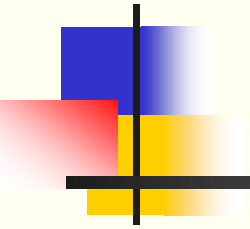
BIOMETRICS 101



Facial Recognition
in Oregon

SB 640

Approved by the Oregon Legislature in 2005
Codified in Oregon Revised Statutes
ORS 807.024 – 807.026

Purpose - *"To address the growing problem of identity theft & fraud in Oregon by requiring the collection & verification of biometric data prior to issuance."*

Supported by the Regional Economic Crime Investigation Center (RECIC) – composed of local, state, & federal law enforcement agencies and the private sector.

SB 640

- KEY COMPONENTS
  - Collection of digital photos to allow facial recognition
  - Verification of identity before issuance
    - One-to-one comparison of photos at the counter
    - One-to-many comparison of photos overnight in batch
  - Interim cards issued at field offices valid up to 60 days
  - Laminated cards with security features are mailed to customers from secure production facility within 5-7 days
  - Biometric data only available to employees acting in official capacity

DRIVING FORCES BEHIND SB 640

- 9/11 – The Threat of Terrorism
- Tighter National Identity Standards - Verification of Identity Documents
- National Standards for Driver Licensing
- Identity Theft Concerns
- Check, Credit Card & Bank Fraud
- Sharing of Driver Records Between States

Uses of Biometric Data

- Primary use is the establishment of the customer's identity
- Identity established when:
  - Biometric data collected matches biometric data in DMV's records for that person
  - Biometric data collected does not match any other person in DMV's records

Uses of Biometric Data

- If person's identity not established:
  - DMV must inform the person and
  - Provide an alternative method for establishing identity
    - Proof of identity/DOB document
    - Letter from a physician if appearance has changed
    - Letter from law enforcement
    - Court document that verifies identity
  - Notify law enforcement if DMV determines the crime of identity theft has been committed

HOW CUSTOMERS ARE AFFECTED

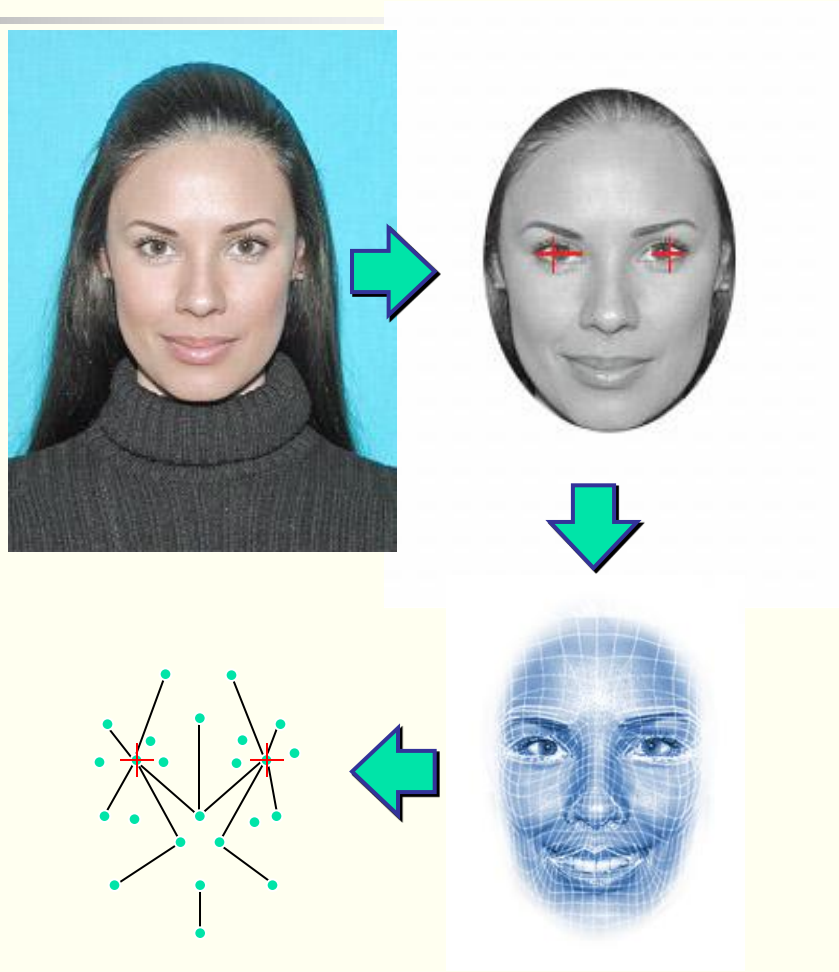
- Tighter issuance standards & requirements increase wait times at DMV
- Increased security measures reduce risk of identity theft
- Driver license or ID card not received immediately
- May not be eligible for driver license or ID card if unable to establish identity

WHAT ARE THE BENEFITS?

