ELECTRONIC FRONTIER FOUNDATION

EFF Statement for the Record on Hearing: Facial Recognition Technology: Examining Its Use by Law Enforcement

To: Members, U.S. House Committee on the Judiciary, Subcommittee on Crime
From: The Electronic Frontier Foundation
Date: July 13, 2020
RE: Facial Recognition Technology: Examining Its Use by Law Enforcement

EFF Statement for the Record

Face surveillance is increasingly an all-encompassing tool for government to track where we are, what we are doing, and who we are with, regardless of whether we're suspected of a crime or not. Many proponents of the technology argue that there is no reasonable expectation of privacy when we spend time in public, and that if we have nothing to hide, we have nothing to fear. However, in his majority opinion in the watershed *Carpenter v. United States* (2018)[1], Supreme Court Chief Justice John Roberts wrote: "A person does not surrender all Fourth Amendment protection by venturing in the public sphere."

Advocates for facial recognition and face analysis technologies often present these systems as a "silver bullet," not just for law enforcement, but also to identify customers, to authorize entry into public and private spaces, and even to track people's moods and emotions. However, these technologies frequently reach erroneous conclusions, especially concerning people of color and women,[2] leading to false arrests of at least three black men.[3] Many of the current means for measuring accuracy fail to take account of operational realities and limitations when these systems are used in real-world situations.

Moreover, these technologies present serious challenges to privacy, free expression, and due process. They turn our movements, and thus our lives, into open books for government scrutiny. They also discourage people from exercising their First Amendment rights. The ability for law enforcement to pan over a crowd at a protest, and using face recognition, attempt to identify everyone in attendance, is a severe threat to free political expression and makes people vulnerable to retribution and reprisals. Just last week, the *South Florida Sun-Sentinel* broke the news that three Florida police departments have used face recognition to identify BLM protesters.[4]

[1] *Carpenter v United States*, 585 U.S. ___ (2018)
[2] Joy Boulamwini, The Algorithmic Justice League, https://www.ajl.org/
[3] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,* N.Y. Times (December 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html
[4] Joanne Cavanaugh Simpson, Marc Freeman, *South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?,* South Florida Sun Sentinel, (June 26, 2021), https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html

Excessive secrecy surrounding face surveillance also violates the due process rights of people accused of crimes. For one example, Willie Allen Lynch is currently serving an eight-year prison sentence after a facial recognition system suggested him as a likely match of a suspect. [5] Prosecutors in the case didn't disclose information about how the algorithm worked, that it produced other matches that were never considered, or why Lynch's photo was targeted as the best match.[6]

Lynch didn't learn that he had been identified by a facial recognition algorithm until just days before his final pretrial hearing, although prosecutors had known for months. The crime analyst who operated the system did not know how the algorithm functioned, and neither did the detective who accepted the analyst's conclusion that Lynch's face was a match. The analyst said the first-listed photo in the search results is not necessarily the best match—it could be one further down the list. A prosecutor doubted the system was reliable enough to meet standards used by courts to assess the credibility of scientific testimony and whether it should be used at trial. Lynch asked for the other matches produced by the technology—but the court refused.

If a human witness who identified Lynch in a line-up said others in the line-up also looked like the criminal, the state would have had to disclose that information, and Lynch could have investigated those alternate leads. The same principle should have required the state to disclose other people the algorithm produced as matches, and also information about how the algorithm functions.

When defendants are facing lengthy prison sentences or even the death penalty, tight controls on the use of facial recognition are crucial. Defendants have a due process right to information about the algorithms used and search results. Of course, current violations of the rights of the accused are just one more reason why government must not use face surveillance at all.

Law enforcement agencies have also proven they cannot be trusted with this technology. While often described as nothing more than an investigatory lead, police have arrested people whose names were produced by face recognition technology without corroborating evidence or follow-up investigation, leading to arrests of innocent people.[7]

Because of these well documented problems and disparate impacts, cities and states across the country have banned government use of face surveillance technology, and many more are weighing proposals to

[5] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. Times (January 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html

[6] Amici Curiae Brief of American Civil Liberties Union, American Civil Liberties Union of Florida, Electronic Frontier Foundation, Georgetown Law's Center on Privacy and Technology, and Innocence Project in support of Petitioner, *Lynch v. Florida*, Amicus Brief Filing # 86179154 (2019), https://www.eff.org/document/lynch-v-florida-amicus-brief

[7] American Civil Liberties Union, *Michigan Father Sues Detroit Police Department for Wrongful Arrest Based on Faulty Facial Recognition Technology* (April 13, 2021), https://www.aclu.org/press-releases/michigan-father-sues-detroit-police-department-wrongful-arrest-based-faulty-facial

do so. From Boston[8] to San Francisco[9], New Orleans[10] to Minneapolis[11], elected officials and activists know that face surveillance gives police the power to track us wherever we go, disproportionately impacts people of color[12], turns us all into perpetual suspects, increases the likelihood of being falsely arrested[13], and chills people's willingness to participate in first amendment protected activities.

Police and other government use of this technology cannot be responsibly regulated. Face surveillance in the hands of the government is a fundamentally harmful technology, even under strict regulations or if the technology was 100% accurate and disclosed. The use of face surveillance by the federal government should be banned, and certain federal funds should be withheld from local and state governments that use the technology.

[8] Matthew Guariglia, *Victory! Boston Bans Government Use of Face Surveillance*, The Electronic Frontier Foundation (June 24, 2020), https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance

[9] Nathan Sheard, *San Francisco Takes a Historic Step Forward in the Fight for Privacy*, Electronic Frontier Foundation (May 14, 2019), https://www.eff.org/deeplinks/2019/05/san-francisco-takes-historic-step-forward-fight-privacy

[10] Michael Isaac Stein, *New Orleans City Council bans facial recognition, predictive policing and other surveillance tech,* The Lens (December 18, 2020) https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech

[11] Kim Lyons, *Minneapolis prohibits use of facial recognition software by its police department*, The Verge (February 13, 2021), https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy

[12] Alex Najibi, *Racial Discrimination in Facial Recognition* Technology, Harvard University (October 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology

[13] Drew Harwell, *Wrongfully arrested man sues Detroit police over false facial recognition match,* Washington Post (April 13, 2021), https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit