San Diego Regional Facial Recognition System Policy

POLICIES CONCERNING THE USE OF AN AUTOMATED FACIAL RECOGNITION FIELD IDENTIFICATION TOOL

Table of Contents

PREFACE

These policies are intended to provide law enforcement agencies uniform guidance regarding their appropriate use of a facial recognition field identification tool. Nlets sponsored the preparation of its *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* to better describe the privacy issues surrounding law enforcement agencies' utilization of facial recognition technologies in the field. These policies were generated in response to the discussions contained in that report.

The intent of these policies is to:

Address the privacy issues raised by the use of facial recognition systems to identify individuals in public.

The language used in these proposed policies must be assigned its plain and ordinary meaning and individual sections should be implemented in such a way as to give effect to the entire policy. Where two proposed provisions deal with the same subject but one is specific and the other general, the more specific policy provision controls.

Part A: PURPOSES FOR COLLECTING FACIAL RECOGNITION INFORMATION

101 Law enforcement agencies collect, compare, and disseminate facial images to aid in the visual identification of:

a) Individuals who come into direct contact with criminal justice practitioners;

b) Individuals who are reasonably suspected of having committed a crime; and

c) Individuals who a law enforcement officer reasonably suspect is about to commit a crime.

102 Law enforcement agencies may request facial recognition comparison information from a criminal justice booking system or other photo repository:

a) To assist an officer in assessing the situation and evaluating any threats to his own safety;

b) To conduct a criminal investigation;

c) To gather information for an intelligence purpose in accordance with 28 C.F.R. Part 23; and

d) To conduct a government security clearance background check.

103 Where appropriate, facial image databases may be accessed to aid in locating a missing person or an individual for whom a warrant has been issued.

Part B: COLLECTION OF FACIAL IMAGES BY LAW ENFORCEMENT AGENCIES

201 Individuals in personal contact with law enforcement officers. Law enforcement officers may collect facial images of individuals with whom they are in personal contact for the purpose of submitting those images to a facial recognition field identification tool in the following circumstances:

a) With the individual's consent;

b) When identifying the individual will assist the officer in assessing the situation and evaluating any threats to his own safety;

c) When state law requires individuals to identify themselves to police officers;

d) When the individual is lawfully detained and when the suspect's identity is related to the investigation of the suspicion that originally justified the detention; and

e) When the individual is lawfully detained and using the facial recognition field identification tool does not prolong the detention beyond the time reasonably required to complete the investigation of the suspicion that originally justified the detention.

202 Individuals not in personal contact with law enforcement officers. Law enforcement officers may capture facial images for the purpose of submitting those images to a facial recognition field identification tool in the following circumstances:

a) As part of the investigation of a crime; and

b) As part of an intelligence-gathering effort that:

> i) Is conducted in compliance with the U.S. Department of Justice's rules and policies governing criminal intelligence systems at 28 C.F.R. Part 23; and
>
> ii) Limits the collection of facial images from areas that reasonably relate to an individual's political, religious or social views, associations, or activities to instances directly related to criminal conduct or activity.

203 No individual shall be physically detained, nor the individual's movement otherwise hindered, for the exclusive purpose of collecting their facial image for submission to a facial recognition field identification tool.

Part C: ACCESS TO FACIAL RECOGNITION FIELD IDENTIFICATION RESULTS

301 Law enforcement officers should not request facial recognition field identification results when an individual presents a valid driver license or state identification card unless:

a) The officer reasonably suspects the driver license or identification card is forged, altered, or otherwise fraudulent; or

b) The officer reasonably suspects the individual is presenting, as his or her own, a driver license or identification card issued by a DMV to another person.

302 Where practical, and where it will not negatively impact officer safety, law enforcement officers should first request verification of an individual's identity through a query of their name, date of birth, and other self-reported identifiers. When verification is not possible, or if the officer reasonably suspects the self-reported information is false, officers may request facial recognition field identification results.

303 Where practical, law enforcement officers should submit publicly observable demographic information related to the facial image when requesting facial recognition field identification results.

304 Law enforcement officers shall only access the personally identifying or biographical information of individuals whose facial image is contained in the results of a facial recognition field identification query:

a) After determining that the individual's enrolled image reasonably matches the facial image submitted for comparison; or

b) When the personally identifying or biographical information would reasonably assist the officer in verifying the identity of the person.

Part D: DISSEMINATION OF FACIAL RECOGNITION INFORMATION

401 Where it will further a legitimate criminal justice function, the facial images obtained through the use of a facial recognition field identification tool may be shared with other criminal justice agency personnel.

