ARAPAHOE COUNTY SHERIFF’S OFFICE (ACSO)
ACCOUNTABILITY REPORT FOR FACIAL RECOGNITION SERVICE

Facial Recognition Service (FRS) Name: Lumen
Vendor: Lexis-Nexis, using an algorithm supplied by Rank One Computing Corporation
Version: ROC SDK version 2.2.1

Description of general capabilities and limitations: Lumen’s facial recognition service may be used as an investigative aid to provide possible leads to help identify potential suspects by comparing a single probe image of an unknown suspect to a collection of candidate facial images provided by the Colorado Information Sharing Consortium (CISC). Lumen provides multiple results, each with a given accuracy score generated by the ROC SDK’s facial recognition algorithms. The accuracy score is designed to indicate the likelihood of the probe image matching a given result. The core facial recognition algorithms depend primarily on the image quality of the probe image and candidate images and on the robustness of the algorithm development process. The primary factors of image quality are capture conditions, including camera sensor quality, field of focus, glare, blur, low light, high contrast, variable lighting, height of the camera, pose of the subject and occlusions between the camera and the subject face. Algorithms are developed by processing training data through machine learning architectures and iteratively testing accuracy on data that represents real-world conditions. Accuracy of a match score may be impacted by poor image quality of the probe image and/or candidate image or to the extent that operational data is fundamentally dissimilar to training data and/or testing data selected in the research and development process.

I. DATA INPUT AND GENERATION

Type of data inputs used: The Lumen facial recognition service accepts images as data inputs.

How the data is generated, collected and processed: Candidate facial image data is collected by the Colorado Information Sharing Consortium (CISC) from member agencies who elect to share images. CISC contributing member agencies provide booking photos, and those facial images from CISC are processed into Lumen’s facial recognition service. The probe image, which will be compared against the candidate facial images, is collected in the course of an investigation and typically consist of stills from surveillance footage, body worn camera footage or other personal images and/or video footage.

Type of data reasonably likely to be generated: The ROC SDK generates a template of each facial image, which is a mathematical model of the unique subject and which may be compared to templates generated from other images to produce a match score. For each facial image, the ROC SDK also generates metadata including pitch, yaw, image quality estimations and facial analytics like age, gender, geographic origin, emotion, facial hair, glasses and mask estimations.

II. DESCRIPTION OF PURPOSE AND PROPOSED USE

Proposed use / purpose for use of the FRS: When provided a probe image to search against a collection of candidate images, Lumen returns multiple results, sorted by the highest match score generated by the ROC SDK's facial recognition algorithms. Once Lumen provides a list of results, a human investigator must review the results before making any determination of a possible match. A possible match determination may be used as an investigative lead that is treated in a similar manner as an anonymous tip. In particular, the investigative lead does not supply adequate probable cause to make an arrest without additional evidence. The intended benefit of using the Lumen facial recognition service is to generate investigative leads for further investigation with the hope of solving crimes that would otherwise go unsolved.

Decision(s) to be made or supported by FRS: Match determinations may be used to provide investigators with possible leads to develop independent probable cause to solve criminal cases and support arrests/case filings. Match determinations will be subject to meaningful human review in accordance with ACSO policies and will not be the sole basis for making decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals. In particular, match determinations will not serve as the sole basis to establish probable cause in a criminal investigation.

Intended benefits of use, including any data or research demonstrating such benefits: Lumen is intended to benefit ACSO by serving as an investigative aid to provide possible leads to help identify potential suspects. In comparable use by the New York City Police Department (NYPD) since 2011, the NYPD has successfully used facial recognition to identify suspects whose images were captured by cameras at robberies, burglaries, assaults, shootings, and other crimes. In 2019 alone, the Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, including possible matches in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies with no known instance in which a person was falsely arrested on the basis of a facial recognition match. See https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page.

III. USE AND DATA MANAGEMENT POLICY

Use and data management policy: The Sheriff's Office is implementing facial recognition policy governing its use of facial recognition services which provides as follows:

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. Italicized content is added for public reference.

DEFINITIONS:

ACCOUNTABILITY REPORT: A report developed pursuant to C.R.S. § 24-18-302(2). [*C.R.S. § 24-18-301(1)*]

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, and dispute data, such as the frequency of occurrence, members involved and suspect demographics.

