Issue Brief: Strong Safeguards Are Needed for Face Recognition Surveillance

Face recognition surveillance is invasive, error-prone, and threatens constitutional rights

Face recognition is a powerful technology that is increasingly used at the local, state, and federal level for surveillance. At least one-in-four police departments can run face recognition searches, including federal agencies like the FBI, ICE, and CBP. Face recognition surveillance poses two distinct but equally important dangers: It can be immensely harmful when it does not function properly, as well as when it does.

Face recognition misidentifications can lead to improper targeting, needless police action, and wrongful arrests. Many face recognition systems are more likely to misidentify women and people of color. And even for the most accurate algorithms, situational factors like photo quality and computer settings can make error more likely. There are already three documented cases in which individuals have been improperly arrested based on face recognition misidentifications, but because use of the tech is often hidden from defendants, the number is likely much higher.

Police will often claim that face recognition is just used for leads, but even in these cases it can still play a major role in an investigation, with misidentifications potentially causing serious harm. Unreliable investigative tools risk unreliable results and wrongful arrests, a problem we have seen again and again with flawed technologies ranging from outdated forensics to unreliable polygraph tests. And because the use of face recognition is rarely disclosed to defendants, their ability to discover and respond to errors is limited.

Better accuracy, however, will not alleviate the danger it poses to civil rights and civil liberties. Without strong limits, face recognition could catalog sensitive activities and interactions, with dramatic and chilling effects on a free society. Face recognition has already been used by police on multiple occasions to identify peaceful protesters, and for selective targeting. In 2015, as demonstrators protested the death of Freddie Gray in police custody, Baltimore police used face recognition to target protesters, scanning the crowd with the technology to find a and arrest anyone who had an outstanding warrant for any offense.

The danger face recognition surveillance poses can only be addressed by a pause in its use or strong and comprehensive limits

Given the range of harms face recognition can cause — and how often it can be prone to error — the most straightforward solution would be to pause its use by law enforcement until it is far more reliable and accurate, and best practices are established to prevent misidentifications. The Facial Recognition and Biometric Technology Moratorium Act (S. 2052; H.R. 3907) would do this, placing a moratorium on face recognition surveillance.

In the absence of a total pause, no jurisdiction should be permitted to use face recognition without strict safeguards. Principal among them are the following:
1) **Require face recognition searches to be based on probable cause:** A probable cause requirement is essential to stopping face recognition from being used to catalog and target individuals engaged in constitutionally protected activities. Since primary police use for face recognition is to scan photographs of individuals taken during the commission of a crime, demonstrating probable cause should not be an onerous burden for supporting legitimate law enforcement goals.

2) **Limit use of face recognition to investigation of serious crimes:** Face recognition should not be used to stockpile suspects for minor offenses. Limiting how face recognition can be used would reduce risk of errors going undetected, which is more likely in low-level cases that receive less scrutiny. It would also prevent the misuse of discretionary powers, including selectively targeting marginalized communities and dissidents. The concept of limiting use of powerful surveillance tools to top-tier investigations has clear precedent: It has been applied for over 50 years to tools such as wiretapping.

3) **Prohibit face recognition from being the sole basis for arrests:** Because factors such as low image quality will always leave a risk of misidentification, giving too much credence to face recognition matches puts innocent individuals at risk. While seeking additional evidence does not fully eliminate this risk, it is an essential safeguard for reducing it.

4) **Require notice to defendants whenever face recognition is used:** Like any other complex forensic tool, face recognition’s effectiveness can depend on technical and environmental factors, making it critical that defendants are notified and given the opportunity to examine the technology whenever it is used in an investigation. Guaranteeing access to this information is not only critical for due process, but also acts as an important safeguard to deter corner cutting and sloppy use of face recognition during investigations.

5) **Prohibit face recognition from being deployed for untargeted surveillance:** Using face recognition not to identify a designated person in an image but rather to conduct untargeted scans of all individuals on video streams is especially dangerous. Pilot programs of this type of system in the United Kingdom produced error rates above 90%. And this type of dragnet surveillance could effortlessly monitor individuals’ movements, interactions, and activities on a mass scale — creating a society far more familiar in authoritarian regimes. Given the severity of these risks, using face recognition for untargeted surveillance should be fully prohibited.

**Limiting face recognition has bipartisan support, and states and cities are already acting**

Limiting face recognition has received bipartisan support during hearings in the House Judiciary Committee and House Committee on Oversight and Reform. It also has broad support from advocacy groups across the ideological spectrum, from the ACLU and Fight For The Future to FreedomWorks and the Heritage Foundation.

We are beginning to see significant action to limit face recognition: Over a dozen cities have banned law enforcement use of the technology. In 2021, Maine passed a statewide law creating a warrant rule, a serious crime limit, and a prohibition on face recognition matches serving as the sole basis for arrests. Other states have passed limits on face recognition as well.

But for the vast majority of Americans, face recognition can still be deployed against them absent any rules or safeguards. Congress needs to act to end the harm this invasive surveillance technology causes to civil rights and civil liberties before it is too late.

*For more information, please contact Jake Laperruque, Senior Policy Counsel for the Constitution Project at the Project On Government Oversight (POGO), at jlaperruque@pogo.org or (973) 951-6344*