County of Los Angeles
Chief Executive Office

FESIA A. DAVENPORT
Chief Executive Officer

PUBLIC SAFETY CLUSTER
AGENDA REVIEW MEETING

DATE: **Wednesday, April 21, 2021**
TIME: **10:00 a.m.**

DUE TO CLOSURE OF ALL COUNTY BUILDING, TO PARTICIPATE IN THE MEETING CALL TELECONFERENCE NUMBER: (323) 776-6996 ID: 169948309#
Click here to join the meeting

AGENDA

Members of the Public may address the Public Safety Cluster on any agenda item by submitting a written request prior to the meeting. Two (2) minutes are allowed per person in total for each item.

1. **CALL TO ORDER**

2. **GENERAL PUBLIC COMMENT**

3. **INFORMATIONAL ITEM(S)** [Any Information Item is subject to discussion and/or presentation at the request of two or more Board offices with advance notification]:

   A. NONE

4. **PRESENTATION/DISCUSSION ITEM(S):**

   A. Board Briefing:
   CIVILIAN OVERSIGHT COMMISSION AND OFFICE OF INSPECTOR GENERAL MONTHLY BRIEFING
   Speaker(s): Brian Williams (COC) and Max Huntsman (OIG)

   B. Board Briefing:
   DJJ TRANSITION COMMITTEE BRIEFING
   Speaker(s): Tom Faust and Brandon Nichols (Probation)

   C. Board Briefing:
   LOS ANGELES SHERIFF DEPARTMENT’S FACIAL RECOGNITION BRIEFING
   Speaker(s): Derek Sabatini (Sheriff’s)

5. **PUBLIC COMMENTS**

CLOSED SESSION:

CS-1 **<u>CONFERENCE WITH LEGAL COUNSEL – EXISTING LITIGATION</u>**
(Subdivision (a) of Government Code Section 54956.9)

<u>Alvaro Jimenez v. County of Los Angeles, et al.</u>
United States District Court Case No. 2-19-CV-08680

Departments: Sheriff's

6. ADJOURNMENT

7. UPCOMING ITEMS:

A. Board Letter:
APPROVAL OF AMENDMENT NUMBER THREE TO SCHOOL LAW ENFORCEMENT SERVICES AGREEMENT FOR THE SCHOOL RESOURCE DEPUTY PROGRAM
Speaker(s): Brian C. Aguilera and Rudy P. Sanchez (Sheriff)

B. Board Briefing:
REOPENING COUNTY JAIL VISITATION
Speaker(s): Hugo Macias (Sheriff)

IF YOU WOULD LIKE TO EMAIL A COMMENT ON AN ITEM ON THE PUBLIC SAFETY CLUSTER AGENDA, PLEASE USE THE FOLLOWING EMAIL AND INCLUDE THE AGENDA NUMBER YOU ARE COMMENTING ON:

PUBLIC_SAFETY_COMMENTS@CEO.LACOUNTY.GOV

LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

Facial Recognition Brief

Board of Supervisor’s Cluster Agenda Review

04/21/2021

TABLE OF CONTENTS

- Who is LACRIS
- What is Facial Recognition
- Authorization and Accountability
- LACRIS Newsletters
- Open Discussion

Who is LACRIS

- A Department Of Justice program (Cal-ID) established in the California Penal Code to assist local law enforcement agencies with biometric collection and identification of arrested individuals.
- The Sheriff of each county is directed to oversee the Cal-ID program, known as the Los Angeles County Regional Identification System (LACRIS) in the county of Los Angeles.
- LACRIS manages the Digital Mugshot System (DMS) which uses Facial Recognition Technology (FRT) to help develop investigative leads; while saving time and resources when searching through the over seven million booking photos we have stored in the DMS.
- We have expert personnel on our staff such as Mark Dolfi who is the Chair of the Facial Identification Scientific Working Group (FISWIG), a member of the International Association for Identification (IAI) and a member of the Organization of Scientific Area Committees (OSAC).

International Association for Identification

FACIAL IDENTIFICATION SCIENTIFIC WORKING GROUP FISWG

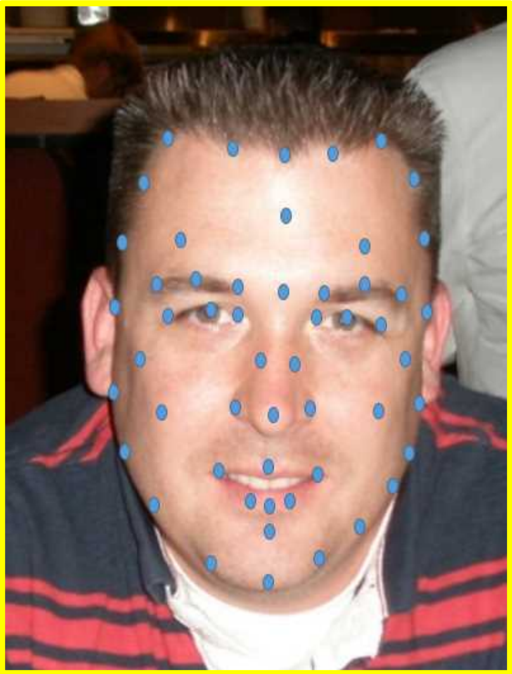
WHAT IS FACIAL RECOGNITION

It is the automated searching of a probe image
(from a crime scene) in a biometric database to generate
an investigative lead

- Measurements of facial features – automates previous practices
- Not identification – It's a lead
- Two parts to a Facial Investigation
    - Facial Recognition – computer driven list of potential candidates
    - Suspect Identification – human investigation generating probable cause for an arrest