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. [*C.R.S. § 24-18-301(3)*]

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. [*C.R.S. § 24-18-301(4)*]

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. [*C.R.S. § 24-18-301(5)*]

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. [*C.R.S. § 24-18-301(6)*]

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. [*C.R.S. § 24-18-301(7)*]

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. [*C.R.S. § 24-18-301(9)*]

ONGOING SURVEILLANCE: (a) 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. (b) 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. [*C.R.S. § 24-18-301(11)*]

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: (a) the facial template that permits the tracking is maintained for more than 48 hours after first enrolling that template; or (b) 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. [*C.R.S. § 24-18-301(12)*]

PROBABLE CAUSE: As defined in ADM 503.

> *From ADM 503: A set of articulable facts which would lead a neutral independent magistrate to believe, under the totality of the circumstances, a crime occurred; or that seizable evidence will be found.*

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.

> *From ADM 503: Particularized and objective basis supported by articulable facts when viewed within the totality of the circumstances, lead a deputy to reasonably believe that criminal activity has been, is being, or is about to be committed by a person.*

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. [*C.R.S. § 24-18-301(13)*]

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.

SUBSTANTIVELY MANIPULATE AN IMAGE or SUBSTANTIVE MANIPULATION OF AN IMAGE: Altering the content of a photographic image by adding, rearranging, reversing, distorting or removing people and/or objects within the frame. Substantively Manipulating an Image does not include modifications to the size, zooming in or out, and/or cropping some portion of the original photographic image.

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. [*C.R.S. § 24-18-301(15)*]

< >: 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:

<u>Section A</u>

Section A of the Policy is directed to:

C.R.S. § 24-18-302(2)(d)(I), addressing how, when, and by whom the facial recognition service will used and made available to, factors determining the same and other relevant information including the circumstances in which it will be operated;

C.R.S. § 24-18-302(2)(d)(III), addressing any measure to minimize inadvertent collection of additional data;

C.R.S. § 24-18-302(2)(d)(V), addressing processes required for use;

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, as set forth in Section E subpart 1. 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 facial recognition system, internal or external, 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

Section B of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(III), addressing any measure to minimize inadvertent collection of additional data;

C.R.S. § 24-18-302(2)(d)(IV), addressing data integrity and retention policies, including maintenance, updating and retention of records; and

C.R.S. § 24-18-302(2)(d)(VIII), addressing other policies governing use

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, and approved by the Sheriff's Office and the Arapahoe

County Information Technology Department, 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. If the provider cannot mitigate the identified performance differences within 90 days after receipt of the test results, the Sheriff's Office will not deploy the facial recognition service that failed to mitigate the identified performance deficiencies.

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. § 24-18-302.
6. Any procurement of a facial recognition service shall comply with applicable Arapahoe County Finance Department and Information Technology Department procurement, cybersecurity, and other applicable requirements and policies.

<u>Section C</u>

Section C of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(I), addressing how, when, and by whom the facial recognition service will used and made available to, factors determining the same and other relevant information including the circumstances in which it will be operated;

C.R.S. § 24-18-302(2)(d)(IV), addressing data integrity and retention policies, including maintenance, updating and retention of records;

C.R.S. § 24-18-302(2)(d)(V), addressing processes required for use; and

C.R.S. § 24-18-302(2)(d)(VIII), addressing other policies governing use

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 substantive manipulation of an image consistent made to a probe image as permitted in Section A subpart 2 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.

<u>Section D</u>

Section D of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(I), addressing how, when, and by whom the facial recognition service will used and made available to, factors determining the same and other relevant information including the circumstances in which it will be operated;

C.R.S. § 24-18-302(2)(d)(III), addressing any measure to minimize inadvertent collection of additional data;

C.R.S. § 24-18-302(2)(d)(IV), addressing data integrity and retention policies, including maintenance, updating and retention of records; and

C.R.S. § 24-18-302(2)(d)(V), addressing processes required for use

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 and the secondary review 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 shall be reported to the facial recognition administrator and monitored over time.

