THE CRIME REPORT
YOUR CRIMINAL JUSTICE NETWORK

Bans on Facial Recognition Technology Spread Across U.S.

Laura Bowen

September 17, 2020

The decision earlier this month by the city of Portland, Or., to ban the use of biometric facial recognition technology by businesses and local police is one of the strictest measures so far taken by U.S. jurisdictions to address spreading concerns about privacy.

“All Portlanders are entitled to a city government that will not use technology with demonstrated racial and gender biases that endanger personal privacy,” Portland Mayor Ted Wheeler said in announcing the ban.

What makes the city’s measure especially unique is its extension to the private sector, according to observers.

While facial recognition technology has become more widespread in recent years, it has also grown in controversy. Many privacy advocates charged the technology contains “built-in racial biases” and is susceptible to abuse.

In 2019, the National Institute of Standards and Technology released a report revealing that facial recognition systems falsely identify people of color more often than their white counterparts.

“Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search,” the report said. ”Native Americans had the highest false-positive rate of all ethnicities.”

However, when it came to the kinds of searches police use, the study showed that Black women were more often misidentified.

It is important to note that the study found that different facial recognition systems varied widely in accuracy. The Information Technology & Innovation Foundation pointed out that the most accurate facial recognition algorithms “did not display a significant demographic bias.”

Other jurisdictions that have either already passed or are have legislation pending on facial recognition by law enforcement in 2020 include Albany, Pittsburgh, Jackson. Ms., and Springfield, Ma.

The Springfield City Council reached a compromise with Mayor Domenic Soreno in February, to adapt a temporary ban on facial recognition by law enforcement until it was provided with satisfactory policy and procedures governing its use.

Other Massachusetts cities such as Boston, Easthampton, and Cambridge implemented similar bans in 2020.

The Jackson, Ms., specifically cited concerns over “privacy, racial bias, and the potential for police abuse of a surveillance system” in its decision to reject the technology.

Federal Bills

Multiple federal bills in 2020 have addressed biometric technology in law enforcement as well.

The George Floyd Justice in Policing Act of 2020 included measures that would ban “authorized or required” cameras or recording devices from using facial recognition technology in its Federal Police Camera and Accountability Act.

The bill has yet to be passed, but has received support from several high-profile athletes.

The National Biometric Information Privacy Act focuses on limiting ways in which people’s biometric data is collected as well as giving them the right to take legal action against a company that violates this protection.

This would allow law enforcement, businesses and companies must get written consent in order to record someone’s biometric data.

News of the National Biometric Information Privacy Act came amidst increased scrutiny of police use of facial recognition data to arrest allegedly violent Black Lives Matter protesters long after protests ended, Threat Post reported.

Threat Post compiled a shortlist of incidents reported by local outlets:

- One incident involved Miami police using Artificial Intelligence (AI) to identify and arrest a woman for pelting a rock at an officer;
- Another involved Columbia, SC officers who reportedly used AI to arrest multiple protestors “long after the event;”
- Philadelphia used AI to utilize Instagram photos in order to identify protesters;
- The New York Police Department used AI to identify a person who allegedly shouted in an officer’s ear during a protest allegedly, and then raided the suspect’s apartment.

However, it was a controversy surrounding San Francisco’s police surveillance that “put the Black Lives Matter movement at the center of a debate about the effect of surveillance on civil rights protests,” Coda Story reported.

San Francisco police obtained access to video taken by private surveillance cameras of protests, which gave the police Homeland Security Unit live access to the “entire system of 375 cameras owned and maintained by USBID (Union Square Business Improvement District” from May 31 to June 6.

Although it is not unusual for police departments to use video from private cameras in investigations, typically officers ask for footage at specific times from specific cameras.

However, in this instance, “the cameras, positioned on storefronts and pointing to the sidewalk, recorded protesters moving through the area and other people simply going about their daily lives,” *Coda Story* reported.

The Homeland Security Unit “received a data dump of all their footage from 5pm on May 30 to 5am on May 31.”

Officers used footage to gather evidence of crimes.

In a statement provided to *Coda Story*, police said they did not choose to livestream the district's cameras because the vandalism, looting and rioting didn't occur there.

"From the perspective of law enforcement, mass surveillance of demonstrations is in the interest of public safety," Coda Story acknowledged.

"But for activists and privacy experts, knowing police are watching has a chilling effect and undermines the civil liberties of anyone using their right to protest."

Will Big Tech Get Stricter?

Black Lives Matter protests have also caused some tech giants to announce either stopping or pausing providing facial recognition technology to police.

First IBM, then Amazon, then Microsoft.

However, skeptics didn't find much substance in their actions.

Skeptics included the *Washington Post*, which described this as "Like dominoes in a lineup of corporate public relations stunts."

CNBC reported that the three companies aren't actually important players in the market and that the big players are actually smaller companies uninterested in cutting their ties with law enforcement.

In fact, IBM "did not have a real product in this space" and Amazon's facial recognition software Rekognition "is widely used in the private sector, but previously only one law enforcement customer was listed on its website."

Microsoft "says it does not currently sell its facial recognition software to police and that it promises not to until there are federal regulations in place."

One of the big players in the market is Clearview AI. Its clientele includes members of the FBI, ICE, Customs and Border Protection and "hundreds of local police departments" and it doesn't plan on going anywhere.

Clearview AI's CEO Hoan Ton-That told CNBC that, due to the company's experience and reach, getting rid of the company would be a mistake because it would result in a lot of crimes going unsolved.

In a 2019 interview with Wired about the controversy surrounding facial recognition technology, Computer Vision Scientist and Lawyer Gretchen Greene said that this technology can help solve cases faster, like kidnappings, in which time is of the essence.

However, she also touched on concerns with the possibility of the wrong person being identified and concerns she's heard about error rates being different for different demographics, among other big picture concerns.

However, Mathew Feeney, director of the Project on Emerging Technologies at the Cato Institute, believes that we shouldn't be quick to demonize a piece of technology.

“I don’t think we should take an approach that a technology is inherently good or bad,” she said. “But I’m not comfortable at the moment with the lack of regulation, having this technology being used among law enforcement.”

The conversation about the overlap of facial recognition technology and law enforcement is not new to 2020; however outright state bans on law enforcement use represent a relatively new phenomenon.

In 2019, San Francisco was the first U.S. city to ban police from using facial recognition technology. It was followed by San Diego, which scrapped the Tactical Identification System (TACIDS) used for facial recognition by over 3o agencies in the area.

California also imposed a three-year ban on incorporating facial recognition technology into police body cams, with the explanation that this would allow enough time “for the technology’s accuracy, the legal framework, and social dialogue to catch up with law enforcement’s ideal.”

The FBI started phasing in facial recognition software around 2011.

Wherever you stand on the issue of facial recognition in law enforcement, it’s proving to be a growing matter of public interest.

“Whether or not they support a ban, researchers and activists across the political spectrum are increasingly speaking out about privacy concerns, algorithmic bias and the lack of transparency and regulation around this tech,” concludes CNBC.