- Deters identity theft
- Promotes consistency between states – minimum licensing standards
- Enhances identity verification processes –"You are who you say you are"
- Strengthens concept of "One Identity – One License – One Driver Control Record"

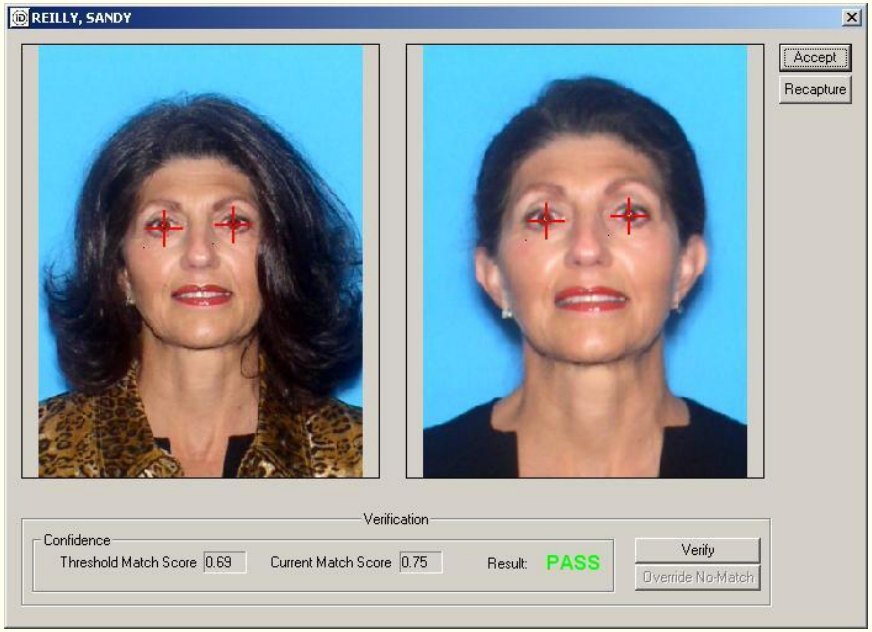
Biometrics – Facial Recognition Workflow

1. Begin with digital image
2. Eye locations are determined
3. Image is converted to grey scale and cropped
4. The image is converted to a template used by the search engine for facial comparison results
5. Searching and matching using a sophisticated algorithm to compare the template to other templates on file



1:1 Facial Matching

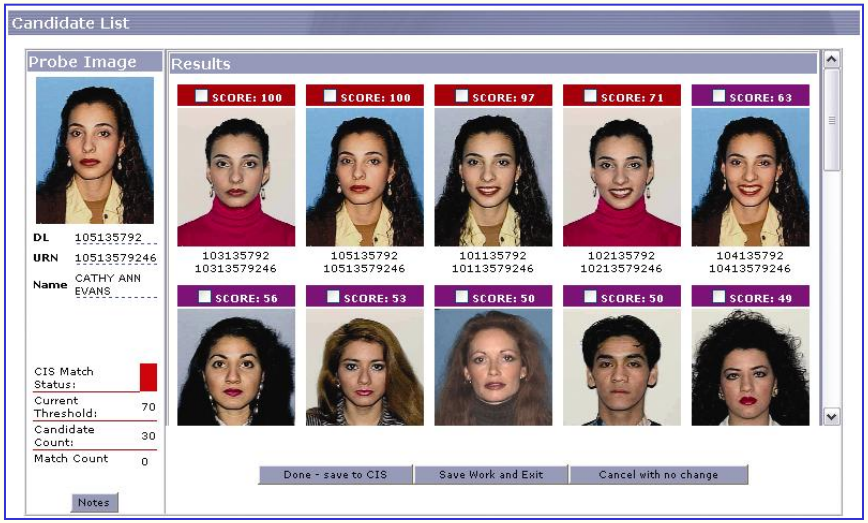
- Verifies the person applying for a renewal license is the person whose previous portrait is in the database
- Compares facial images
  - Compare picture from renewal process image stored in the database
- Usually occurs immediately after image capture



1:1 Facial Matching helps ensure a renewed license is issued to the original applicant.

Biometrics – 1:Many Facial Recognition

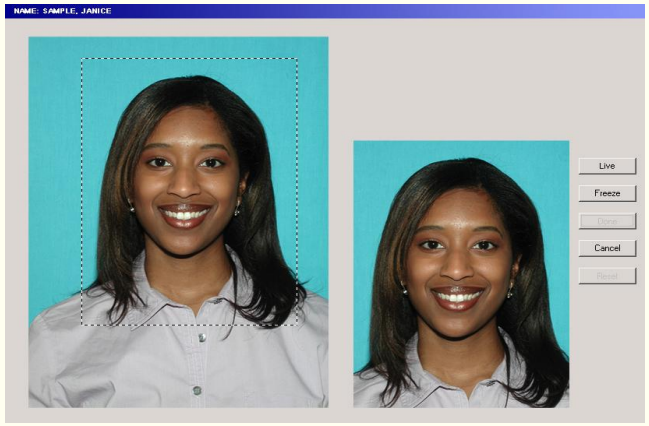
- Search a large database of images quickly to obtain a small number of candidate matches
- Compares the applicant's face template with all the templates in the image database and returns top candidates for a match
- Typically run offline in a batch mode to better identify same-day multiple issuance fraud cases
- Jurisdictions can block DL/ID issuance if fraud is suspected