Section E

Section E of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(I), addressing how, when, and by whom the facial recognition service will used and made available to, factors determining the same and other relevant information including the circumstances in which it will be operated;

C.R.S. § 24-18-302(2)(d)(III), addressing any measure to minimize inadvertent collection of additional data; and

C.R.S. § 24-18-302(2)(d)(V), addressing processes required for use

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

Section F of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(I), addressing how, when, and by whom the facial recognition service will used and made available to, factors determining the same and other relevant information including the circumstances in which it will be operated;

C.R.S. § 24-18-302(2)(d)(III), addressing any measure to minimize inadvertent collection of additional data; and

C.R.S. § 24-18-302(2)(d)(V), addressing processes required for use

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

Section G of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(V), addressing processes required prior to use;

C.R.S. § 24-18-302(2)(d)(VI), addressing applicable data security measures; and

C.R.S. § 24-18-302(2)(d)(VII), addressing the Sheriff's Office's training procedures

Training

1. Training will be provided to all authorized users of any facial recognition service on an annual basis. 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

Section H of the Policy is primarily directed to:

C.R.S. § 24-18-302(2)(d)(IV), addressing data integrity and retention policies, including maintenance, updating and retention of records; and

C.R.S. § 24-18-302(2)(d)(VIII), addressing other policies governing use

1. The facial recognition administrator, or designee, shall ensure and evaluate the compliance of users with the facial 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 and underlying data 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 facial 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 all jurisdictions for which the Sheriff's Office is contracted to provide law enforcement services.

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 will also be provided to all jurisdictions for which the Sheriff's Office is contracted to provide law enforcement services no later than January 31, when applicable.

The Sheriff's Office's Policy does not provide for a third party to operate or use a facial recognition service on its behalf and therefore does address those circumstances under C.R.S. § 24-18-302(2)(d)(II).

