ARAPAHOE COUNTY SHERIFF'S OFFICE

POLICY AND PROCEDURE MANUAL PUBLIC SAFETY BUREAU	EFFECTIVE 00/00/0000	REVISED 00/00/0000
TITLE FACIAL RECOGNITION	POLICY NUMBER PSB ???	

PURPOSE:

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face using biometric data-detecting algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, assist in the identification of individuals who refuse to identify themselves when required to do so by law and help in the identification of persons unable to identify themselves or deceased persons. The purpose of this policy is to provide guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a facial recognition program.

DEFINITIONS:

ACCOUNTABILITY REPORT: A report developed pursuant to C.R.S. § 24-18-302(2).

AUDIT: A review conducted by the Facial Recognition Administrator to include all use of facial recognition software/technology. The audit will include all user's activity, such as user log-ins and log-outs, each user's activity in detail, what commands were issued to the system, and what records or files were accessed.

CANDIDATE IMAGES: The possible results of a facial recognition search. When facial recognition software compares a probe image against the images contained in a repository, the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to, or most likely resemble, the probe image to warrant further analysis. A candidate image is an investigative lead ONLY and does not establish probable cause without further investigation.

DECISIONS THAT PRODUCE LEGAL EFFECTS CONCERNING INDIVIDUALS OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING INDIVIDUALS (Decisions that Produce Legal Effects): Decisions that: (a) result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health-care services, or access to basic necessities such as food and water; or (b) impact the civil rights of individuals.

ENROLL, ENROLLED, OR ENROLLING: The process by which a facial recognition service creates a facial template from one or more images of an individual and adds the facial template to a gallery that is used by the facial recognition service for recognition or persistent tracking of individuals; or the act of adding an existing facial template directly into a gallery that is used by a facial recognition service.

FACIAL RECOGNITION ADMINISTRATOR: Investigations Captain, who will be the point of contact for facial recognition service access, training, and audits.

FACIAL RECOGNITION SERVICE: Technology, including facial recognition software, that analyzes facial features to facilitate the identification, verification, or persistent tracking of individuals in still or video images. Facial recognition service does not include: (a) the analysis of facial features to grant or deny access to an electronic device; (b) a generally available consumer product, including a tablet or smartphone, that allows for the analysis of facial features in order to facilitate the user's ability to manage an address book or still or video images for personal or household use; or (c) the use of an automated or semi-automated process by a law enforcement agency for the purpose of redacting a recording for release or disclosure to protect the privacy of a subject depicted in the recording, so long as the process does not generate or result in the retention of any biometric data or surveillance information.

FACIAL RECOGNITION SOFTWARE: Third-party software that uses specific proprietary algorithms to compare human facial features from one specific picture (probe image) to many others that are stored in an image repository to determine the most likely candidates for further investigation.

FACIAL RECOGNITION USER: A member who has been approved for access and granted account access by the facial recognition administrator.

FACIAL TEMPLATE: A machine-interpretable pattern of facial features extracted from one or more images of an individual by a facial recognition service.

IDENTIFICATION: The use of a facial recognition service by an agency to determine whether an unknown individual matches any individual whose identity is known to the agency and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

IMAGE REPOSITORY: A location where a group of images of known individuals and biometric templates is stored and managed. An image repository is searched during a facial recognition search process whereby a probe image is used by a facial recognition service for comparison with the images (or features within images) contained in the image repository.

INVESTIGATIVE LEAD: Any information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

MEANINGFUL HUMAN REVIEW: Review or oversight by one or more individuals who are trained in accordance with C.R.S. § 24-18-305 and who have the authority to alter a decision under review.

ONGOING SURVEILLANCE: The continual use of a facial recognition service by an agency to track in real-time the physical movements of a specified individual through one or more public places. Ongoing surveillance does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time with the use of a facial recognition service after the individual has been recognized.

PERSISTENT TRACKING: The use of a facial recognition service by an agency to track the movements of an individual on a persistent basis without identification or verification of the individual. Tracking becomes persistent as soon as the facial template that permits the tracking is maintained for more than 48 hours after first enrolling that template or data created by the facial recognition service is linked to any other data such as the individual who has been tracked is identified or identifiable.

PROBABLE CAUSE: As defined in ADM 503.

PROBE IMAGE: Any uploaded face image used by facial recognition software for comparison with the facial images contained within a facial image repository.

REASONABLE SUSPICION: As defined in ADM 503.

