Police Face Recognition Technology

What is face recognition?

Face recognition is the automated process of comparing two images of faces to determine whether they are the same person.

Before it can identify someone, a face recognition algorithm must first find that person's face within the photo. Next, the algorithm extracts features from the face that can be quantified, like eye position or skin texture. Finally, the algorithm examines pairs of faces and issues a numerical score reflecting the similarity of their features. In the most common use of face recognition by law enforcement, an officer or analyst will compare a photo of an unknown person—taken from sources like CCTV cameras or social media photos—to a database of known people, typically a mug shot or driver's license database.

As used by law enforcement, face recognition does not (yet) produce a positive identification, but rather finds more- or less-likely matches. Most police systems will provide a list either of the top few most similar photos or all photos above a certain similarity threshold—for example the faces have 75% or more "identity points" in common. These photos are called "candidates" for further investigation. It is then up to an officer or analyst to determine whether any of the candidates are, in fact, the subject in the original photo.

Key facts and figures

> 133.5 million adults:

Over 54% of U.S. adults are in a face recognition network accessed by police.

> Driver's license searches:

At least 31 states allow law enforcement to run or request searches against their driver's license and ID photo database.

> Live video surveillance:

Major police departments are exploring using face recognition on live video streams.

> Differential error rates:

Face recognition seems to perform differently depending on the race, gender, and age of the subject being searched. Evidence suggests it may be least accurate on those it is most likely to be used on—African Americans.

> Almost completely unregulated:

No state has passed a law comprehensively regulating police face recognition. Few jurisdictions have public use policies.

> No standardization or minimum requirements:

There are no minimum image quality standards, minimum number of "nodal points," or minimum similarity thresholds. There are also no face analysis training standards or procedures, nor are there minimum required post-search identity verification procedures.

Adapted from *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, www.perpetuallineup.org. For more information, email Clare Garvie at cag104@georgetown.edu.

Face recognition discovery wish list—working draft

1. Name & manufacturer of the facial recognition software used to conduct the search in this case, and the algorithm(s) version number(s) and year(s) developed, if available.
2. Source code for the face recognition algorithm(s).
3. What measurements, nodal points, or other unique identifying marks are used by the system in creating facial feature vectors. If weighted differently, the scores given to each respective mark.
4. Error rates for the facial recognition system used, including false accept and false reject rates (also called false match and false non-match rates—FMR and FNMR). Documentation of how the error rates were calculated, including whether they reflect test or operational conditions.
5. Performance of the algorithm(s) on applicable NIST Face Recognition Vendor Tests, if available.
6. The original copy of the query or "probe" photo submitted to the [face recognition unit].
7. All edited copies of the query or "probe" photo submitted to the facial recognition system, noting if applicable which edited copy produced the candidate list the defendant was in, and a list of edits, filters, or any other modifications made to that photo.
8. Copy of the database photo matched to the query or "probe" photo and the percentage of the match, rank number, or confidence score assigned to the photo by the facial recognition system in the candidate list.
9. A list or description of the rank number or confidence scores produced by the system, including the scale on which the system is based (e.g. percentage, logarithmic, other).
10. A copy of the complete candidate list returned by the face recognition or the first 20 candidates in the candidate list if longer than 20, in rank order and including the percentage of the match or confidence score assigned to each photo by the facial recognition system.
11. Parameters of the database used:
    1. How many photos are in the database;
    2. How are the photos obtained;
    3. How long the photos are stored;
    4. How often the database is purged;
    5. What the process is for getting removed from the database;
    6. Who has access to the database;
    7. How the database is maintained;
    8. The Privacy Policy for the database.
12. The report produced by the analyst or technician who ran the facial recognition software, including any notes made about the possible match.
13. The name and training, certifications, or qualifications of the analyst who ran facial recognition search query.

If possible, if you file a motion using the information provided above, please give Clare Garvie at the Center on Privacy & Technology a heads up! (cag104@georgetown.edu or 202-661-6707) We are trying to track State responses to and court rulings on face recognition motions and need your help.