WHAT IS FACIAL RECOGNITION

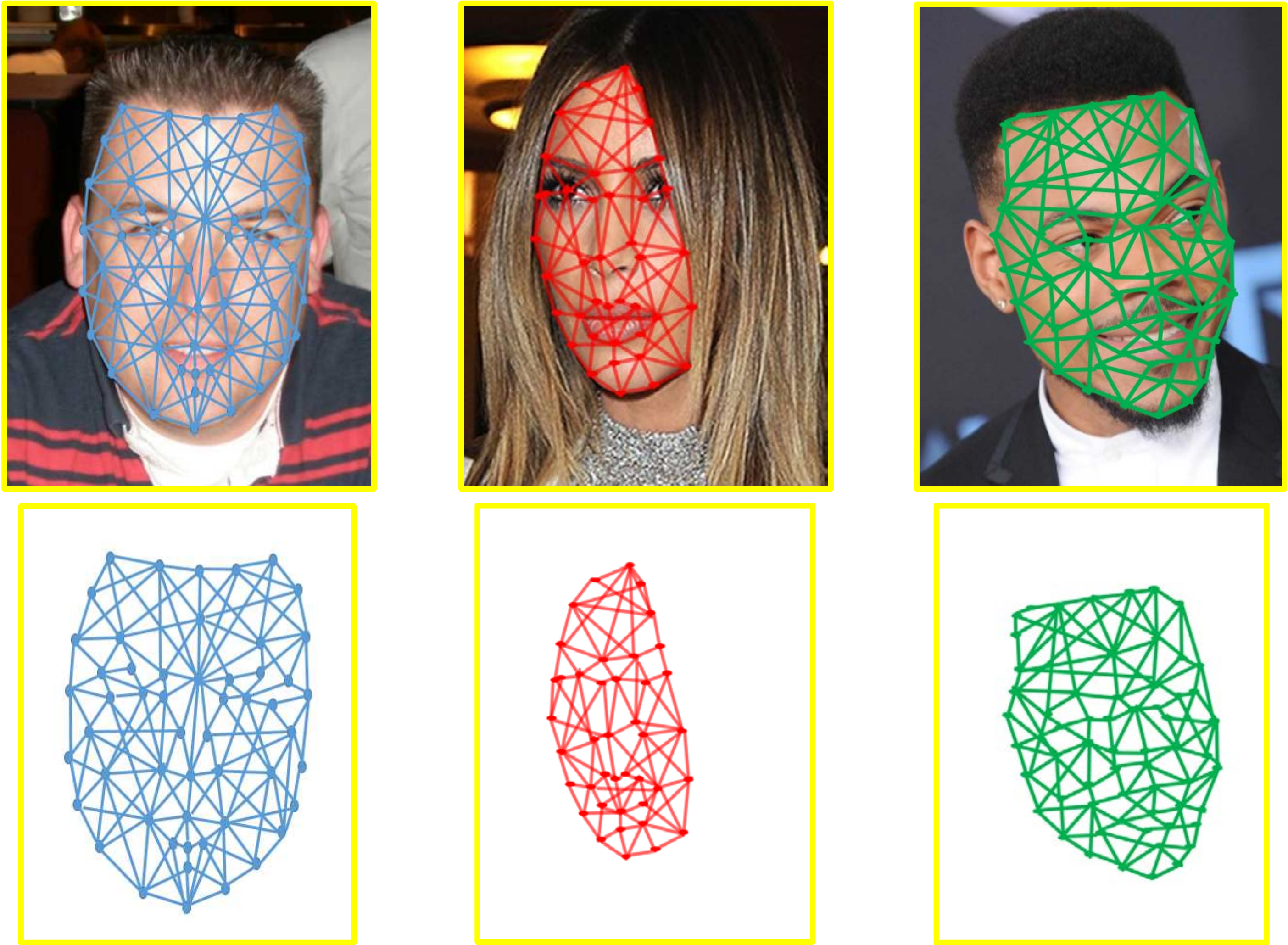
Upload
Unknown
(Probe)
Image



Face is Plotted
by Algorithm

Plotted
at the pixel level

WHAT IS FACIAL RECOGNITION



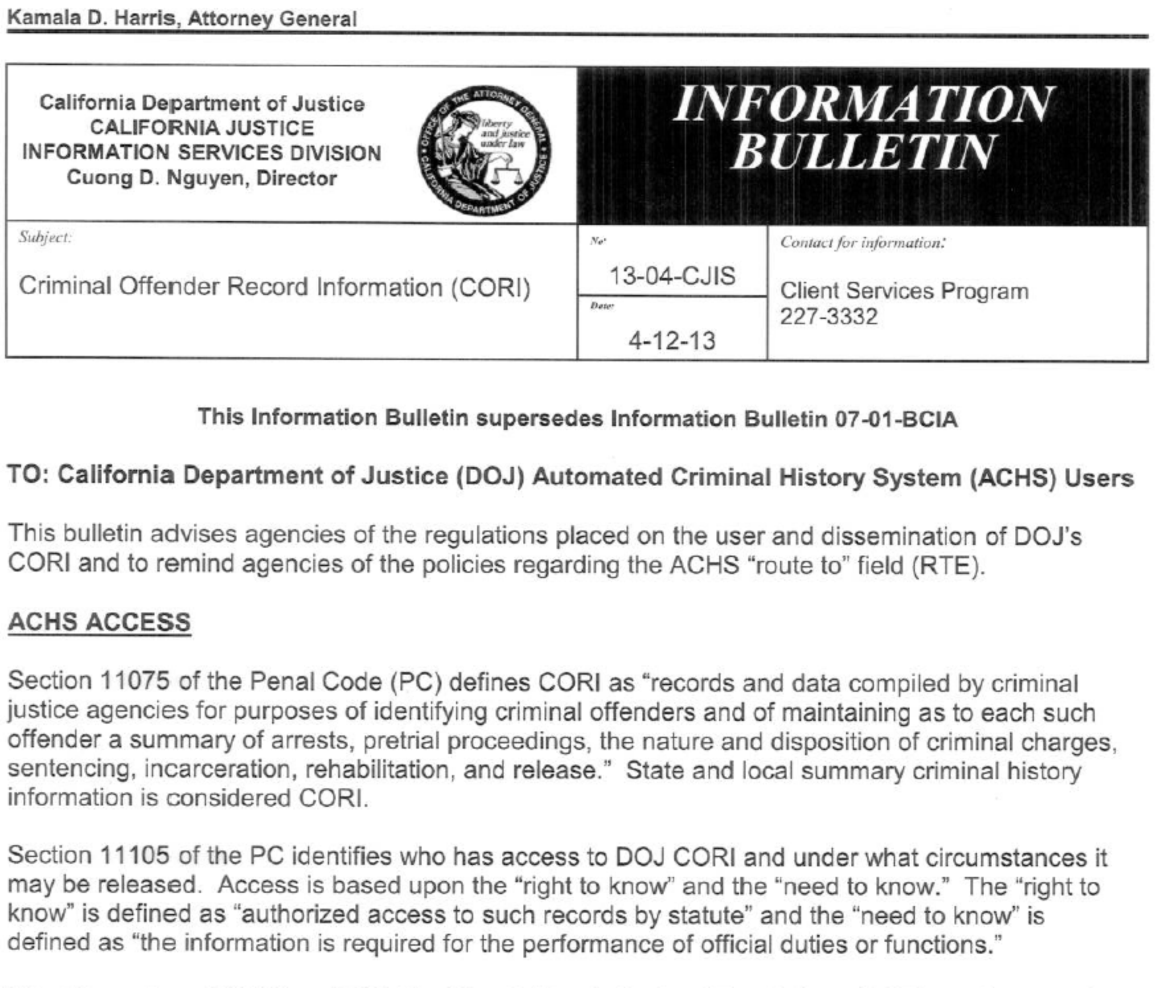
AUTHORIZATION AND ACCOUNTABILITY

IN USE SINCE 2009

- Criminal Offender Records Information (CORI)
  - Right to know and need to know
  - Criminal penalties when not followed
- Policy in place
  - Purpose
  - Identify source and content of database
  - Training prior to utilization
- The DMS does not have connectivity to public records (DMV photos, social media accounts, etc.)

AUTHORIZATION AND ACCOUNTABILITY

Criminal Offender Records Information (CORI)



Kamala D. Harris, Attorney General

California Department of Justice
CALIFORNIA JUSTICE
INFORMATION SERVICES DIVISION
Cuong D. Nguyen, Director

INFORMATION BULLETIN

Subject: Criminal Offender Record Information (CORI)	*No* 13-04-CJIS *Date* 4-12-13	*Contact for information:* Client Services Program 227-3332

This Information Bulletin supersedes Information Bulletin 07-01-BCIA

