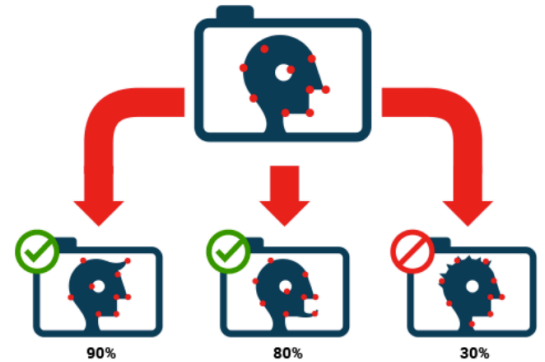## Biometrics: Facial Recognition

Law enforcement and other government agencies like DMVs and the State Department collect photographs of people's faces.

The digital images are then converted into a mathematical representation of pre-designated measurements, often called a "face template," and uploaded into a common database.

When law enforcement wants to identify someone in a photo collected from such places as social media, CCTV, "Smart city" traffic cameras, or in the field, they can compare the face template from the photo with the known photos in the database(s), using facial recognition algorithms that rely on unique physical markers on your face to find the closest mathematical matches.

These databases may contain mugshots of arrestees, but law enforcement can also ask other government agencies (like the DMV or the State Dept.) to access their non-criminal databases.

A Few Problems

- Perpetual facial dragnet: One in two American adults may have their image in a facial recognition network, impacting more than 117 million people. Law enforcement in at least 26 states uses facial recognition in combination with driver's license and ID photos. Sixteen states grant the FBI access to their DMV databases. At least five large cities, including Los Angeles, Chicago, and Dallas, use or have considered using facial recognition to scan the faces of pedestrians in real time with surveillance cameras.

- Lack of regulation & privacy protection: Facial recognition is almost completely unregulated. No states have passed comprehensive laws limiting police use of facial recognition, and only one of 52 agencies surveyed expressly forbids police from using facial recognition to surveil people engaged in political, religious, or other First Amendment protected activities. Very few have taken measures to ensure accuracy of facial recognition results or have audited their systems for abuse.

For more information on facial recognition, please contact India McKinney, at india@eff.org.