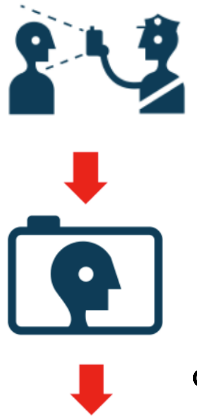
ELECTRONIC FRONTIER FOUNDATION
The leading nonprofit defending digital privacy, free speech, & innovation.

Biometrics: Facial Recognition

A Guide for Criminal Defense Attorneys

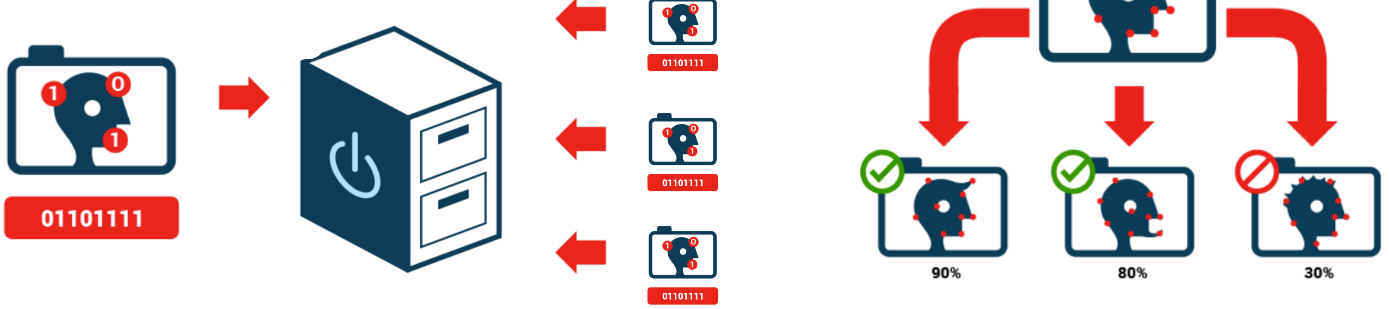
1. What is biometric facial recognition and how does it work?



a. First, law enforcement collects photographic mugshots of arrestees and asks other government agencies (like the DMV or the State Dept.) that also collect photographs of people's faces to share their info.

b. Second, the digital images are then converted into a mathematical representation of pre-designated measurements.

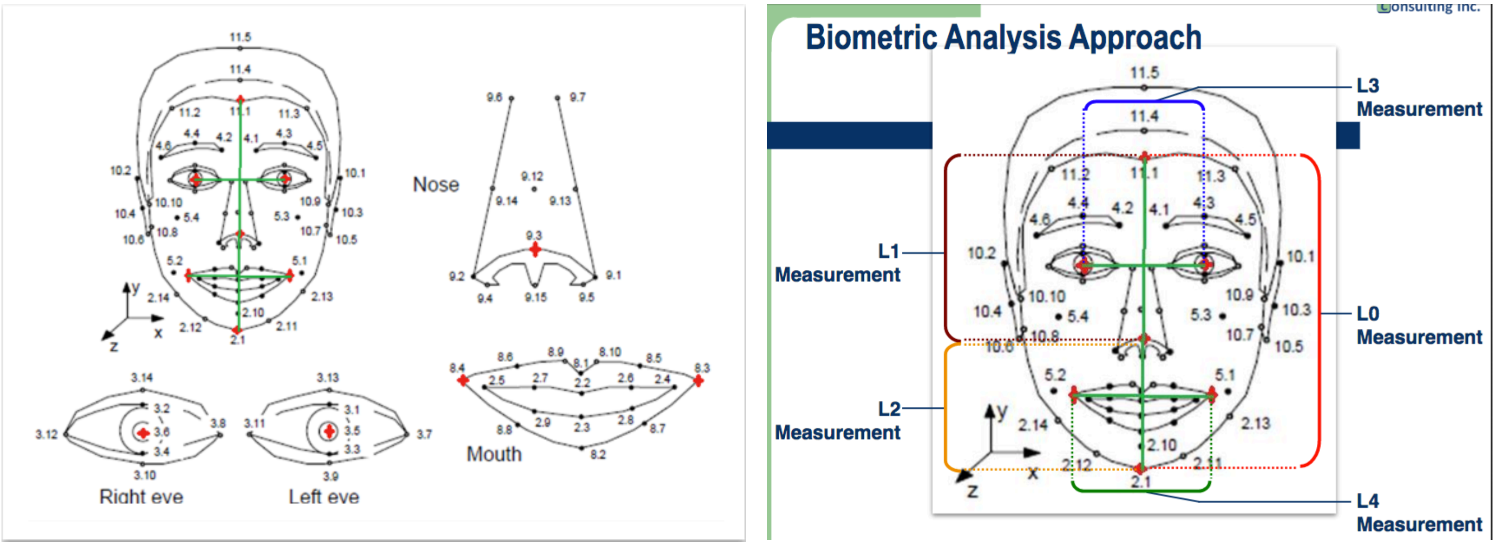
c. Third, these mathematical templates are uploaded into a common database.



d. Finally, when law enforcement has a query photo they wish to identify taken from such places as social media, CCTV, "Smart city" traffic cameras, or in the field, they convert the image into a mathematical representation that can be compared 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.

2. Some factors that may indicate law enforcement used facial recognition:
   a. An officer or witness took your client's photo before booking
   b. Your client was arrested in an unusual location or without notice
   c. Buzzwords to look for in reports:
      i. "photos from a police database"
      ii. Next Generation Identification-Interstate Photo System ("NGI-IPS") – FBI database of nearly 73 million criminal records and over 53 million civilian records

iii. Facial Analysis, Comparison and Evaluation (“FACE”) Services – over 411 million non-criminal photos from DMV & passports
iv. Universal Control Number (“UCN”) – ID # assigned to photo
v. Repository for Individuals of Special Concern (“RISC”)
vi. “Candidate List” – list of potential matches



Slides from 96th IAI Educational Conference in Milwaukee, Wisconsin on August 10, 2011 by AFIS and Biometrics Consulting Inc. produced to EFF in response to FOIA

3. How do I challenge FR evidence?
   a. Subpoena contract between the LEA (law enforcement agency), DOJ, and FR prgm developers to review limits in programming capabilities
   b. Object to error rates and false positives: NGI purports to provide the “true candidate” in the top 50 profiles only 85% of the time – and that’s presumably only if the “true candidate” is even contained within the database – leaving the system prone to false positives.
   c. Consider filing a motion to compel the FR algorithm source code to search for flaws that may affect search results
   d. If in IL and a stock photo is taken from a private actor, take advantage of the IL Biometric Information Privacy Act (740 ILCS 14/15, § 15(b)) that requires notice and consent before use of FR tech

4. How do I learn more?
   a. Read Govt Accountability Office report on FR: https://eff.org/FRGAO2016
   b. EFF’s 2017 Senate 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 training: https://eff.org/FRLEAtraining
   e. Review of FR program flaws: https://eff.org/FRflaws
   f. NGI/RISC Privacy Impact Assessment: https://eff.org/FRPIA

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