TO: California Department of Justice (DOJ) Automated Criminal History System (ACHS) Users

This bulletin advises agencies of the regulations placed on the user and dissemination of DOJ's CORI and to remind agencies of the policies regarding the ACHS "route to" field (RTE).

ACHS ACCESS

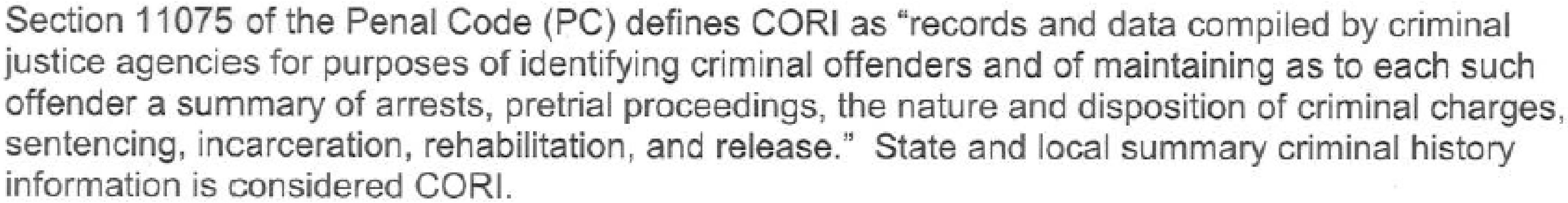
Section 11075 of the Penal Code (PC) defines CORI as "records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release." State and local summary criminal history information is considered CORI.

Section 11105 of the PC identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the "right to know" and the "need to know." The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions."

AUTHORIZATION AND ACCOUNTABILITY

Criminal Offender Records Information (CORI)

11075 PC defines CORI as “records and data compiled by criminal justice agencies for the purpose of identifying criminal offenders.

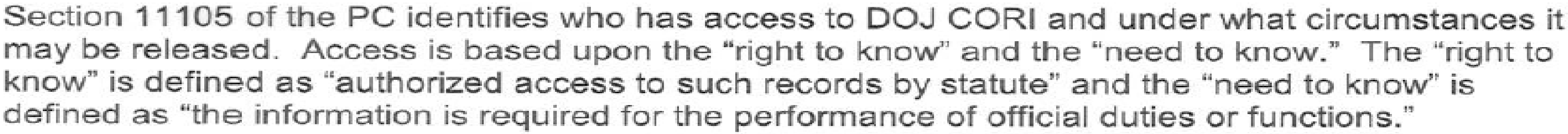


Section 11075 of the Penal Code (PC) defines CORI as “records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.” State and local summary criminal history information is considered CORI.

