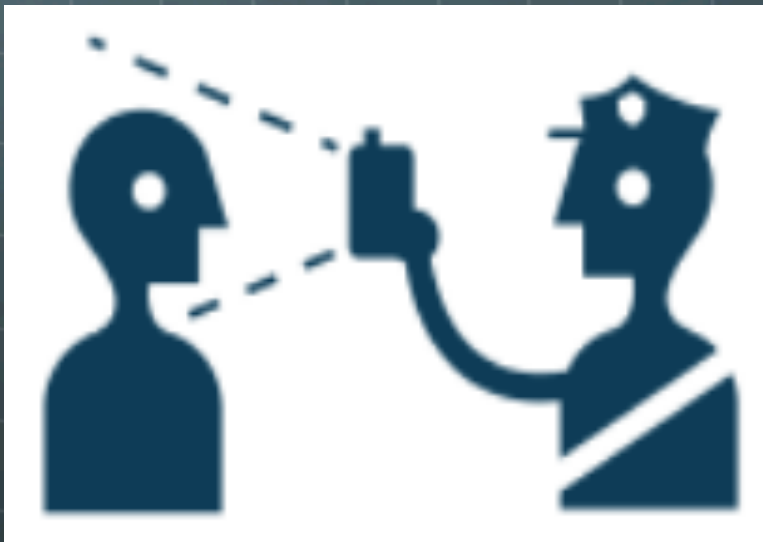


Facial Recognition

What is it and how does it work?

1. LEAs collect photo mugshots of arrestees and ask other government agencies (like the DMV or the State Dept.) that also collect photos of faces to share their info