402 No personally identifying information, including but not limited to regional mug shot facial images, obtained through the use of a facial recognition field identification tool shall be disseminated to members of the general public or news media. This prohibition is subject only to the following specific exceptions:

a) Public safety exception – Where the head law enforcement official or the elected prosecutor of a jurisdiction reasonably determines that an individual poses a threat of substantial harm to the public, facial images and relevant personally identifying information may be released to the public.

> i) Documentation of determination – A determination that the public safety exception at Section 402(a) applies must be documented in writing and retained in the same manner as a secondary dissemination log.
>
> ii) Limited release of information – The release of facial images and personally identifying information must be limited to information that could reasonably protect the public from harm.

b) Photo line-up exception – A suspect's facial images may be used in a photo line-up to further the particular investigation for which the suspect's image was requested.

c) Warrant exception – Where a warrant has been issued for a known suspect, and where the suspect's facial image has been verified by an independent witness, the suspect's facial image can be publicly disclosed for the purposes of locating the suspect or protecting the public.

d) Missing person exception – Upon its verification by an independent third-party, the facial image of an individual reported missing can be publicly disclosed to help authorities locate the missing person.

403 Dissemination of facial images obtained through the use of a facial recognition field identification tool, other than as set forth in Sections 501 and 502, is prohibited.

Part E: RETENTION OF FACIAL RECOGNITION INFORMATION

501 Retention of captured facial images.

a) Law enforcement agencies may retain facial images captured as part of their investigation records.

b) Law enforcement agencies must retain facial images captured in accordance with the review and purge provisions of the U.S. Department of Justice's rules and policies governing criminal intelligence systems at 28 C.F.R. Part 23.20(h).

502 Retention of facial recognition field identification results.

a) Law enforcement agencies may retain candidate galleries and facial images provided by facial recognition systems in response to a query via a facial recognition field identification tool where there is an evidentiary or investigative need.

b) When a law enforcement agency uses a facial recognition field identification tool for intelligence gathering purposes, candidate galleries and facial images provided by facial recognition systems must be retained in accordance with the review and purge provisions of the U.S. Department of Justice's rules and policies governing criminal intelligence systems at 28 C.F.R. Part 23.20(h).

503 Retention of audit and dissemination logs.

a) The facial recognition system hosting agency shall retain its log of all transactions made via the facial recognition field identification tool in accordance with standard audit and retention policies. Automated audit logs of facial recognition field identification tool transactions will be maintained for the same length of time as other regulated transaction logs.

b) The facial recognition system hosting agency may retain a copy of the query response, including any facial images of potential candidate matches, as part of the facial recognition field identification tool's audit logging capabilities.

Part F: DATA QUALITY

601 Operational guidelines to ensure quality of facial recognition field identification results.

a) Because it retains full control and ownership of its identification data as well as its facial recognition software, each participating facial recognition system hosting agency is ultimately responsible for the quality and accuracy of facial images and personally identifying information it makes available through a field identification tool.

b) The facial recognition system hosting agency may limit the total number of facial images provided to a requesting law enforcement officer in response to a request for facial recognition comparison.

c) The facial recognition system hosting agency may limit its response to a law enforcement officer's request for facial recognition comparison to those facial images in its database that resemble the submitted image within a certain level or degree of similarity.

d) The facial recognition system hosting agency may limit the facial images provided to a requesting law enforcement officer in response to a request for facial recognition comparison to those taken within a certain period of time.

e) The facial recognition system hosting agency may rank or otherwise sort the facial images provided to a requesting law enforcement officer in response to a request for facial recognition comparison.

602 Individual right to review or challenge facial recognition field identification information.

a) An individual has a right to access, review, or challenge facial images captured by a law enforcement agency only as permitted under the statutes and rules of the jurisdiction and provided for by agency policies.

b) An individual has no right to access, review, or challenge the comparison results or galleries of potential candidate matches generated by a facial recognition system or transmitted to a law enforcement officer via a facial recognition field identification tool.

c) An individual has no right to access, review, or challenge network-maintained transaction or audit logs of facial recognition field identification tool queries and responses.

Part G: ACCOUNTABILITY FOR FACIAL RECOGNITION INFORMATION

701 Audit logs. Queries and responses transmitted via a facial recognition field identification tool must be logged by the hosting agency. Transaction audit logs must contain the following information:

a) The identity of the agency requesting facial recognition;

b) The date and time the transaction occurred;

c) Header information, including the identity of the agency that responded to the inquiry; and

d) An assigned number and date of image capture that uniquely identifies the facial images transmitted in response to the facial recognition query or a notation that no facial images were available.