AUTHORIZATION AND ACCOUNTABILITY

Criminal Offender Records Information (CORI)

11105 PC identifies who has access to CORI based on a “right to know” and a “need to know.”

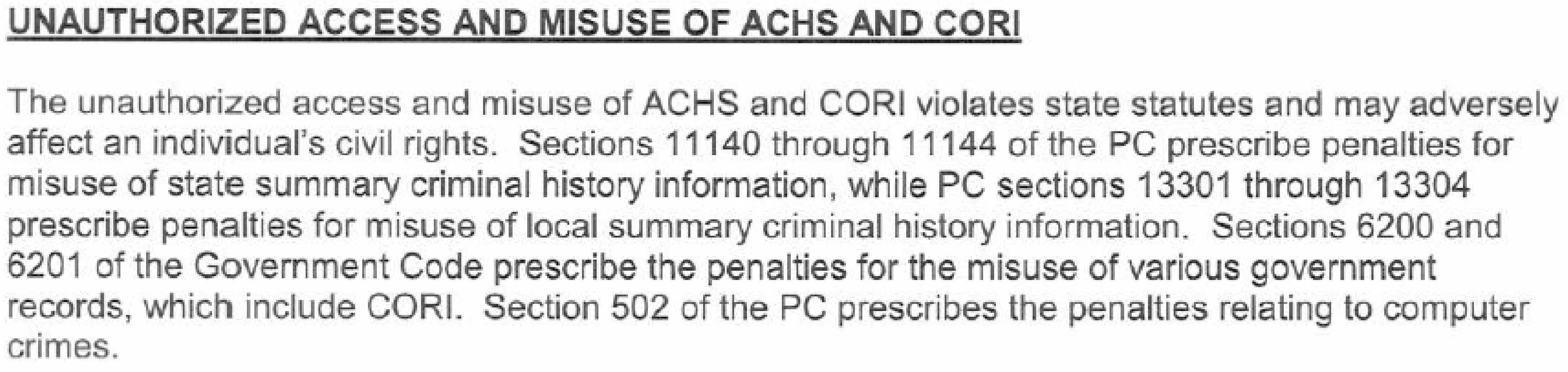


Section 11105 of the PC identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the “right to know” and the “need to know.” The “right to know” is defined as “authorized access to such records by statute” and the “need to know” is defined as “the information is required for the performance of official duties or functions.”

AUTHORIZATION AND ACCOUNTABILITY

Criminal Offender Records Information (CORI)

Numerous Penal Code sections and Government Code sections identifying penalties for misuse and unauthorized access to CORI records.



UNAUTHORIZED ACCESS AND MISUSE OF ACHS AND CORI

The unauthorized access and misuse of ACHS and CORI violates state statutes and may adversely affect an individual's civil rights. Sections 11140 through 11144 of the PC prescribe penalties for misuse of state summary criminal history information, while PC sections 13301 through 13304 prescribe penalties for misuse of local summary criminal history information. Sections 6200 and 6201 of the Government Code prescribe the penalties for the misuse of various government records, which include CORI. Section 502 of the PC prescribes the penalties relating to computer crimes.

AUTHORIZATION AND ACCOUNTABILITY

Local Policy

LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

FACE RECOGNITION POLICY

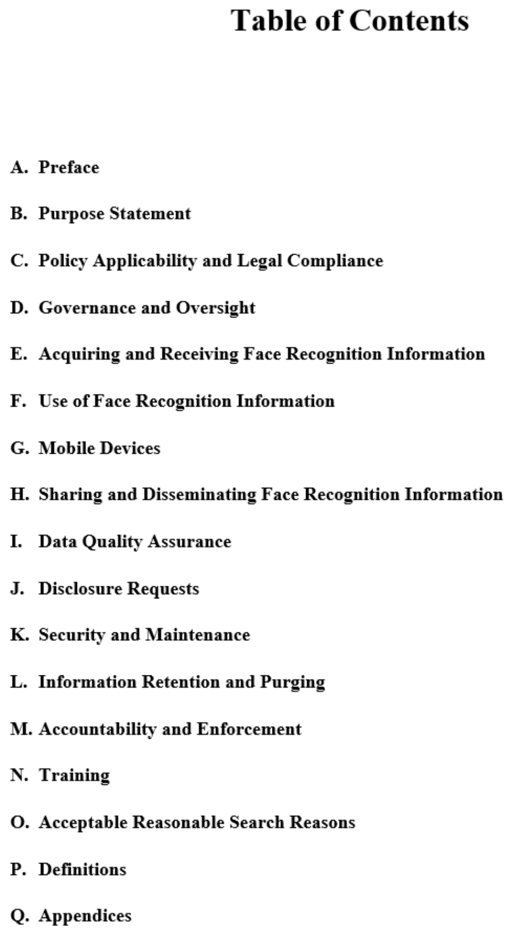


Table of Contents

A. Preface

B. Purpose Statement

C. Policy Applicability and Legal Compliance

D. Governance and Oversight

E. Acquiring and Receiving Face Recognition Information

F. Use of Face Recognition Information

G. Mobile Devices

H. Sharing and Disseminating Face Recognition Information

I. Data Quality Assurance

J. Disclosure Requests

K. Security and Maintenance

L. Information Retention and Purging

M. Accountability and Enforcement

N. Training

O. Acceptable Reasonable Search Reasons

P. Definitions

Q. Appendices

AUTHORIZATION AND ACCOUNTABILITY

Local Policy

It is the purpose of this policy to provide Los Angeles County law enforcement personnel with standards, guidelines, and recommendations for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of an FR program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

Further, this policy will delineate the manner in which FR requests are received, processed, catalogued, and responded to. The California Criminal Offender Records Information (CORI) Information Bulletin 13-04-CJIS and the United States Federal Trade Commission's Fair Information Practice Principles (FIPP) form the core of the privacy framework for this policy

AUTHORIZATION AND ACCOUNTABILITY

Local Policy

The result of an FR search is provided by LACRIS only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

LACRIS does not connect the DMS system to any interface that performs live video surveillance, including but not limited to, surveillance cameras, license plate readers, drone footage, and body-worn cameras. The DMS system is configured to conduct FR analysis from a recorded video or still image(s).

AUTHORIZATION AND ACCOUNTABILITY

Local Policy - Training

LACRIS provides an FR training course and follows the recommendations of the Facial Identification Scientific Working Group's (FISWG.ORG) ***Minimum Training Criteria for Usage of Facial Recognition Systems***. If an agency creates their own additional training it cannot conflict with LACRIS's policies or training, and it is recommended they follow the above document.