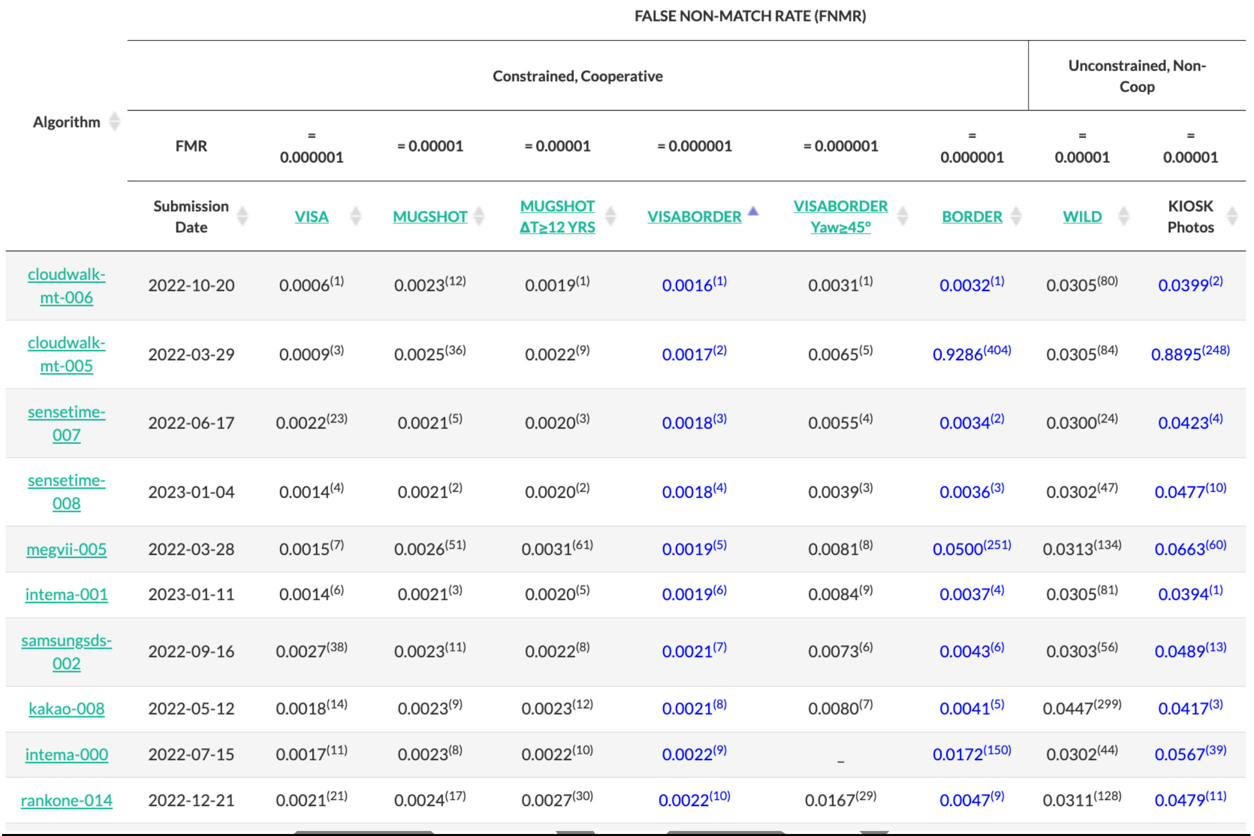
IV. TESTING INFORMATION

Description of operational testing performed on FRS: Rank One Computing submits the ROC SDK for testing in the following series of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) Ongoing:
1:1 Verification (https://pages.nist.gov/frvt/html/frvt11.html),
1:N Identification (https://pages.nist.gov/frvt/html/frvt1N.html),
Quality Assessment (https://pages.nist.gov/frvt/html/frvt_quality.html),
Demographic Effects (https://pages.nist.gov/frvt/html/frvt_demographics.html),
Paperless Travel (https://pages.nist.gov/frvt/html/frvt_paperless_travel.html) and
Presentation Attack Detection (https://pages.nist.gov/frvt/html/frvt_pad.html).

Description of any additional ACSO testing performed: ACSO has not yet implemented the Lumen facial recognition service.

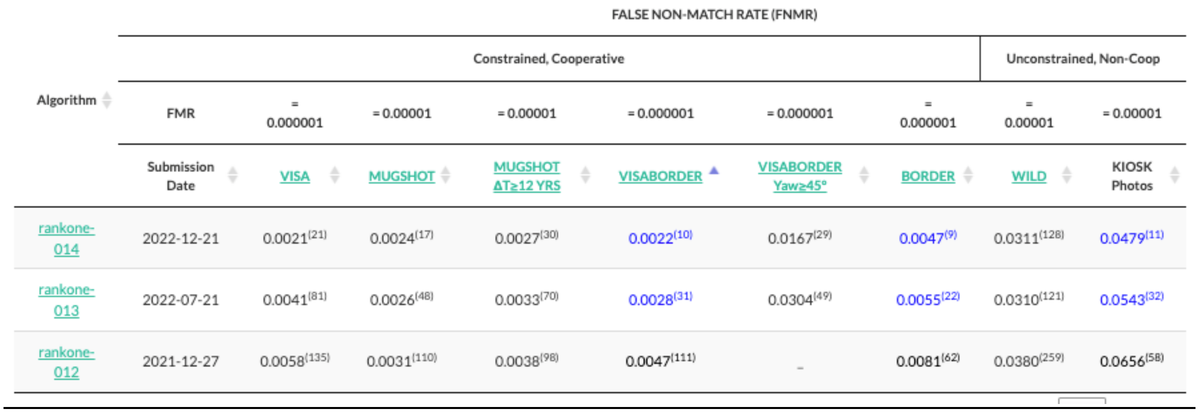
V. INFORMATION REGARDING FALSE MATCHES

Rate of false matches: On the NIST 1:1 leaderboard (available at https://pages.nist.gov/frvt/html/frvt11.html), the latest version of the ROC SDK, version 2.4, is currently listed as the #10 algorithm out of 478 total entries (top 2%), placing Rank One Computing in the top 7 among vendors overall. Three of the vendors producing algorithms ahead of Rank One are produced by Chinese companies who are prohibited from doing business in the United States due to human rights violations (CloudWalk, SenseTime and Megvii):



