Facial Recognition

Face recognition is poised to become one of the most pervasive and intrusive of all surveillance technologies. Today, law enforcement officers can use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face scanning and identification capabilities; and federal, state, and local law enforcement agencies have access to hundreds of millions of images of faces of law-abiding Americans

This technology poses a threat to our privacy, chills protest in public places, and disparately impacts people of color. Congress should ban government use of face surveillance.

How It Works

Some law enforcement and other government agencies (like state DMVs and the U.S. State Department) collect photographs of people's faces for a variety of purposes. The digital images are then converted into a mathematical representation of pre-designated measurements, often called a "face template," and uploaded into a shared database.

When the government wants to identify someone in a photo collected from such places as social media, CCTV, "Smartcity" traffic cameras, or in the field, they can compare the face template from the photo with the known photos in the database(s). They use facial recognition algorithms that rely on unique physical markers on people's faces to find the closest mathematical matches.

A rapidly growing number of government agencies use face surveillance. The FBI's Next Generation Identification database has 30 million face recognition records, and its Facial Analysis, Comparison and Evaluation Services can access 641 million more. CBP plans to use face recognition technology for all travelers entering and leaving the U.S. TSA's Biometric Roadmap outlines all the ways the agency seeks to "leverage" face recognition technology. Amazon is selling police an inexpensive face surveillance system called Rekognition.

Manufacturers and advocates for facial recognition technologies often present these systems as a "silver bullet" for law enforcement, but they are error-prone and present serious challenges to privacy and due process. This has led to the development of unproven, inaccurate systems that will impinge on constitutional rights and disproportionately impact women, children, and people of color

Key Problems

Privacy: Face surveillance is becoming 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. Today, most drivers' DMV photos are shared with law enforcement agencies.

Protest: Face surveillance will chill and deter people from protesting in public places.

Error: Many face recognition systems have unacceptably high error rates. This means innocent people will be subjected to erroneous police scrutiny.

Discrimination: The "false positive" error rates are significantly higher for women, children, and people of color. This means that face recognition has an unfair discriminatory impact. Also, cameras are over-deployed in neighborhoods with immigrants and people of color, and new spying technologies like face surveillance amplify existing disparities in the criminal justice system.

Solution

Congress should immediately put a moratorium on any use of face surveillance by federal agencies or with federal funds.

Want more information? Please contact India McKinney at **india@eff.org**.