Before access to LACRIS's DMS is authorized, the Cal-ID Manager requires the following individuals to participate in training regarding implementation of and adherence to this face recognition policy:

All authorized LACRIS personnel
All authorized participating agency personnel
All authorized contractor personnel

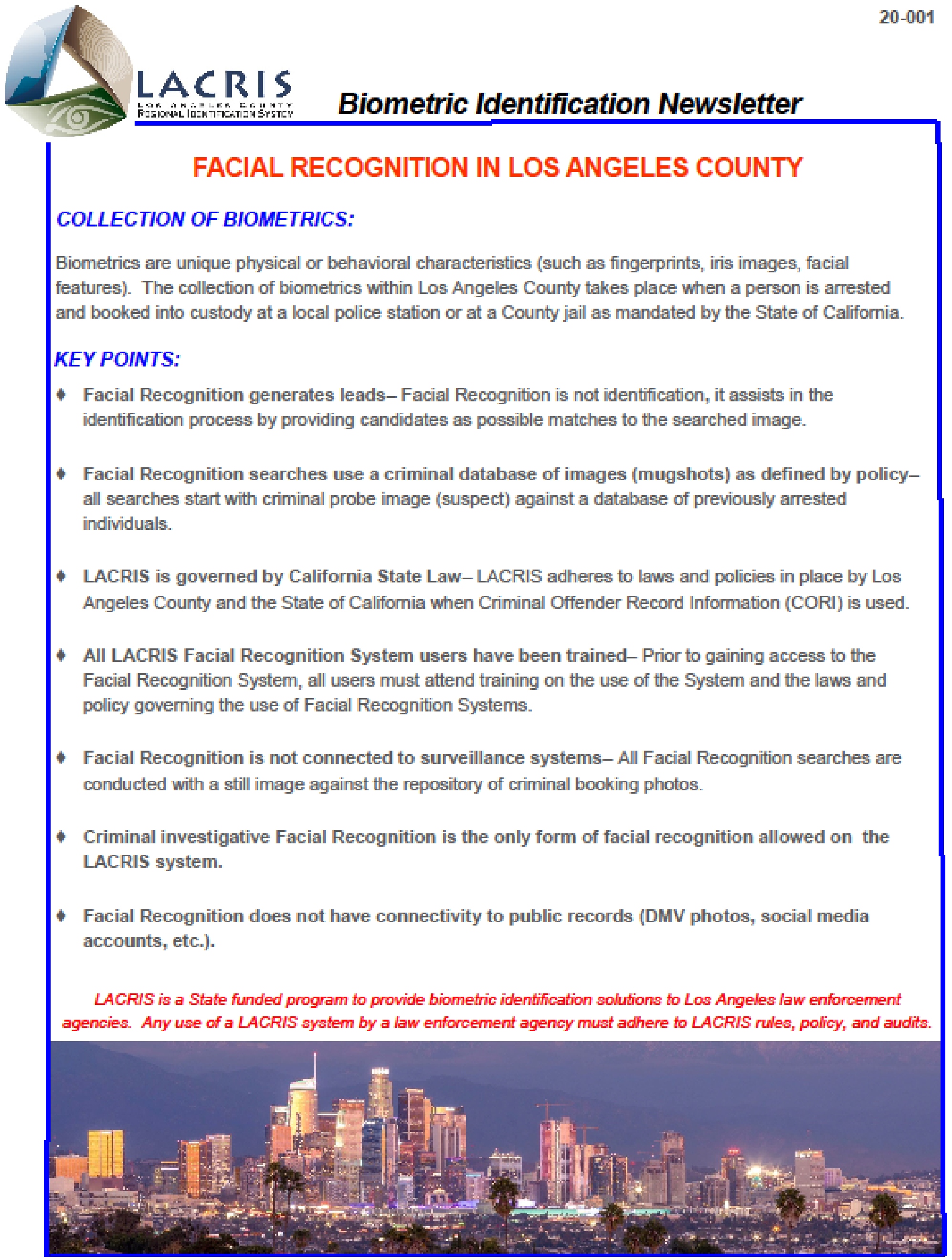
AUTHORIZATION AND ACCOUNTABILITY

Local Policy – Auditing

LACRIS maintains an audit trail on the use of the DMS. This audit trail includes user activity within the DMS (i.e. searches conducted, photos views, photos printed, etc.). The audit trail is maintained separately for each photo in the DMS.

LACRIS conducts random audits of user activity to ensure the use of the DMS is justified and a reason for access is provided to follow the CORI act and LACRIS policy. In addition to the audits LACRIS conducts on all users activity, each agency is assigned a local administrator who is responsible for auditing their users in their agency/bureau for compliance of the laws and policies in regards to use of the DMS.

All audits and audit trails are kept for a minimum of three (3) years.