Can determine if an applicant has multiple enrollments, perhaps under multiple identities, in the database

Portrait Capture Software

- Find-a-face software
  - Fully automatic feature
  - Ultimate portrait consistency
  - Locates applicant face and crops to standard size
- Automatic color correction
  - Ensures uniform portrait brightness for varying complexions



AAMVA STANDARD

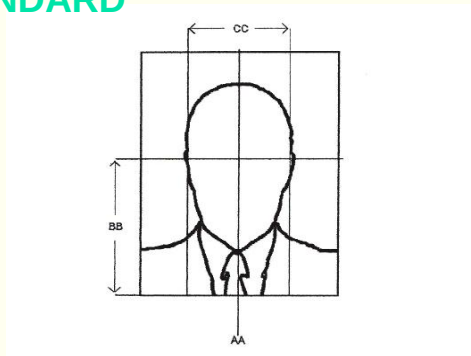
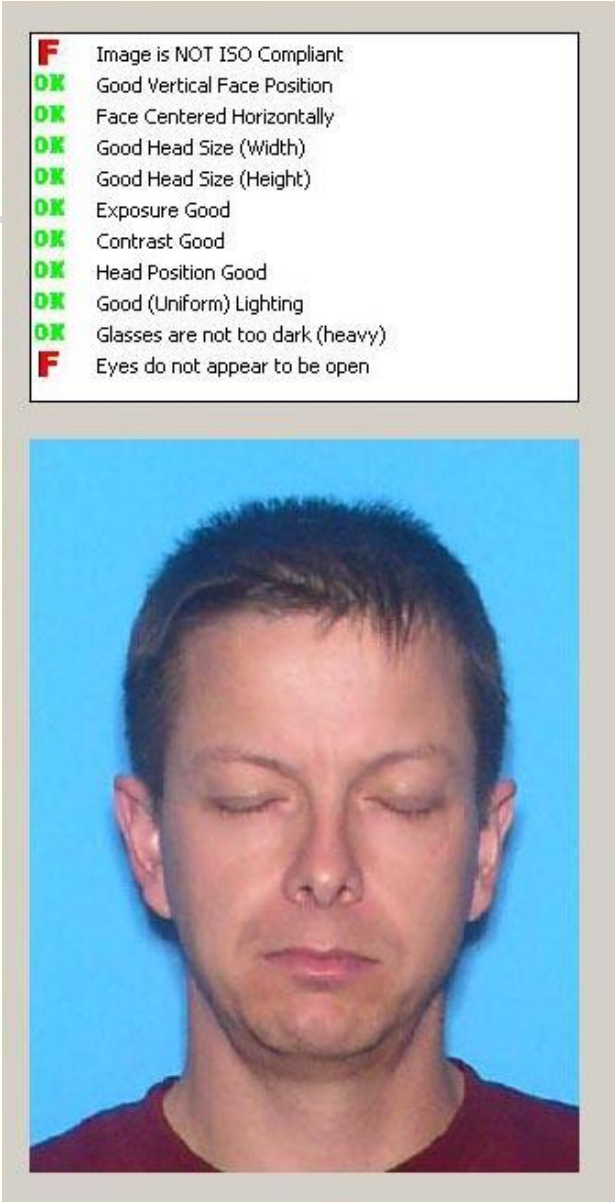


Image Consistency

- Portrait image analysis software
  - Automatically finds applicant's eyes
  - Analyzes image suitability for facial recognition
- Parameters checked
  - Head size
  - Face centering
  - Eyes open and visible
  - Face present
  - Sufficient resolution
  - Others
- Image thoroughly analyzed for compliance with ISO biometric data interchange standard for face images (ISO/IEC 19794-5)



The Blue Man

Privacy of Biometric Data

- Data protection and Security a top priority
- Access granted only as allowed by law
- Access to biometric data is very restricted today

Access to Biometric Data

- General rule: biometric data may not be made available to anyone other than employees of the department acting in an official capacity
- Exception: notification to law enforcement if DMV determines crime of identity theft has occurred

Access to Biometric Data

- Access to results within DMV
  - Generally: only Driver Issuance Unit employees may view results
  - Exception: DMV Administrator or Service Group manager approval

STATISTICS

- 774 cases referred to Law Enforcement since 2008 when program began
- In 2010, 651 license suspension actions initiated

OREGON DMV CONTACTS

- Carol Meireis – Driver Programs
  - Carol.L.Meireis@odot.state.or.us
  - (503) 945-5107
- Allen Duren – DMV Fraud Unit Manager
  - Allen.D.Duren@odot.state.or.use
  - (503) 945-8916

More Information

National Institute of Standards and Technology

- **Report on the Evaluation of 2D Still-Image Face Recognition Algorithms**
- http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968