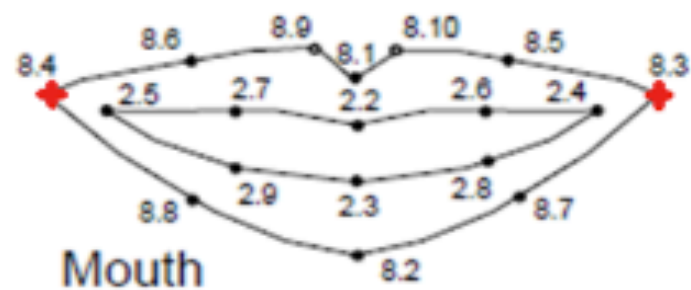
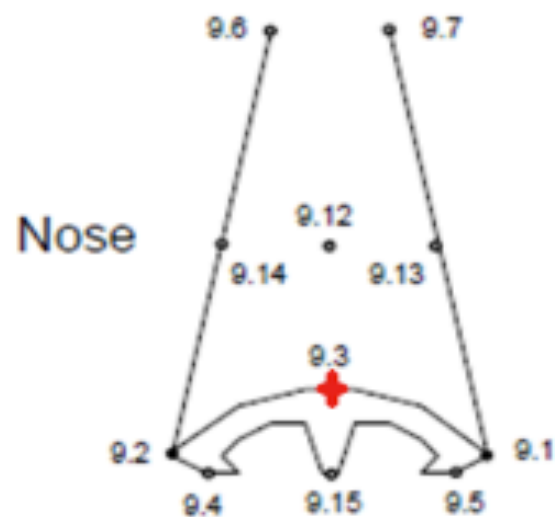
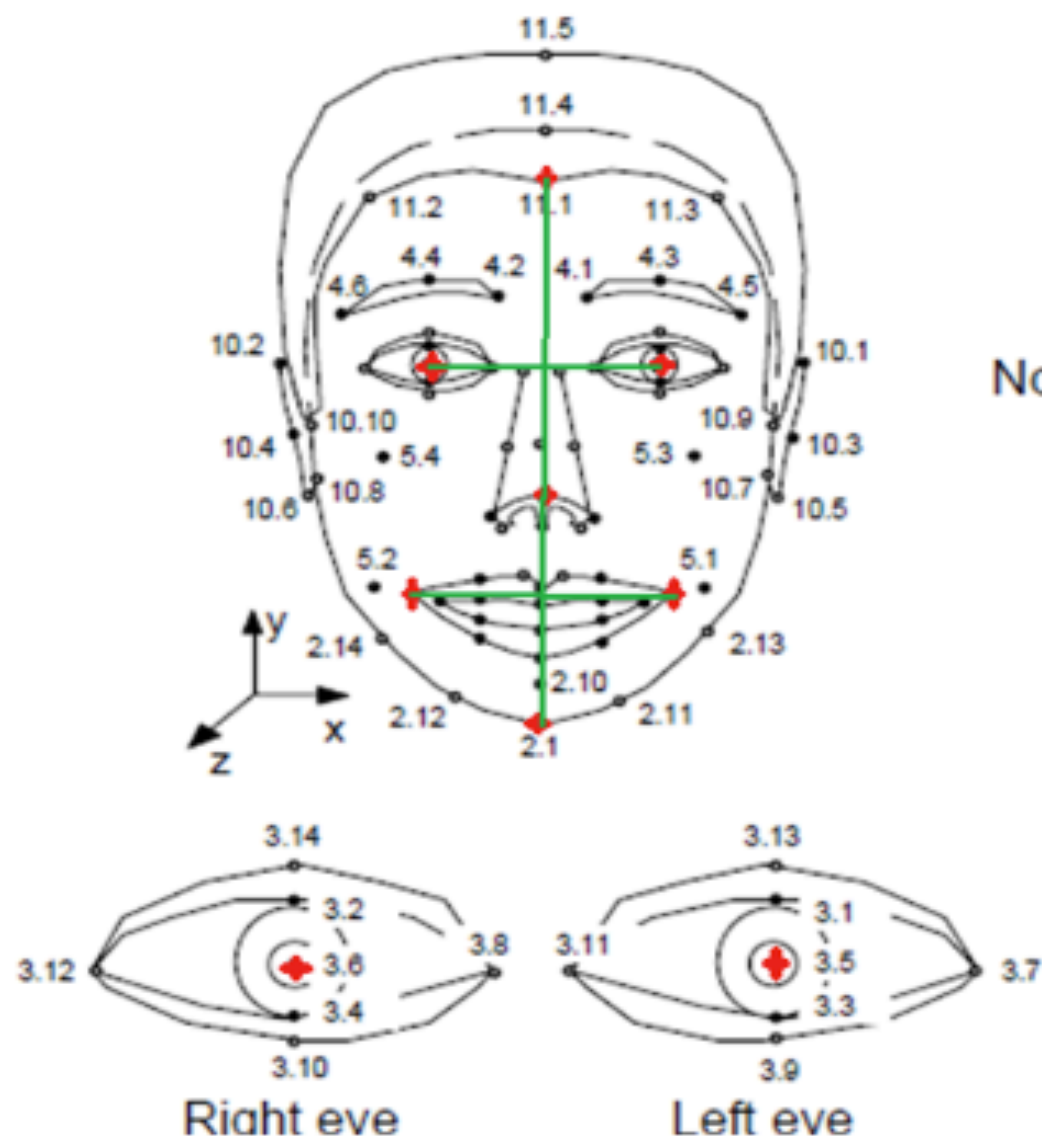