20-001

LACRIS

LOS ANGELES COUNTY REGIONAL IDENTIFICATION SYSTEM

Biometric Identification Newsletter

FACIAL RECOGNITION IN LOS ANGELES COUNTY

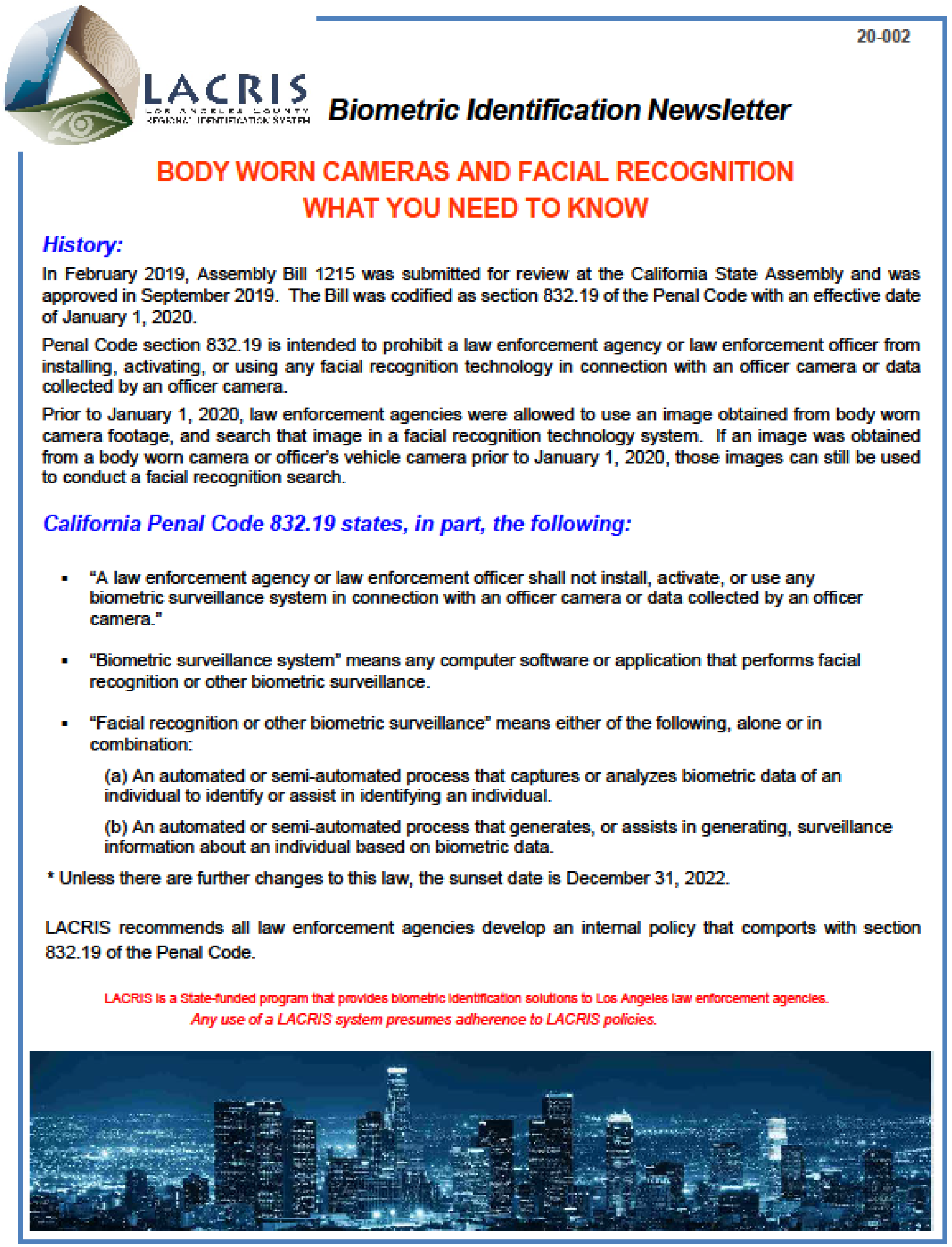
COLLECTION OF BIOMETRICS:

Biometrics are unique physical or behavioral characteristics (such as fingerprints, iris images, facial features). The collection of biometrics within Los Angeles County takes place when a person is arrested and booked into custody at a local police station or at a County jail as mandated by the State of California.

KEY POINTS:

- **Facial Recognition generates leads**– Facial Recognition is not identification, it assists in the identification process by providing candidates as possible matches to the searched image.
- **Facial Recognition searches use a criminal database of images (mugshots) as defined by policy**– all searches start with criminal probe image (suspect) against a database of previously arrested individuals.
- **LACRIS is governed by California State Law**– LACRIS adheres to laws and policies in place by Los Angeles County and the State of California when Criminal Offender Record Information (CORI) is used.
- **All LACRIS Facial Recognition System users have been trained**– Prior to gaining access to the Facial Recognition System, all users must attend training on the use of the System and the laws and policy governing the use of Facial Recognition Systems.
- **Facial Recognition is not connected to surveillance systems**– All Facial Recognition searches are conducted with a still image against the repository of criminal booking photos.
- **Criminal investigative Facial Recognition is the only form of facial recognition allowed on the LACRIS system.**
- **Facial Recognition does not have connectivity to public records (DMV photos, social media accounts, etc.).**

LACRIS is a State funded program to provide biometric identification solutions to Los Angeles law enforcement agencies. Any use of a LACRIS system by a law enforcement agency must adhere to LACRIS rules, policy, and audits.



20-002

LACRIS

LOS ANGELES COUNTY REGIONAL IDENTIFICATION SYSTEM

Biometric Identification Newsletter

BODY WORN CAMERAS AND FACIAL RECOGNITION WHAT YOU NEED TO KNOW

History:

In February 2019, Assembly Bill 1215 was submitted for review at the California State Assembly and was approved in September 2019. The Bill was codified as section 832.19 of the Penal Code with an effective date of January 1, 2020.

Penal Code section 832.19 is intended to prohibit a law enforcement agency or law enforcement officer from installing, activating, or using any facial recognition technology in connection with an officer camera or data collected by an officer camera.

Prior to January 1, 2020, law enforcement agencies were allowed to use an image obtained from body worn camera footage, and search that image in a facial recognition technology system. If an image was obtained from a body worn camera or officer's vehicle camera prior to January 1, 2020, those images can still be used to conduct a facial recognition search.

California Penal Code 832.19 states, in part, the following:

- "A law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera."
- "Biometric surveillance system" means any computer software or application that performs facial recognition or other biometric surveillance.
- "Facial recognition or other biometric surveillance" means either of the following, alone or in combination:

  (a) An automated or semi-automated process that captures or analyzes biometric data of an individual to identify or assist in identifying an individual.

  (b) An automated or semi-automated process that generates, or assists in generating, surveillance information about an individual based on biometric data.

* Unless there are further changes to this law, the sunset date is December 31, 2022.

LACRIS recommends all law enforcement agencies develop an internal policy that comports with section 832.19 of the Penal Code.

LACRIS is a State-funded program that provides biometric identification solutions to Los Angeles law enforcement agencies.