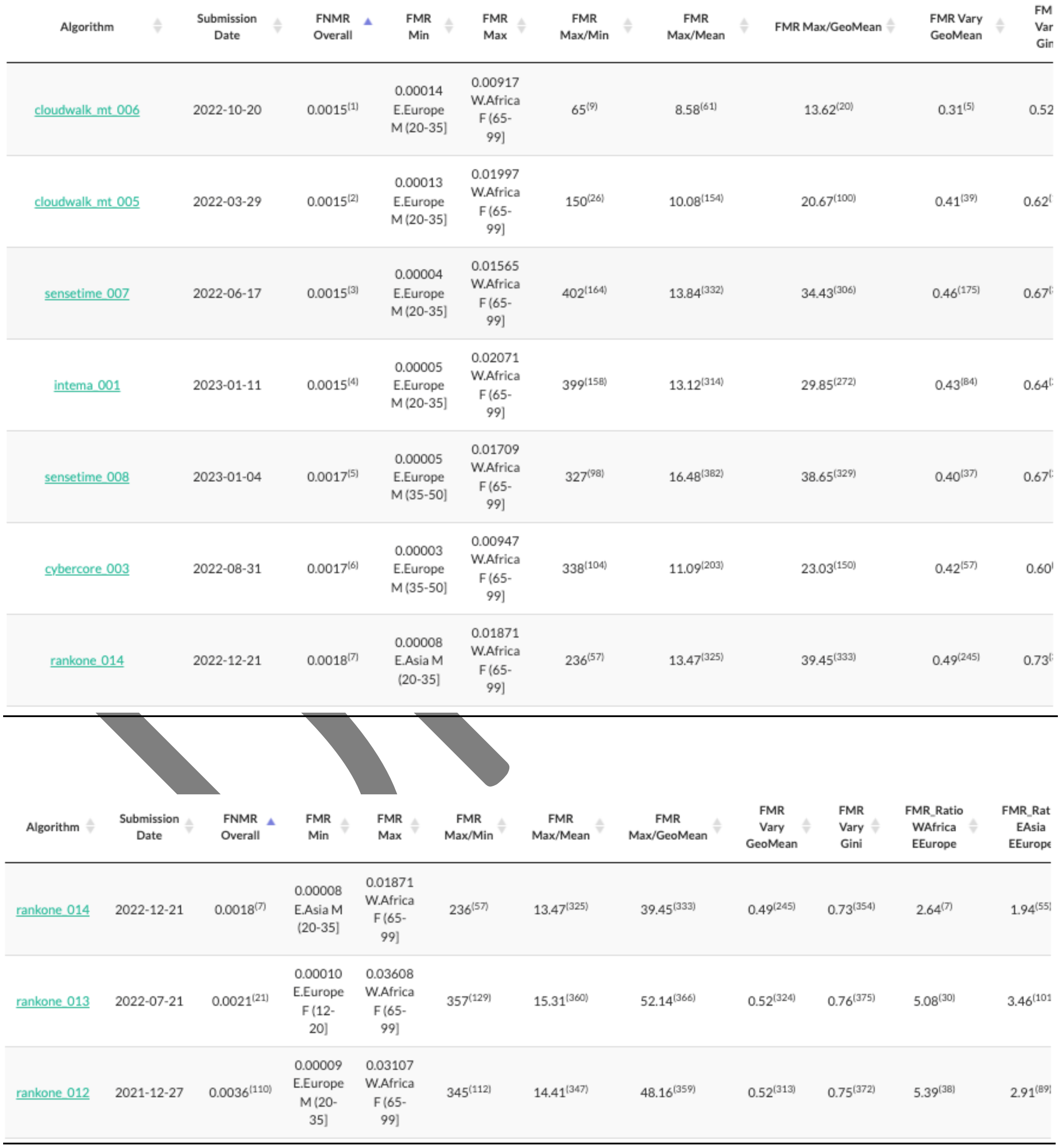
Algorithm	FALSE NON-MATCH RATE (FNMR)								
	Constrained, Cooperative							Unconstrained, Non-Coop	
	FMR	= 0.000001	= 0.00001	= 0.00001	= 0.000001	= 0.000001	= 0.000001	= 0.00001	= 0.00001
	Submission Date	VISA	MUGSHOT	MUGSHOT ΔT≥12 YRS	VISABORDER	VISABORDER Yaw≥45°	BORDER	WILD	KIOSK Photos
cloudwalk-mt-006	2022-10-20	0.0006$^{(1)}$	0.0023$^{(12)}$	0.0019$^{(1)}$	0.0016$^{(1)}$	0.0031$^{(1)}$	0.0032$^{(1)}$	0.0305$^{(80)}$	0.0399$^{(2)}$
cloudwalk-mt-005	2022-03-29	0.0009$^{(3)}$	0.0025$^{(36)}$	0.0022$^{(9)}$	0.0017$^{(2)}$	0.0065$^{(5)}$	0.9286$^{(404)}$	0.0305$^{(84)}$	0.8895$^{(248)}$
sensetime-007	2022-06-17	0.0022$^{(23)}$	0.0021$^{(5)}$	0.0020$^{(3)}$	0.0018$^{(3)}$	0.0055$^{(4)}$	0.0034$^{(2)}$	0.0300$^{(24)}$	0.0423$^{(4)}$
sensetime-008	2023-01-04	0.0014$^{(4)}$	0.0021$^{(2)}$	0.0020$^{(2)}$	0.0018$^{(4)}$	0.0039$^{(3)}$	0.0036$^{(3)}$	0.0302$^{(47)}$	0.0477$^{(10)}$
megvii-005	2022-03-28	0.0015$^{(7)}$	0.0026$^{(51)}$	0.0031$^{(61)}$	0.0019$^{(5)}$	0.0081$^{(8)}$	0.0500$^{(251)}$	0.0313$^{(134)}$	0.0663$^{(60)}$
intema-001	2023-01-11	0.0014$^{(6)}$	0.0021$^{(3)}$	0.0020$^{(5)}$	0.0019$^{(6)}$	0.0084$^{(9)}$	0.0037$^{(4)}$	0.0305$^{(81)}$	0.0394$^{(1)}$
samsungsds-002	2022-09-16	0.0027$^{(38)}$	0.0023$^{(11)}$	0.0022$^{(8)}$	0.0021$^{(7)}$	0.0073$^{(6)}$	0.0043$^{(6)}$	0.0303$^{(56)}$	0.0489$^{(13)}$
kakao-008	2022-05-12	0.0018$^{(14)}$	0.0023$^{(9)}$	0.0023$^{(12)}$	0.0021$^{(8)}$	0.0080$^{(7)}$	0.0041$^{(5)}$	0.0447$^{(299)}$	0.0417$^{(3)}$
intema-000	2022-07-15	0.0017$^{(11)}$	0.0023$^{(8)}$	0.0022$^{(10)}$	0.0022$^{(9)}$	_	0.0172$^{(150)}$	0.0302$^{(44)}$	0.0567$^{(39)}$
rankone-014	2022-12-21	0.0021$^{(21)}$	0.0024$^{(17)}$	0.0027$^{(30)}$	0.0022$^{(10)}$	0.0167$^{(29)}$	0.0047$^{(9)}$	0.0311$^{(128)}$	0.0479$^{(11)}$

