ELECTRONIC FRONTIER FOUNDATION
The leading nonprofit defending digital privacy, free speech, & innovation.

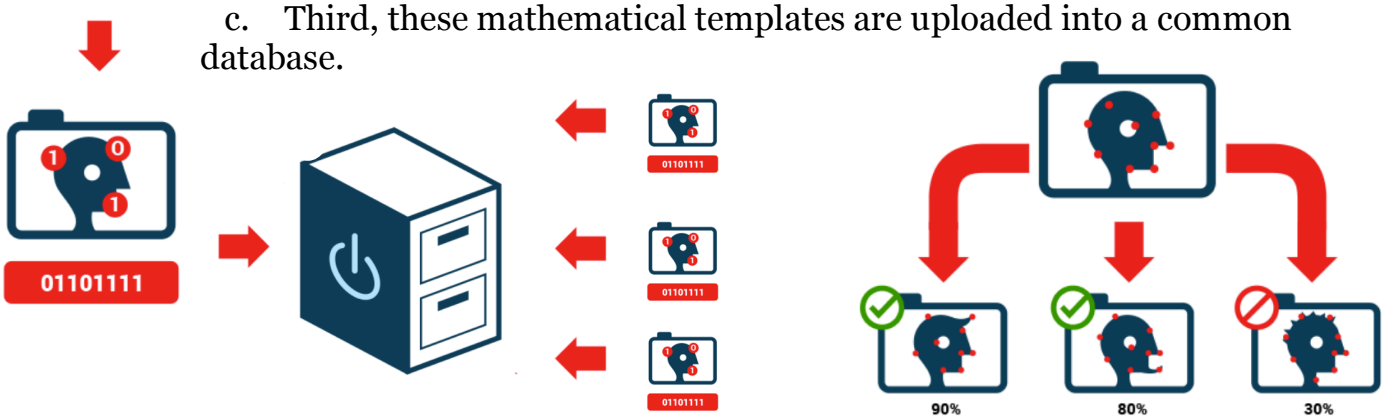
Biometrics: Facial Recognition

1. What is biometric facial recognition and how does it work?

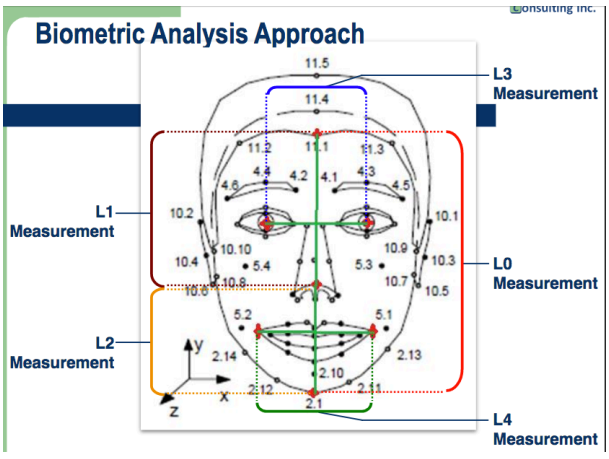
a. First, law enforcement and other government agencies like DMVs and the State Department collect photographs of people's faces.

b. Second, the digital images are then converted into a mathematical representation of pre-designated measurements, often called a "face template."

c. Third, these mathematical templates are uploaded into a common database.



d. Finally, 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.



Slide from presentation by AFIS and Biometrics Consulting Inc., at the 96th Int'l Assoc. for Identification Educational Conference in Milwaukee, Wisconsin on August 10, 2011. http://afisandbiometrics.com/yahoo_site_admin/assets/docs/Facial_Image_Comparison_for_Courts_-_V1_08-10-2011.2983828.pdf

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

2. Why should I care?

a. 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.

b. 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.

c. Racial Bias: Facial recognition systems have a disproportionate impact on Communities of Color. One study, which included an FBI researcher, found facial recognition is less reliable when analyzing African American faces. Because African Americans are already arrested at a disproportionate rate, their mugshots are likewise overrepresented in facial recognition databases. If the technology has a higher rate of misidentification for people of color, this will also increase the chance that they will be considered a suspect for a crime they didn't commit.

3. How do I learn more?

a. Read Govt Accountability Office report on FR: https://eff.org/FRGAO2016
b. EFF's 2017 Congressional Testimony on FR: https://eff.org/FR2017
c. Georgetown Law's Report on FR: https://www.perpetuallineup.org/
d. Ex. of law enforcement's FR trainings:
    i. https://eff.org/FRLEAtraining
    ii. https://eff.org/FRFBI2010
e. Review of FR program flaws: https://eff.org/FRflaws
f. NGI/RISC Privacy Impact Assessment: https://eff.org/FRPIA
g. Visit EFF's deeplinks blog:
    i. https://www.eff.org/deeplinks/2016/05/fbi-ngi-privacyact
    ii. https://www.eff.org/deeplinks/2016/06/danger-corporate-facial-recognition-tech

Stephanie Lacambra, Criminal Defense Staff Attorney
415-436-9333 x130, stephanie@eff.org

Support EFF and become a member today! www.eff.org/support