702 Secondary dissemination logs. Law enforcement agencies that disseminate facial images or personally identifying information obtained through the use of a facial recognition field identification tool shall maintain a secondary dissemination log.

a) A secondary dissemination log must contain the following information:

> i) A copy or description of the facial image record disseminated;
>
> ii) The date and time the information was disseminated;
>
> iii) The identity of the individual to whom the information was released, including their agency and contact information; and

703 Monitoring system use and conducting audits

a) The use of a facial recognition field identification tool over the ARJIS, SDLAW or Nlets network will be monitored and audited in accordance with standard policies to guard against inappropriate or unauthorized use.

b) Law enforcement agencies utilizing a facial recognition field identification tool must:

> i) Have an internal or regional policy regarding the appropriate use of the facial recognition field identification tool;
>
> ii) Certify that each officer using the facial recognition field identification tool has been trained in accordance with Section 901 of this policy; and

iii) Limit the use of the facial recognition field identification tool to only those officers who have been trained in its use.

Part H: POLICY AWARENESS AND TRAINING

801 User training. Law enforcement agencies must train each officer utilizing a facial recognition field identification tool in the following areas:

a) The proper collection of facial images for facial recognition purposes;

b) How to take high quality facial images in the field;

c) How to interpret the facial recognition comparison results obtained via a facial recognition field identification tool and not base decisions entirely upon the comparison results;

d) The appropriate use and sharing of information obtained from a facial recognition field identification tool; and

e) How facial recognition field identification tool policies will be enforced, including any penalties for committing violations of the policy provisions.

802 Policy awareness and policy updates.

a) Participating law enforcement entities will be provided access to, and acknowledge a thorough understanding of, any policies and procedures governing the use of a facial recognition field identification tool.

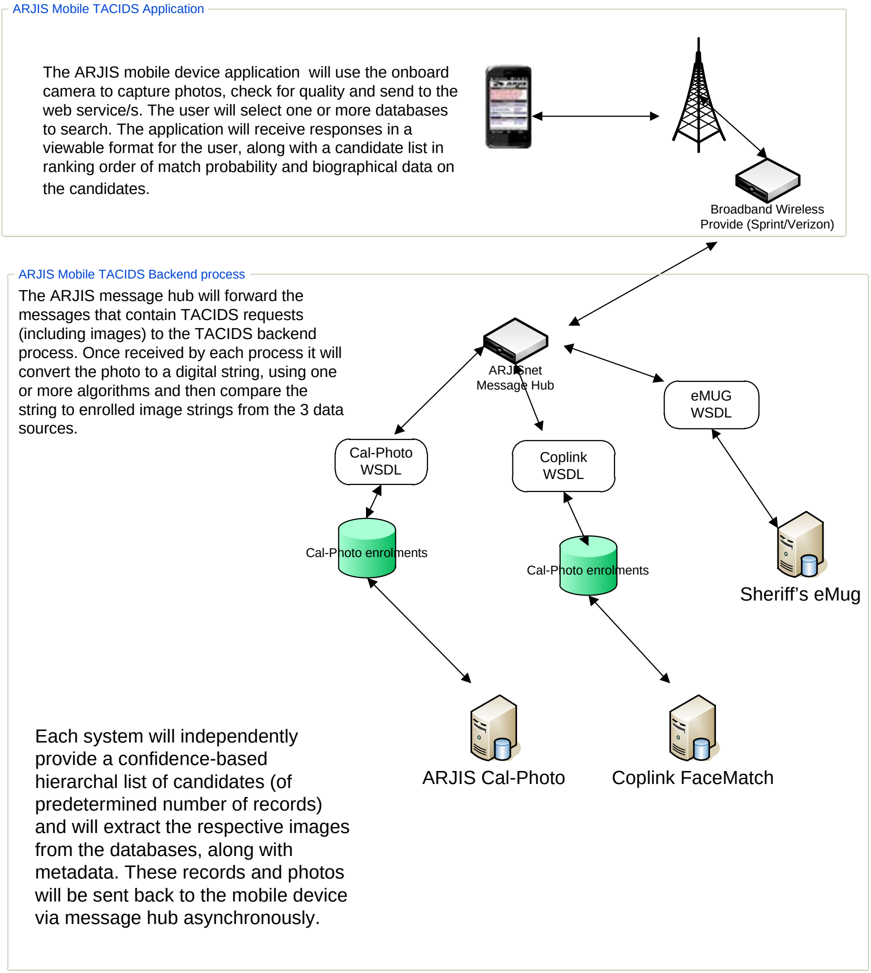
b) Participating law enforcement entities shall regularly review and update their policies and practices concerning the sharing of facial recognition field identification information to comport with any changes in relevant laws and regulations governing biometric data systems and data sharing.

