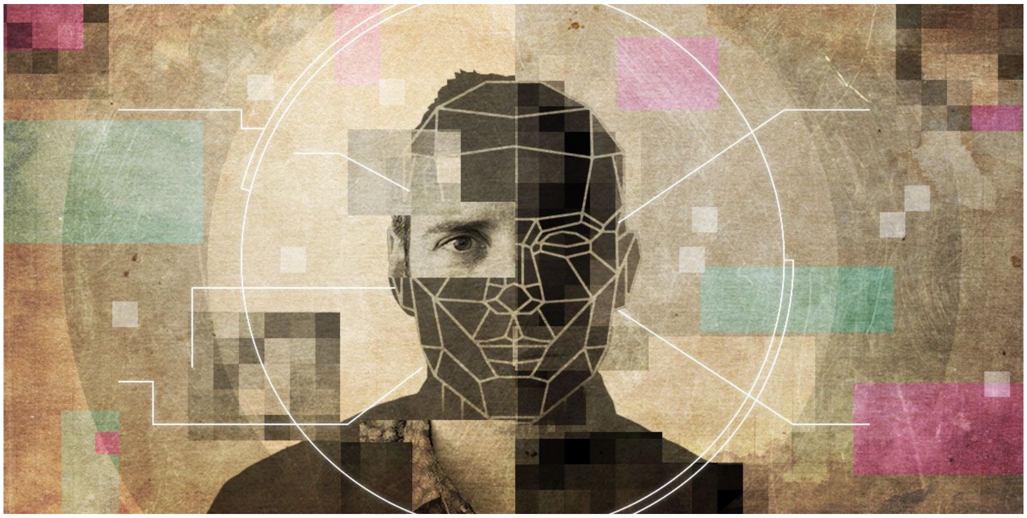
About Face Surveillance



EFF One-Pager

Learn more:
https://www.eff.org/pages/face-recognition

Support our work:
eff.org/donate

The proliferation of new face surveillance platforms is raising significant questions about what civil rights abuses look like in the digital age.

Historically, allegations of police misconduct were based on visible behavior: people generally know when they have been assaulted, detained unjustly, or had their property searched or seized without due process. Today, civil rights violations can also occur on computer screens, amplified by automated processes. These violations are exacted invisibly and indiscriminately on large populations.

What is Face Surveillance?

Face surveillance is an automated or semi-automated method of identifying or verifying the identity of an individual by analyzing unique features of their face. Face recognition systems can be used to identify people in photos, videos, or in real-time. Law enforcement may also use mobile devices to identify people.

Face recognition technology may also be used to track individuals' movements. Given the proliferation of video surveillance cameras and the rapid advances in the technology, this raises some of the same privacy concerns as the uncontrolled use of Automated License Plate Readers and other surveillance technologies. Real-time face recognition is already being used in other countries and even at sporting events in the United States, and face surveillance has also been used in the US to target people engaging in protected speech.

- Americans would not support a measure requiring every person to carry and display a photo ID card at all times. Face surveillance is the technological equivalent but worse. With Face surveillance this data collection could easily take place without the knowledge of affected community members.

- Face surveillance presents unique threats to safety and privacy. We can change most of our personal identifiers, like a license plate, driver's license, social security card, or password. But changing your face after a security breach is simply not an option.

- Face recognition technology can be prone to error, implicating people for crimes they haven't committed.

- Face recognition software is particularly bad at recognizing women, young people, and people with darker skin. This can result in misidentification or failed identification, disparately impacting certain groups.

- Misidentification by face-scanning systems will lead to more – not fewer – dangerous encounters between police and the public.

- At a time when public protest is widespread and the federal government is scrutinizing immigrant communities and falsely labeling activists as criminals, law enforcement use of face surveillance would chill First-Amendment protected activity.

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org