Results also continue to be available for the earlier submitted versions ROC SDK v2.2, listed as rankone-013 and ROC SDK v2.0, listed as rankone-012:



Algorithm	FALSE NON-MATCH RATE (FNMR)								
	Constrained, Cooperative							Unconstrained, Non-Coop	
	FMR	= 0.000001	= 0.00001	= 0.00001	= 0.000001	= 0.000001	= 0.000001	= 0.00001	= 0.00001
	Submission Date	VISA	MUGSHOT	MUGSHOT ΔT≥12 YRS	VISABORDER	VISABORDER Yaw≥45°	BORDER	WILD	KIOSK Photos
rankone-014	2022-12-21	0.0021$^{(21)}$	0.0024$^{(17)}$	0.0027$^{(30)}$	0.0022$^{(10)}$	0.0167$^{(29)}$	0.0047$^{(9)}$	0.0311$^{(128)}$	0.0479$^{(11)}$
rankone-013	2022-07-21	0.0041$^{(81)}$	0.0026$^{(48)}$	0.0033$^{(70)}$	0.0028$^{(31)}$	0.0304$^{(49)}$	0.0055$^{(22)}$	0.0310$^{(121)}$	0.0543$^{(32)}$
rankone-012	2021-12-27	0.0058$^{(135)}$	0.0031$^{(110)}$	0.0038$^{(98)}$	0.0047$^{(111)}$	_	0.0081$^{(62)}$	0.0380$^{(259)}$	0.0656$^{(58)}$