Facial Recognition

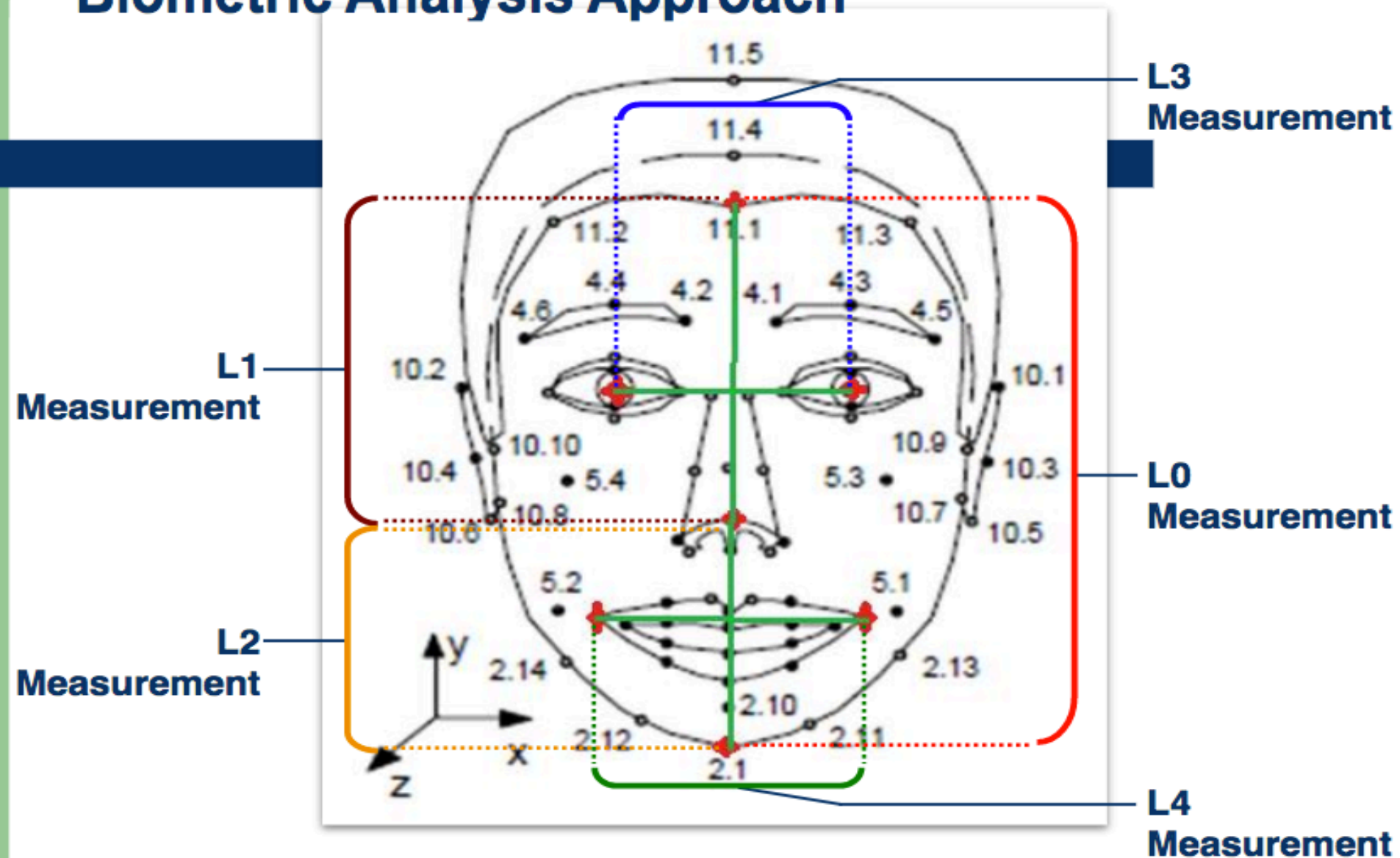
What is it and how does it work?

2. The digital images are then converted into a mathematical representation of pre-designated measurements





Biometric Analysis Approach



Facial Recognition

What is it and how does it work?

