even more questions about the technology’s accuracy, what determines if an individual is placed on a blocklist and what due process is in place for blocked individuals.

“They say that it’s not tied to identity verification, that it does not block human users from identifying their identity, but **CYBERSCOOP** on that list, how can it not cause you problems?” He said.

In reference to its 1:1 matching, ID.me [stated in a press release](#) that “there was no statistically significant difference in the propensity to pass or fail the face match step across demographic groups, including groups with different skin tones, as corroborated by NIST, ID.me, and a state government agency.” The company’s 1:1 or 1:many facial recognition technologies have not been made available for public auditing.

ID.me declined to share how many attempts a user is given before a potentially fraudulent photo is escalated to review. “Through January 25th, 2022 there have been 20,901,406 accounts that have been secured against identity theft with 1:many fraud checks,” the spokesperson wrote. “For every 10,000 identity proofing attempts, on average 8 attempts would have been flagged for review.”

“It’s all very opaque,” Stanley said. “And that’s a recipe for injustice.”

Multiple studies have shown that, even in ideal lab conditions, facial recognition technology disproportionately results in false positives when used on people of color. Some lawmakers have

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)

The new information adds to growing scrutiny over the IRS's recently announced decision to use the technology to verify credentials for its online web portal. The move has been questioned by privacy advocates as well as lawmakers, including Sen. Ron Wyden, D-Ore.,

Concerns with the company aren't new. Users navigating the company's technology [to receive unemployment benefits during the pandemic reported](#) hours-long wait for verification, incorrectly rejected matches, and waiting months to rectify denials.

Cybersecurity reporter Brian Krebs [reported a similar experience](#) using the company's technology to create IRS credentials through the system.

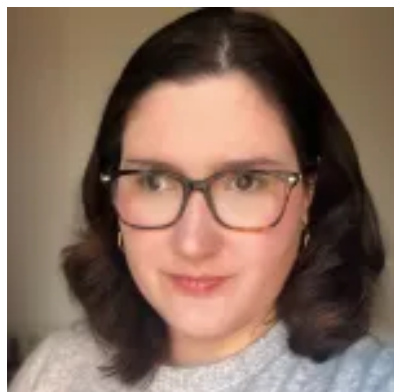
CYBERSCOOP

In addition to the IRS, ID.me has contracts with the Veteran's Affairs Department and Social Security Administration. ID.me says it discloses its use of 1:many facial recognition to government partners "when active."

The IRS did not respond to questions sent by CyberScoop.

Updated 1/26/22: *To include additional information about internal company discussions and comment from the ACLU.*

Updated 1/27/22: *To include responses from ID.me.*



Written by Tonya Riley

Tonya Riley covers privacy, surveillance and cryptocurrency for CyberScoop News. She previously wrote the Cybersecurity 202 newsletter for The Washington Post and before that worked as a fellow at Mother Jones magazine. Her work has appeared in Wired, CNBC, Esquire and other outlets. She received a BA in history from Brown University. You can reach Tonya with sensitive tips on Signal at 202-642-0021. PR pitches to Signal will be ignored and

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)

[BIOMETRICS](#)[PRIVACY](#)[RON WYDEN](#)[ID.ME](#)[IDENTITY MANAGEMENT](#)[FACIAL RECOGNITION](#)[IRS](#)

More Scoops >



Weaponized AI: The new frontier of fraud and identity spoofing

As fake identity fraud is projected to cause \$40 billion in losses next year, leaders must abandon static security in favor of rapid-iteration, AI-enabled defenses that adapt...

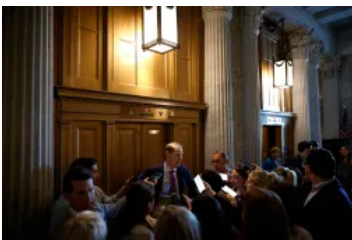
CYBERSCOOP

BY FERNANDA SOTTIL



As 23andMe declares bankruptcy, privacy advocates sound alarm about DNA data

BY DEREK B. JOHNSON



Exclusive: Senator calls on Commerce to tighten proposed rules on exporting surveillance, hacking tech to problematic nations

BY TIM STARKS

Nationwide push to require social media age verification raises questions about privacy, industry standards

BY TONYA RILEY

Illinois' biometric privacy law provides blueprint as states seek to curb data collection

BY TONYA RILEY

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)

BY TONYA RILEY

ID.me misled IRS on processing times for identity verification, congressional investigators found

BY TONYA RILEY

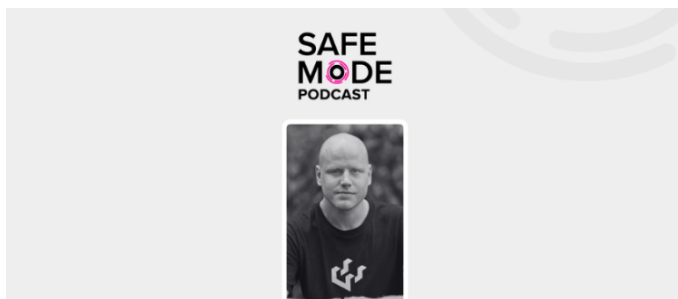
Latest Podcasts



🎙 What the Section 702 lapse means for cybersecurity



🎙 AI-adaptable security platforms are critical for autonomous decision-making



🎙 Defending in the middle of the vulnpocalypse

Get our latest cybersecurity news first on Google.

CLICK HERE!



 The Vulnpocalypse arrived early

Government

CISA promotes a fresh way to deter cyberattackers: Lie to them

CYBERSCOOP

Coast Guard, FBI board US-bound foreign ships in order to probe for cyberattacks

What's next for CISA's CDM program that gives cybersecurity tools to federal agencies

Supreme Court denies Trump request to allow USPS mail ballot changes

Technology

Researchers say OpenAI agents were behind May hacking campaign targeting RubyGems

The G7 tells industry to hurry up and prep for post-quantum encryption

FCC proposes public scorecard to rate telecoms on anti-robocall efforts

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)

Threats

Authorities seize popular, long-running DDoS-for-hire service domains

Cisco warns customers of actively exploited zero-day in email gateways

Five alleged leaders of Black Axe's operations in South Africa extradited to US

GitLab's critical flaw is already drawing internet-wide probes

CYBERSCOOP

Policy

Cyberattack causes a flight delay? Airlines won't owe you a hotel or meal

Hawley probes OpenAI over Hugging Face breach

Governments 'buying time' in race between innovation, security, national cyber director says

FTC rescinds policy statement requiring health apps to notify customers after a breach

Get our latest cybersecurity news first on Google.

[CLICK HERE!](#)



ABOUT US

FEDSCOOP

CYBERSCOOP
DEFENSESCOOP

STATESCOOP

EDSCOOP

CYBERSCOOP

AISCOOP

NEWSLETTERS

ADVERTISE WITH US

AD SPECS

(202) 887-8001

HELLO@CYBERSCOOP.COM



Get our latest cybersecurity news first on Google.

CLICK HERE!