For the ROC SDK v2.2, listed as rankone-013, the overall false match rates (FMR) range from 0.001% (1 in 100,000) to 0.0001% (1 in 1,000,000) with the equivalent false non-match rates (FNMR) shown above, ranging from 0.26% to 5.43%. The direct impact of an erroneously high match score from the ROC SDK is that a candidate would rank higher on the list of results returned by Lumen for human investigator review. The human investigator would then apply his or her skills, training and experience in facial examination to closely review the unique facial characteristics of each of the candidates on the list. The human investigator may select one of the candidates from the list of results and make a possible match determination on the basis of similarity of facial characteristics between the candidate and suspect image, or instead may determine that none of the candidates from the list of results are a possible match. If the false match eluded both the ROC SDK and the human investigator, it could become an investigative lead, which may trigger additional investigation into the relevant candidate.



Algorithm	Submission Date	FNMR Overall	FMR Min	FMR Max	FMR Max/Min	FMR Max/Mean	FMR Max/GeoMean	FMR Vary GeoMean	FM Var Gin
cloudwalk_mt_006	2022-10-20	$0.0015^{(1)}$	0.00014 E.Europe M (20-35]	0.00917 W.Africa F (65-99]	$65^{(9)}$	$8.58^{(61)}$	$13.62^{(20)}$	$0.31^{(5)}$	0.52
cloudwalk_mt_005	2022-03-29	$0.0015^{(2)}$	0.00013 E.Europe M (20-35]	0.01997 W.Africa F (65-99]	$150^{(26)}$	$10.08^{(154)}$	$20.67^{(100)}$	$0.41^{(39)}$	0.62
sensetime_007	2022-06-17	$0.0015^{(3)}$	0.00004 E.Europe M (20-35]	0.01565 W.Africa F (65-99]	$402^{(164)}$	$13.84^{(332)}$	$34.43^{(306)}$	$0.46^{(175)}$	0.67
intema_001	2023-01-11	$0.0015^{(4)}$	0.00005 E.Europe M (20-35]	0.02071 W.Africa F (65-99]	$399^{(158)}$	$13.12^{(314)}$	$29.85^{(272)}$	$0.43^{(84)}$	0.64
sensetime_008	2023-01-04	$0.0017^{(5)}$	0.00005 E.Europe M (35-50]	0.01709 W.Africa F (65-99]	$327^{(98)}$	$16.48^{(382)}$	$38.65^{(329)}$	$0.40^{(37)}$	0.67
cybercore_003	2022-08-31	$0.0017^{(6)}$	0.00003 E.Europe M (35-50]	0.00947 W.Africa F (65-99]	$338^{(104)}$	$11.09^{(203)}$	$23.03^{(150)}$	$0.42^{(57)}$	0.60
rankone_014	2022-12-21	$0.0018^{(7)}$	0.00008 E.Asia M (20-35]	0.01871 W.Africa F (65-99]	$236^{(57)}$	$13.47^{(325)}$	$39.45^{(333)}$	$0.49^{(245)}$	0.73

Algorithm	Submission Date	FNMR Overall	FMR Min	FMR Max	FMR Max/Min	FMR Max/Mean	FMR Max/GeoMean	FMR Vary GeoMean	FMR Vary Gini	FMR_Ratio WAfrica EEurope	FMR_Rat EAsia EEurope
rankone_014	2022-12-21	$0.0018^{(7)}$	0.00008 E.Asia M (20-35]	0.01871 W.Africa F (65-99]	$236^{(57)}$	$13.47^{(325)}$	$39.45^{(333)}$	$0.49^{(245)}$	$0.73^{(354)}$	$2.64^{(7)}$	$1.94^{(55)}$
rankone_013	2022-07-21	$0.0021^{(21)}$	0.00010 E.Europe F (12-20]	0.03608 W.Africa F (65-99]	$357^{(129)}$	$15.31^{(360)}$	$52.14^{(366)}$	$0.52^{(324)}$	$0.76^{(375)}$	$5.08^{(30)}$	$3.46^{(101}$
rankone_012	2021-12-27	$0.0036^{(110)}$	0.00009 E.Europe M (20-35]	0.03107 W.Africa F (65-99]	$345^{(112)}$	$14.41^{(347)}$	$48.16^{(359)}$	$0.52^{(313)}$	$0.75^{(372)}$	$5.39^{(38)}$	$2.91^{(89)}$