RECOGNITION: The use of a facial recognition service by an agency to determine whether an unknown individual matches any individual who has been enrolled in a gallery used by the facial recognition service or a specific individual who has been enrolled in a gallery used by the facial recognition service.

RFI: Request for information.

RFI LOG: A credentialed log for the purposes of internal and external facial recognition data sharing and requests that documents the name of the agency/requestor, name of the person completing the request, date and time the request was completed, case number, and reason for the request. The RFI log may be a part of the software auditing process.

VERIFICATION: The use of a facial recognition service by an agency to determine whether an individual is a specific individual whose identity is known to the agency and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

< >: Numbers in brackets are Accreditation references.

POLICY:

Facial recognition services provide many opportunities for the enhancement of productivity, increased crime solvability, investigative effectiveness, and increased safety for both citizens and members. It is the policy of the Sheriff's Office to utilize facial recognition services to develop leads of unknown subjects for law enforcement investigations in a manner that safeguards against potential abuses.

This policy ensures that the use of facial recognition services by the Sheriff's Office and its members is consistent with authorized purposes while not violating anyone's privacy, civil rights, and civil liberties and complies with the statutory requirements described in C.R.S. §§ 24-18-301 thru 309. Further, this policy delineates the way requests for facial recognition information are received, processed, documented, and acted upon.

This policy assists the Sheriff's Office and its members in:

1. Increasing public safety and improving state, local, tribal, territorial, and national security.

2. Minimizing the threat and risk of injury to specific individuals.

3. Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.

4. Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.

5. Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.

6. Minimizing the threat and risk of damage to real or personal property.

7. Fostering trust in the government by strengthening transparency, oversight, and accountability.

8. Making the most effective use of public resources allocated to public safety entities.

PROCEDURE:

Section A

General Requirements for Use of a Facial Recognition Service

1. The use of any facial recognition service, and access to any data generated by a facial recognition service, requires a legitimate law enforcement purpose. No member may use or authorize the use of or access to any facial recognition service or data for any other reason.

2. Probe images are specifically limited to those obtained lawfully. Any uploaded Probe Image shall be that of an unknown person for the sole purpose of obtaining a possible identification and investigative lead in an official law enforcement investigation based on reasonable suspicion. The only exception to this requirement is if the uploading of a known Probe Image may result in additional investigative leads, such as the identification of potential aliases, alias social media accounts, etc. Members shall not substantively manipulate an image for use in a facial recognition service in a manner not consistent with the facial recognition service provider's intended use and training.

3. Facial Recognition is an investigative tool and any law enforcement action taken based on a submission to any other facial recognition system shall be based on the agency's own identity determination and not solely the results of a facial recognition search. The result of a facial recognition search shall only be considered as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT OR PROBABLE CAUSE FOR ARREST**. Any possible connection or involvement of any subject to an investigation must be determined through further investigation and investigative resources.
4. The Sheriff's Office may share facial recognition data or requests only with an authorized law enforcement agency. External data sharing or requests shall be at the approval of the facial recognition administrator or designee documented via the RFI process. Any data sharing shall comply with this facial recognition policy.

Section B

Facial Recognition Service Selection and Program Management

1. Prior to procuring or implementing any facial recognition service, the Sheriff's Office shall require a provider whose facial recognition service is under consideration to disclose any complaints or reports of bias regarding the provider's facial recognition service.

2. The Sheriff's Office shall, to the extent reasonably practicable as determined by the Sheriff or designee, use facial recognition service providers who participate in the face recognition

vendor test ongoing project of the National Institute of Standards and Technology (NIST Project). If the Sheriff's Office seeks to procure or implement a facial recognition service from a provider who is not participating in the NIST Project and the facial recognition service will be deployed in a context in which it will be used to make Decisions that Produce Legal Effects, the Sheriff's Office will test the facial recognition service in operational conditions before it is deployed.

a. The Sheriff's Office will follow all guidance provided by the developer of the facial recognition service to ensure the best quality results.

b. If the Sheriff's Office deploys a facial recognition service provider that is not participating in the NIST Project, the Sheriff's Office will require the provider to supply an application programming interface, or other technical capabilities, chosen by the provider, to allow for legitimate, independent and reasonable tests of the facial recognition service for accuracy and to identify unfair performance differences across distinct subpopulations, including those that are visually detectable characteristics (i.e., race, skin tone, ethnicity, gender, age, disability status). The provider will not, however, be required to provide proprietary material or provide an interface or technical capability in a way that would increase the risk of cyber-attacks.

c. If the results of independent testing identify material unfair performance differences across subpopulations, the Sheriff's Office will require the provider to develop and implement a plan to mitigate the identified performance differences within 90 days after receipt of the test results.