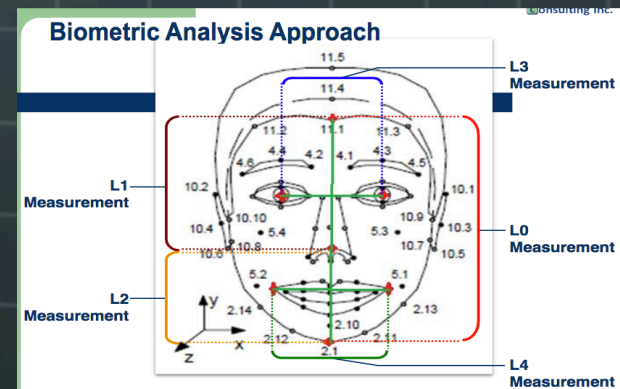
3. The mathematical templates are uploaded into a common database

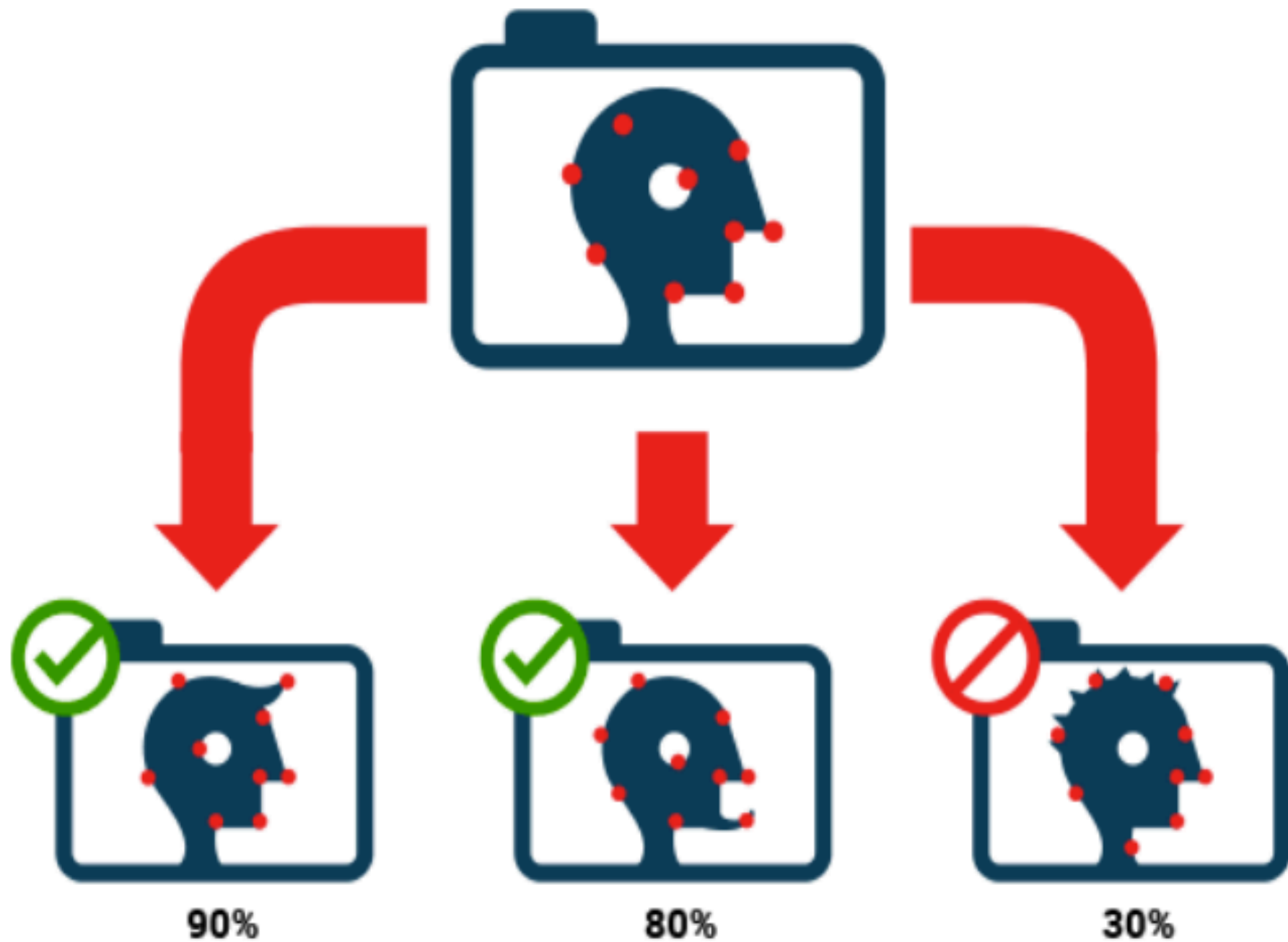


Facial Recognition

What is it and how does it work?

