

Ban Government Use of Face Recognition

Face recognition is one of the most intrusive surveillance technologies. There are numerous instances of law enforcement misidentifying and arresting innocent people with it. Now, immigration agents are harassing people on the streets using this technology, including U.S. citizens.

When face recognition software linked to a surveillance camera scans a person's face, it creates warrantless biometric records of all people walking by, whether they are suspected of a crime or not. This technology poses a threat to our privacy and safety. Congress should immediately ban government use of face surveillance.

How It Works

Government agencies (like state DMVs and the U.S. State Department) collect photos of people's faces for many legitimate, specific, reasons. These digital images are converted into a mathematical representation of pre-designated measurements, often called a "face template," which are stored in agency databases. Increasingly, law enforcement also contracts with private companies to compare photos to the face templates in private databases. One such company, Clearview AI, has compiled their database of 70 billion face templates by scraping public images off the internet images.

When law enforcement wants to identify someone in a photo collected from public or private cameras, the internet, or from a mobile device in the field, they can compare them to the face templates in these databases. Through this process, unsuspecting Americans become the subject of what has been called the "perpetual lineup." These systems use facial recognition algorithms to assign a likeness score to each image. When the algorithm gets it wrong, or returns a low likeness score as the "best" match, innocent people suffer real and unjust consequences.

Facial recognition technologies are often presented as a "silver bullet" for law enforcement, but they present serious challenges to privacy and due process.

Key Problems

Face surveillance is becoming an all-encompassing tool for the 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. For example, most drivers' DMV photos are shared with law enforcement agencies and included in database searches as possible matches.

Experts at [MIT Media Lab](#), the [National Institute of Standards and Technology](#), and [Georgetown's Center on Privacy and Technology](#) have shown that face recognition technology is riddled with errors. Overly relying on these systems means that innocent Americans have been and will continue to be subjected to erroneous arrest.



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

Want more information? Please contact Director of Federal Affairs India McKinney at india@eff.org and Assistant Director of Federal Affairs Maddie Daly at maddie@eff.org.