3. All technology associated with a facial recognition service, including all related hardware and software support, shall be bound by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) security policy. Information contained within or generated through the use of an FRS is considered highly restricted personal information, which may only be transmitted, accessed, used, and disseminated in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent federal CJIS Security policy.

4. The facial recognition administrator will be responsible for deploying, managing, and controlling access to the facial recognition program and for ensuring that access, management, and use of the technology is consistent with Sheriff's Office policy and with statutory requirements in C.R.S. §§ 24-18-301 thru 24-18-309.

5. Any authorization for the Sheriff's Office to develop, procure, use, or continue to use a facial recognition service shall comply with all applicable requirements of C.R.S. § 24-19-302.

Section C

Access, Security, Auditing, and Retention

1. Access to facial recognition search results will be provided only to individuals within the Sheriff's Office who are authorized to have access and have completed applicable training. Authorized access to any facial recognition service will be granted only to personnel whose

positions and job duties (Investigations, Intelligence, and Analysts) require such access and to the IT personnel responsible for system administration and maintenance of the facial recognition service.

2. The facial recognition administrator shall grant and audit all user access, following the required account approval.

3. All authorized facial recognition users shall be required to have individual access for use of the facial recognition software/technology.

4. Authorized facial recognition users will analyze, review, and evaluate the quality and suitability of probe images, including factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

5. Original probe images shall not be altered, changed, or modified to protect the integrity of the image. Any enhancements made to a probe image will be made as a separate copy, saved as a separate image, documented to indicate what enhancements were made, including the date and time of change and the name of the person who made the change, and disclosed in discovery if an arrest is made.

6. Resulting images, if any, shall be manually compared with the probe image by the authorized user conducting the comparison. In accordance with training, any candidate image that is incompatible with a probe image shall be removed from the candidate image list.

7. Any upload of a probe image, query, or request shall include the name of the agency/requestor, the name of the person completing the request, the date and time the request was completed, the case number, and the reason for the request. This information will be logged, tracked, and available for auditing and review.

8. The Sheriff's Office and all authorized facial recognition users shall comply with all requirements stipulated in any contract or agreement related to any authorized facial recognition enrollment databases unless such requirement is contrary to applicable law. Any questions or clarification regarding the permissible use of any facial recognition service should be directed to the facial recognition administrator, the Legal Advisor's office, or the vendor.
9. Data retrieved by the Sheriff's Office, including images, from facial recognition searches will be maintained and retained in accordance with the applicable Sheriff's Office evidence policies in the case.

Section D

Secondary Peer Review

1. Per C.R.S. § 24-18-303, "[a]n agency using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals must ensure that those decisions are subject to meaningful human review."

2. Prior to completing the facial recognition investigation, a peer review process should be implemented. The goal of this review process is to provide an additional level of consistency and control concerning the application of standardized training practices.

3. A secondary (peer) review should consist of a separate facial recognition-trained member reviewing the findings of the initiating investigator. This can be a review of the facial recognition report alone or a complete secondary search of the probe imagery within the facial recognition service. During the secondary review, the reviewing peer investigator should document in the case report either a concurrence with the provided results or a rejection of the provided results. The secondary reviewer should be able to provide specific and articulable reasons for agreeing or not agreeing with the provided results.

4. The outcome of the secondary review should be documented in a supplemental report and subsequently reviewed by the investigations supervisor. The cause for any lack of concurrence with results should be analyzed by the investigations supervisor and the circumstances of the disagreement should be reviewed with the initial investigating member. The investigations supervisor will have ultimate decision-making authority on the progression of the case after considering all the available identifying factors. The number and nature of facial recognition investigations with disagreements over the results should be monitored over time.

Section E

Authorized Use of Facial Recognition Services and Data

1. All use of a facial recognition service and any resulting data shall be for official law enforcement use only and considered law enforcement sensitive information. The following are authorized uses of facial recognition information:

    a. A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.

    b. An active or ongoing criminal investigation.

    c. To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.

    d. To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (such as an incapacitated, deceased, or otherwise at-risk person).

    e. To investigate and/or corroborate tips and leads.

    f. To assist in the identification of potential witnesses and/or victims of violent crime.

    g. To support law enforcement in critical incident responses.