4. Cops take a “query” photo they want to ID, 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.





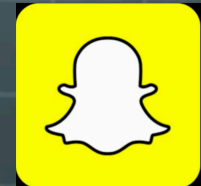
Facial Recognition

Where do cops get a query photo?

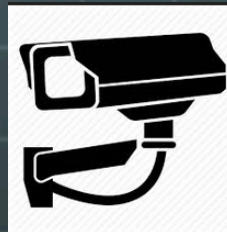
1. In the field:



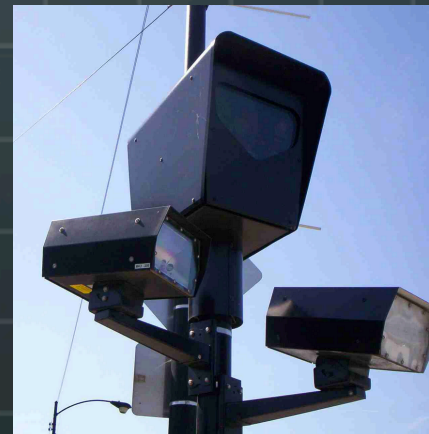
2. Social media:



3. CCTV:






4. Smart City cameras:



Facial Recognition

How do I know if cops used FR in my case ?

Look for the following factors which may indicate use of FR:

-  An officer or witness took your client's photo before booking.
-  Your client was arrested in an unusual location or without notice.
-  You see certain buzzwords in the police report.



Facial Recognition

Buzzwords to look for in reports:

- 🌐 “photos from a police database”
- 🌐 Next Generation Identification-Interstate Photo System (“NGI-IPS”) – FBI database of nearly 73 million criminal records and over 53 million civilian records
- 🌐 Facial Analysis, Comparison and Evaluation (“FACE”) Services – over 411 million non-criminal photos from DMV & passports
- 🌐 Universal Control Number (“UCN”) – ID # assigned to photo
- 🌐 Repository for Individuals of Special Concern (“RISC”)
- 🌐 “Candidate List” – list of potential matches

Facial Recognition

How do I challenge FR evidence?

-  Subpoena contract between the LEA, DOJ, and FR prgm developers to review limits in programming capabilities.
-  Object to error rates and false positives: NGL 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.

Facial Recognition

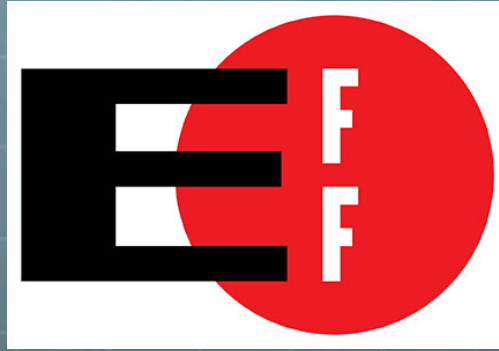
How do I challenge FR evidence?

- 🌐 Consider filing a motion to compel the FR algorithm source code in order to search for flaws that may affect search results
- 🌐 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

Facial Recognition

How do I learn more?

- Read Govt Accountability Office report on FR: eff.org/FRGAO2016
- EFF's 2017 Senate Testimony on FR: eff.org/FR2017
- Georgetown's Law's Report on FR: <https://www.perpetuallineup.org/>
- Ex. of law enforcement's FR training: eff.org/FRLEAtraining
- Review of FR program flaws: eff.org/FRflaws
- NGI/RISC Privacy Impact Assessment: eff.org/FRPIA



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