Any use of a LACRIS system presumes adherence to LACRIS policies.

20-003

LACRIS
LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

Biometric Identification Newsletter

FACIAL RECOGNITION IN LOS ANGELES COUNTY

REMEMBER:

Facial recognition creates leads. All Facial Recognition (FR) identifications in the stories below were generated from investigative leads; FR does not identify. In order to simplify the stories below, FR identifications mean leads that led to identifications through investigations. The LACRIS Digital Mugshot System (DMS) has an FR tool to develop candidate lists, to which an investigator may be able to develop a lead. It is the investigators responsibility to conduct a thorough investigation in order to identify the suspect from the DMS investigative leads.

SUCCESS STORIES:

- **Los Angeles Police Department**– A suspect entered a LA Family Dollar Store, brandished a handgun and demanded the money. He received approximately $200 and left the location and ran into a nearby medical facility where he was caught on their surveillance cameras waiting for his girlfriend. The store surveillance video was not of good quality, but an image from the medical system was entered into DMS and a solid candidate resulted. Upon further investigation and an identification from the victims in the Family Dollar Store, the suspect was apprehended.

- **Los Angeles Police Department**– A home invasion occurred where one of the suspects shot and killed the resident. The shooter was detained by the victim's family, however his accomplice fled the scene. The shooter's girlfriend provided a photo of the suspect, but didn't know his name. The photo was entered into DMS, a lead was developed and the suspect was identified by the surviving victims.

- **Long Beach Police Department**– A male and female entered a home and stole property. A home monitoring system was able to produce an image of the female, but not the male. Her image was entered into DMS and a candidate was identified through further investigation. She provided the name of the male suspect.

- **Arcadia Police Department**– A home invasion robbery and assault occurred after the victim was followed home from a casino. Video of the suspects were obtained from the casino. A lead was developed after his image was entered into DMS. The suspect was positively identified in a lineup and the victim's property was recovered in his possession.

LACRIS is a State funded program to provide biometric identification solutions to Los Angeles law enforcement agencies. Any use of a LACRIS system by a law enforcement agency must adhere to LACRIS rules, policy, and audits.

OPEN DISCUSSION

LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

LACRIS Facial Recognition Policy

LACRIS Facial Recognition Policy

A. Preface

B. Purpose Statement

C. Digital Mugshot System

D. Authority

E. Training

F. Auditing

G. Accountability and Enforcement

H. Face Search Request

A. Preface

The Los Angeles County Regional Identification System (LACRIS) has developed a policy that shall be used as the foundation for those agencies that choose to utilize the LACRIS facial recognition system. LACRIS is responsible for the governance, oversight, and operation of its facial recognition system and program which it provides to the law enforcement community inside the county of Los Angeles. This policy is intended for LACRIS personnel and any authorized agency personnel accessing the system. Agencies are encouraged to implement their own policy which complements and does not contradict the LACRIS policy.

B. Purpose Statement

Facial recognition technology involves the ability to examine and compare significant characteristics of the human face. This technology can be a valuable tool to create investigative leads, reduce an imminent threat to health or safety, and help in the identification of deceased persons or persons unable to identify themselves. This facial recognition application supports the investigative efforts of law enforcement and public safety agencies within Los Angeles County resides in the County's Digital Mugshot System (DMS).

C. Digital Mugshot System

Established October 1, 2009, the DMS is the County's repository of all criminal mugshots. It only contains criminal mugshots which are supported by a fingerprint comparison conducted by the California Department of Justice (DOJ). Section 13150 of the California Penal Code requires at time of booking, a subject's fingerprints, photos, and arrest data to be collected, stored, and reported to the DOJ. This information is maintained in the DMS and used for investigative purposes by law enforcement personnel.

D. Authority

All deployments of the DMS facial recognition application are for official use only and considered law enforcement sensitive. The DMS is subject to the DOJ regulations placed on users and the dissemination of Criminal Offender Record Information (CORI).

The California Attorney General's Office issued Information Bulletin 13-04-CJIS, which provides guidance to law enforcement personnel on “right to know” and “need to know” access to CORI for investigative and official business purposes. This Bulletin, while not legally binding, references the relevant statutory codes (see below) that must be adhered to by users accessing the system.

Section 11075 of the California Penal Code (PC) defines CORI as “records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.”

Section 11105 of the PC identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the "right to know" and the "need to know." The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions." Title 11, sections 703 (d) and 707 (b) of the California Code of Regulations (CCR) require agencies to conduct record clearances on all personnel hired who have access to CORI. The unauthorized access and misuse of ACHS and CORI violates state statutes and may adversely affect an Individual's civil rights. Sections 11140 through 11144 of the PC prescribe penalties for misuse of state summary criminal history information, while PC sections 13301 through 13304 prescribe penalties for misuse of local summary criminal history information. Sections 6200 and 6201 of the Government Code prescribe the penalties for the misuse of various government records, which include CORI. Section 502 of the PC prescribes the penalties relating to computer crimes.

Title 11, section 707 (c) of the CCR requires each authorized agency to maintain, and make available for inspection, an audit trail for a period of three years from the date of release of CORI from an automated system. The audit trail must provide an agency with sufficient information to substantiate the "need to know."

Section 11078 of the PC requires each agency, holding or receiving CORI in a computerized system, to maintain a listing (audit trail) of the agencies to which it has released or communicated CORI. Also, pursuant to section 707 (c) of the CCR, this audit trail must be maintained for a period of three years and must include any routine releases.

All code sections, which may be amended from time to time, are current as of the time of the implementation of this policy.

E. Training

LACRIS provides training to those investigators who have requested and are authorized to access the facial recognition application for official use. Personnel who are authorized by their participating agency may utilize the facial recognition application *only* after they have been successfully trained by LACRIS personnel. Facial recognition Training provided by LACRIS meets the FBI's Criminal Justice Information Services (CJIS) minimum training criteria for usage of facial recognition systems.