2. The results of a facial recognition service shall not be used as the sole basis to establish probable cause in a criminal investigation. The results of a facial recognition service may be

used in conjunction with other information and evidence lawfully obtained by a member to establish probable cause in a criminal investigation.

3. Facial recognition information will be included in the case file and timely disclosed as part of the criminal discovery process.

Section F

Unauthorized Use of Facial Recognition Services

1. The use of a facial recognition service for the sole purpose of intelligence gathering is prohibited. Additionally, the technology will not be used solely for identifying anyone exercising their constitutionally protected rights. The use of facial recognition services in conjunction with public safety cameras outside the above guidelines is prohibited.

2. The Sheriff's Office strictly prohibits access to and use of any facial recognition service, including dissemination of facial recognition search results, for the following purposes:

    a. Non-law enforcement purposes, including but not limited to personal purposes.

    b. Any purpose that violates the U.S. Constitution or laws of the United States, including protections of the First, Fourth, and Fourteenth Amendments, or that violates the Colorado Constitution or the laws of the State of Colorado.

    c. Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by or secured by the U.S. Constitution or the Colorado Constitution or any other constitutionally protected right or attribute.

    d. Harassing and/or intimidating an individual or group.

    e. Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. Facial recognition services shall not be used to obtain similar images to a subject for the purpose of using them as filler images in a photographic lineup.

4. Per C.R.S. § 24-18-307, members shall not use a facial recognition service to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless:

    a. The Sheriff's Office obtains a warrant authorizing such use;

    b. Such use is necessary to develop leads in an investigation;

    c. The Sheriff's Office has established probable cause for such use; or

    d. The Sheriff's Office obtains a court order authorizing the use of the service for the sole purpose of locating or identifying a missing person or identifying a deceased person.

5. The Sheriff's Office shall not apply a facial recognition service to any individual based on the individual's religious, political, or social views or activities; participation in a particular

noncriminal organization or lawful event; or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender expression, gender identity, sexual orientation, or other characteristic protected by law.

Section G

Training

1. Training will be provided to all authorized users of any facial recognition service. This training will be arranged and documented by the facial recognition administrator, or designee, and account access will not be created or provided until training has been completed. The facial recognition administrator shall provide copies of all training documentation to the training section for archive purposes.

2. Training will cover both the use of facial recognition services and a specific review and acknowledgment of all elements of this policy.

3. Per C.R.S. § 24-18-305, the training will, at a minimum, include:

    a. The capabilities and limitations of the facial recognition service;

    b. Procedures to interpret and act on the output of the facial recognition service; and

    c. To the extent applicable to the deployment context, the meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals.

4. The use of each authorized enrollment database will include specific training that includes the following:

    a. An authorized user accesses their individual account,

    b. The authorized user shall enter the required information to support the authorized use of facial recognition satisfying an official law enforcement purpose,

    c. A lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system,

    d. The software automatically compares the probe image to candidate images within the repository,

    e. Results of the comparison are returned and provide a potential investigative lead.

5. Updated training shall be identified with any policy revisions or updates in facial recognition software or applicable legal or statutory updates.

Section H

Accountability

1. The facial recognition administrator, or designee, shall ensure and evaluate the compliance of users with the face recognition service requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record of the audits will be maintained by the facial recognition administrator, or designee, pursuant to the Sheriff's Office's retention policy. Audits may be completed by an independent third party or the facial recognition administrator or designee.

2. The facial recognition administrator, or designee, will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition service and the results of the audit review, as applicable.

3. The facial recognition administrator, or designee, will review and update any final accountability report at least every two years and shall submit the updated final accountability report to the Board of County Commissioners. A courtesy copy of the updated final accountability report will be provided to the City Council for the City of Centennial.

4. In January of each year, the facial recognition administrator, or designee, will determine if the Sheriff's Office applied for any warrant, or an extension of a warrant, authorizing the use of a facial recognition service to conduct ongoing surveillance or persistent tracking, as described in Section F subpart 4, during the prior calendar year. If the Sheriff's Office applied for any such warrant or extension of a warrant, the facial recognition administrator, or designee, will prepare a report summarizing the gender, race, ethnicity, age, and location of each individual named in any such warrant applications and provide the report to the Board of County Commissioners no later than January 31. A courtesy copy of any reports involving the City of Centennial will also be provided to the City Council no later than January 31, when applicable.