Part I: SECURITY SAFEGUARDS

901 Network Connection Diagram

a) The diagram below is a sample graphical representation of the various connectivity paths that may be used to share facial images. The diagram identifies critical policy enforcement points typical within the criminal justice community that are required to share criminal justice information. The diagram does not attempt to depict all possible connectivity options. Rather, it is a general overview of the interconnection of law enforcement and criminal justice agencies that may participate in the exchange of facial images.

ARJIS Mobile Facial Recognition Application
Conceptual Technical Diagram
1/24/2012



The ARJIS mobile device application will use the onboard camera to capture photos, check for quality and send to the web service/s. The user will select one or more databases to search. The application will receive responses in a viewable format for the user, along with a candidate list in ranking order of match probability and biographical data on the candidates.

The ARJIS message hub will forward the messages that contain TACIDS requests (including images) to the TACIDS backend process. Once received by each process it will convert the photo to a digital string, using one or more algorithms and then compare the string to enrolled image strings from the 3 data sources.

Each system will independently provide a confidence-based hierarchal list of candidates (of predetermined number of records) and will extract the respective images from the databases, along with metadata. These records and photos will be sent back to the mobile device via message hub asynchronously.

902 Site Security

a) Establish an environment to protect the physical security of computer site and related infrastructure technology supporting exchange of facial Images including information system servers, networking equipment, security equipment and monitoring facilities, electronic and printed storage facilities (both online and offline) and personal computing devices. Physical security controls must provide adequate security to protect against unauthorized use.

b) Maintain a physically secure location for the storage of the facial recognition system hardware and software.

c) Access to the physically secure location shall be logged. Logging entries must include accurate date and time records capturing the asserted identity of the person granted access. Entry logs must be maintained for 1 year.

d) All visitors to physically secure areas must be accompanied by an authorized user at all times. Names of visitors must be recorded in a visitor log, to include date and time of visit, name of visitor, purpose of visit, name of accompanying authorized user, and date and time of departure. The visitor logs shall be maintained for 1 year.

e) All devices physically or logically connected to the LEA network must be protected against use or access by unauthorized persons.

903 System Integrity

a) Maintain a level of system integrity commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of facial recognition data.

b) Maintain a log of all access and dissemination of facial recognition data including record requests and responses for a period of no less than 1 year.

c) Periodically assess the inquiries of facial recognition systems made through the LEA network and subsequent information dissemination to determine accordance with applicable policies and regulations set forth in the following:

d) All dissemination of facial recognition data will be considered "Sensitive but Unclassified, For Official Use Only", bearing the label "FOR OFFICIAL USE ONLY" on any printed pages.

e) All resources including facial recognition system data intended for printing such as report output shall bear a header and/or footer with the label "FOR OFFICIAL USE ONLY". All resources including facial recognition data intended for printing such as report output shall bear a header and/or footer with the label "FOR OFFICIAL USE ONLY."

f) Other electronic resources not typically intended for printing that lack this designation will be stamped with the label "FOR OFFICIAL USE ONLY" prominently on the cover page.

904 Personnel Security

a) Maintain a level of system integrity commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of facial recognition data.

b) All personnel involved in the handling, maintenance and processing of facial recognition data must meet the requirements for personnel security.

905 System Security

a) All systems processing, handling or storing facial recognition data shall be subject to compliance with the Agency's Information Security Policy.

b) Under no circumstances may facial recognition data be stored on systems whose access is governed by policies that vary from the Agency's Information Security Policy.

c) All reasonable measures should be taken to ensure that the ability to identify and account for all activities on a facial recognition system are preserved, including but not limited to the following:

(i) Recording of successful user login and logout;

(ii) Recording of failed user login attempts;

(iii) Recording of the unique identifiers for queries and the corresponding responses with the associated request for facial images;

(iv) All IP addresses associated with the authentication and access of request and response data transferred through the ARJIS or SDLAW network.

d) Unique identification and authentication credentials will be used for all personnel accessing facial imagery. Under no circumstances will authorized personnel share their assigned authentication credentials with other authorized or unauthorized users.

e) Auditing controls will be used to identify the changes and attempted changes to system or data resources, including the identity of the user requesting the change.

f) Electronic access control mechanisms will be used on communications devices (routers, firewalls) to limit access to facial recognition systems.

(i) Access to facial recognition systems should be granted following an explicit grant policy, denying all traffic not explicitly permitted by electronic access control mechanisms.

(ii) Access attempts that are rejected should be logged identifying the source address information for the system requesting access and the requested service that was rejected.

h) Provide a system for ensuring the confidentiality of facial recognition data over public networks such as the Internet.

i) All facial recognition data transmitted across an untrusted network shall, at minimum, be encrypted using AES-128.

j) Devices responsible for encryption shall meet the requirements for FIPS 140-2.