F. Auditing

LACRIS will ensure that the DMS technology provided complies with the then current CJIS Security Policy in regard to audits. The DMS automatically audits user actions such as, logon time, date search, subject viewed, etc. LACRIS personnel will conduct random audits of users and report their findings directly to the user's agency. LACRIS audits user's search and activity compliance to include search reason, number of searches, subject status, watch list entries, etc. Audit report data will be complied and stored at LACRIS for a minimum of three (3) years.

G. Accountability and Enforcement

LACRIS maintains several applications that must adhere to regulations and laws which includes user access. Through audits, if LACRIS determines there was misuse or a violation of these regulations and/or laws, it must take corrective action. Depending on the severity of the violation, LACRIS will hold those user(s) accountable for their actions. Penalties may include but are not limited to restricted access, revoked access, or prosecution. Users may also be subject to additional discipline from their respective agency, as well as other law enforcement agencies, including but not limited to State or Federal agencies.

H. Face Search Request

Outside agencies, or investigators from outside agencies, may request facial recognition searches to assist with investigations through LACRIS only if the LACRIS ***Face Recognition Search Request Form*** is completed. This form can be obtained through the LACRIS Help Desk at lacrishd@lasd.org and will require the following minimum information:

- Requesting Agency
- Requester Name Requester Phone Number
- Requester Email
- Requester Signature
- Requester Date
- Reason for Search
- Case/File Number
- Number of Images Submitted

LACRIS personnel will review each request prior to processing to ensure compliance with this policy. Users acknowledge the result of any facial recognition search provided by LACRIS shall be deemed only an investigative lead and **RESULTS ARE NOT TO BE CONSIDERED AS PROVIDING A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

Facial Recognition Technology: Ensuring Transparency for LEA in Los Angeles County

Statement for the Record

The following is a statement from the Los Angeles County Regional Identification System (LACRIS) on the use of Facial Recognition Technology (FRT) being used by all Law Enforcement Agencies (LEA) in Los Angeles County (County).

Facial Recognition (FR), when used properly, can greatly enhance law enforcement capabilities to better protect public safety. However, if used carelessly and improperly, may negatively impact privacy and infringe on civil liberties. LACRIS has made FRT available to the LEA community within the County since 2006. The current software solution, Los Angeles PhotoManager (LAPH) was implemented in 2009.

LACRIS is committed to the protection of privacy and civil liberties when our systems are utilized by LEA. We provide some of the most comprehensive training for all of the systems we procure and support, FR among them. The training program require~~d~~ users to attend training and successfully pass before they can utilize FRT. This is in line with the Federal Bureau of Investigation's (FBI) standards and procedures. The FBI's training program was co-developed by Mark Dolfi, who is a LACRIS employee. Mr. Dolfi also chairs the Facial Identification Scientific Working Group's (FISWG) Training Task Group. The FISWG Training Task Group created the training standards adopted by the FBI. LACRIS' training program is known throughout the country as one of only a few class offerings that meet/exceed the requirements put forth by the FBI when it comes to using FRT.

Key points of FRT that LACRIS provides to the LEA community:

- LACRIS policy strictly governs the circumstances in which FR may be utilized, including what probe images may be used.
- FRT is provided strictly for law enforcement purposes with human review and additional investigation needed for each search.
- The use of FR produces a potential investigative lead and requires investigative follow-up to corroborate the lead before any action is taken.
- LACRIS is committed to ensuring that the FRT capabilities are regularly tested, evaluated, and improved.
- FR is not identification, nor can it be the sole basis of an arrest or detention.
- Audits of user activity within the system are routinely audited to prevent misuse, and to identify potential training topics for future users.
- FR tools offered to the Los Angeles Law Enforcement community is not surveillance. The system does not have the capability to record, ingest, process, scan, or save live video feeds.

It is important to mention that from a technical and information security perspective; FRT operates as a subsystem within LACRIS systems. All LACRIS subsystems (i.e. FR, Mobile ID, etc.) must follow security protocols and receive the appropriate security testing and authorization to operate within the Sheriff's Data Network (SDN).

The Los Angeles PhotoManager (LAPH) is a photograph repository that is known as the Digital Mugshot System (DMS). In the DMS, all criminal mugshots are associated with criminal tenprint fingerprints and a criminal history record. The DMS allows automated FR searches by trained and authorized users. The user submits an unknown or "probe" photo that is obtained pursuant to an authorized law enforcement investigation, to be searched against the mugshot repository. The DMS then returns a gallery of "candidate" photos. During the second step of the process, the user manually reviews the candidate photos and performs a more thorough one-to-one investigation to determine if any of the candidate photos are potentially the same person as the probe photo.

In March 2020, LACRIS enacted policy that required all law enforcement users to have completed training prior to conducting FR searches within the DMS. The training is conducted by LACRIS personnel and is consistent with the *Guidelines and Recommendations for Facial Comparison Training to Competency*, as outlined by FISWG. This document provides the recommended elements of training to achieve competency in facial comparisons.

As FR use expands, it is necessary for law enforcement agencies to ensure that comprehensive policies are developed, adopted, and implemented. Having such policies will guide the agency and its personnel in the day-to-day access and use of FRT. Once the policies are implemented, full compliance of the Criminal Offender Record Information (CORI) act and LACRIS policies will be achieved.

LACRIS performs audits of user activity within the DMS as they serve an important role in identifying and mitigating risks associated with users of information systems not meeting policy requirements. In addition, LACRIS requires all participating LEA to conduct their own audits of their employees.

LACRIS continues to identify and use new biometric criminal investigative technologies, such as new algorithms for FRT, to meet the high expectations of the law enforcement community when investigating crimes. The LACRIS mission is to collect criminal biometrics for the California Department of Justice, while providing biometric technology for safer communities. In order to comply with our mission, we embrace technologies such as FRT, while ensuring strong policies and auditing are in place to safeguard the public's civil liberties.