The flap over facial recognition

In recent years, police forces have developed quite the appetite for facial recognition technology with massive federal databases dedicated to these efforts. It's been estimated that about one-in-two US adults are logged in one law enforcement facial recognition network, according to a Center on Privacy & Technology at Georgetown Law report.

Members of the United States Congress recently introduced a bill designed to limit the use of facial regognition. Called *The Facial Recognition and Biometric Technology Moratorium Act of 2020*, it would prohibit the use of U.S. federal funds to acquire facial recognition systems or “any biometric surveillance system” use by federal government officials. It would also withhold federal funding through the Byrne grant program for state and local governments that use the technology.

The bill is sponsored by Senators Ed Markey (D-MA) and Jeff Merkley (D-OR) as well as Representatives Ayanna Pressley (D-MA) and Pramila Jayapal (D-WA).

As well, the New York City Council today voted 44 to 6 in favor of the Public Oversight of Surveillance Technology (POST) Act, a bill that requires the New York City Police Department (NYPD) to disclose their use of surveillance technologies. The POST Act also mandates that the NYPD develop policies on how it deploys those tools, as well as establish oversight of the department’s surveillance programs to ensure they remain compliant.

In another government action, Rep. Jimmy Gomez (D-CA) has asked Amazon CEO Jeff Bezos about exactly how the company plans to implement a one-year moratorium on facial recognition sales to police. Amazon announced the moratorium in a brief blog post one week ago today.

The letter asks when Amazon plans to submit Rekognition for evaluation by the Department of Commerce’s National Institute of Standards and Technology (NIST). A NIST spokesperson last week told VentureBeat that Amazon has yet to submit Rekognition or any other algorithm for review under its Facial Recognition Vendor Test program. Previous NIST analysis, as well as audits by the Gender Shades project in 2018, found that facial recognition systems generally work best on White men and worst on women with dark skin.

This comes on the heels of a 2019 National Institute of Standards and Technology (NIST) study found that facial recognition algorithms are woefully riddled with flaws overall. Minority groups including Asians and African Americans had higher false positives in one-to-one matching. At times, these false-positives increased by a factor of up to 100 for these groups. The report also discovered gender biases, as African American females had a higher rate of false positives for one-to-many matching datasets.

In response, recent moves by IBM, Amazon, and Microsoft mark a rare moment of self-regulation within the private sector. The moratorium on sharing the technology with the police arrives as academics, civil rights advocates, and the company’s own employees have all expressed concerns that Amazon’s Rekognition facial-recognition technology will lead to policing abuses.

Dr. Charles Romine from the U.S. Department of Commerce’s National Institute for Standards and Technology testified before Congress in January that NIST was in talks with Amazon to evaluate its Rekognition software. However, a NIST spokesperson today told VentureBeat that Amazon has not submitted any algorithm for analysis under the Facial Recognition Vendor Test (FRVT) program.

The American Civil Liberties Union (ACLU) is a supporter of facial recognition ban legislation passed in places like San Francisco and frequently called attention to Rekognition classifying lawmakers and NFL athletes as criminals. The ACLU also filed a lawsuit targeting Amazon and Microsoft government contracts last fall.

“It took two years for Amazon to get to this point, but we’re glad the company is finally recognizing the dangers face recognition poses to Black and Brown communities and civil rights more broadly,” said ACLU Northern California tech director Nicole Ozer said in a statement shared with VentureBeat. “We urge Microsoft and other companies to join IBM, Google, and Amazon in moving towards the right side of history.”

Microsoft and IBM have recently made similar announcements, respectively pausing and abandoning facial recognition research altogether. Controversial startup Clearview AI, on the other hand, says it plans to continue supplying police with the problematic tech. Regardless of what positions companies take, larger questions remain wholly unanswered about why these technologies have been allowed to disproportionately target minority populations for so long. Moving forward, even larger concerns remain.

Microsoft President Brad Smith says the U.S. needs to first enact a federal law on facial-recognition tech before the company will consider selling it to police departments.

“We’ve decided that we will not sell facial-recognition technology to police departments in the United States until we have a national law in place grounded in human rights that will govern this technology,” Microsoft President Brad Smith told Washington Post Live.

In addition, Smith says Microsoft will be extra careful in determining which customers will get access to the company’s facial-recognition system. “We’ll also put in place some additional review factors, so that we’re looking at other potential uses of this technology that go even beyond what we already have,” he said.

Not every tech company is following the lead of Amazon and IBM when it comes to facial-recognition technology. Clearview AI – a startup that’s amassed over 3 billion images of people that were posted on the internet – will continue providing its tool to law enforcement.

Clearview AI offers its system to hundreds of police departments, and it has no plans to stop. “While Amazon, Google, and IBM have decided to exit the marketplace, Clearview AI believes in the mission of responsibly used facial recognition to protect children, victims of financial fraud, and other crimes that afflict our communities,” CEO Hoan Ton-That said in a statement.

Ton-That has described his system as a search engine for faces. Clients such as police officers can upload a picture of someone’s face, and Clearview will return matching images along with links to the person’s identity. However, as The New York Times documented earlier this year, the company’s database was created by scraping people’s images from news sites and social media profiles, without asking for anyone’s consent.

“Companies like Clearview will end privacy as we know it, and must be stopped,” according Nathan Freed Wessler, a staff attorney with the American Civil Liberties Union.

Last month, the ACLU filed a lawsuit in Illinois against Clearview, charging the company has violated local laws by collecting people’s facial data without their permission. That prompted Clearview to end its relationships with "non-governmental customers.

Meanwhile, US senators, including Ron Wyden (D-Oregon) and Cory Booker (D-New Jersey), have been urging the Trump administration to avoid using facial-recognition systems such as Clearview to identity protesters in the recent George Floyd marches.

“Scientific studies have repeatedly shown that facial-recognition algorithms are significantly less accurate for people with non-white skin tones,” the senators wrote in a letter to US Attorney General William Barr on Wednesday.

Despite the scrutiny and the criticism, Clearview has refused to back down on offering its technology to law enforcement. “Facial recognition has existed for 20 years, and Clearview AI has created groundbreaking technology that actually works,” Ton-That said in his statement. “Unlike Amazon Rekognition, which misidentified people of color, an independent study, using the same methodology, indicated that Clearview AI has no racial bias.” (The ACLU disagrees, and says the study was flawed.)

All of this is still in various phases of implementation and followthrough. What the end result actually will be may not be assessable until later this, or early next year – stay tuned.