Potential impacts on protected subpopulations: In the NIST Demographic Effects series (available here: https://pages.nist.gov/frvt/html/frvt_demographics.html), the ROC SDK shows less than a 4% FMR, with less than a 0.2% FNMR across all 70 sub-populations of the NIST test data, with the lowest scoring demographic being West African females aged 65-99 years old. The potential impact of a false match, including on protected subpopulations, is mitigated by the human investigator review requirement and the requirement to develop additional evidence prior to making an arrest as well as the prohibition on relying solely on match determinations to establish probable cause for an arrest.

ACSO procedures for addressing error rates in excess of one percent (1%): ACSO's policy provides for substantial secondary human review of match results as well as additional review by an investigations supervisor in the event of any conflict between reviewers relating to the results.

VI. ASSESSMENT OF POTENTIAL IMPACTS

Potential impacts of FRS on civil rights and liberties: The potential impacts of ACSO's use of Lumen on civil rights and liberties are minimal. To begin with, law enforcement use is limited by statute to minimize those impacts. For example, under C.R.S. § 24-18-307, law enforcement agencies are prohibited from applying a facial recognition service to individuals based on their religious, political or social views or activities; based on their participation in non-criminal organizations or lawful events; based on their actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender expression, gender identity, sexual orientation or other protected characteristics; or for purposes of creating a record depicting an individual's exercise of their First Amendment rights. Similarly, Fourth Amendment violations are minimized by the statutory prohibitions on using match determinations as the sole basis for establishing probable cause in a criminal investigation and limitations on the use of a facial recognition service to engage in ongoing surveillance, conduct real-time or near real-time identification or conduct persistent tracking. In addition, ACSO's policy requires that match determinations be used only as investigative leads to aid in the development and collection of additional evidence.

Potential impacts to privacy: ACSO's use of Lumen as an investigative aid will have minimal impacts on individual privacy rights because the collection of candidate images is limited to booking photos and not DMV photos, social media photos or related images. Because the candidate images are limited to photos procured of individuals who have had law enforcement contact, the use of this facial recognition service poses minimal risk of infringing on the privacy rights of law-abiding citizens.

Potential disparate impacts on marginalized communities: The NIST data regarding false matches shows a limited disparate impact on Western African females of 2%. However, the NIST data derives its photo images from Visa applications. Research using U.S. booking photos as the candidate images shows the highest error rates are for white males, suggesting that the use of Lumen, which relies exclusively on booking photos, may pose less risk of potential disparate impact on marginalized communities.

Specific steps ACSO will take to mitigate foregoing potential impacts: As discussed above, the nature of the photos included in Lumen's candidate images, and the specific intended use for the Lumen facial recognition service significantly limit any potential impacts on individual rights and privacy interests. In addition, ACSO conducts annual anti-bias training and has implemented an anti-bias policy to make its members aware of potential biases and limit the impact of bias in practice. ACSO's policy governing use of a facial recognition service also requires meaningful human review of all results and mandates secondary human review and requires further human review in the event of any disputes before an arrest is made, further minimizing the potential that the facial recognition service could disparately impact marginalized communities.

VII. FEEDBACK PROCEDURES

ACSO procedures and channels for receiving feedback from individuals affected by FRS: ACSO will publish notice of and conduct three community meetings to obtain feedback on its facial recognition policy and the Lumen product specifically. In addition, this Accountability Report and its policy will be posted on its website for public review. ACSO also has well-established channels for taking and evaluating public complaints through its Internal Affairs unit. Information on how to submit complaints to Internal Affairs is publicly available on its website.

ACSO procedures and channels for receiving feedback from community at large: In addition to the procedures described above for accepting complaints, ACSO maintains open lines of communication with the public through a variety means including all of its social media platforms such as Facebook, Twitter, Instagram and Nextdoor. These social media sites are maintained by ACSO's Public Information Office and are monitored daily. The Sheriff also offers the public the opportunity for direct communication during periodic Facebook Live programs. In addition, emails can be sent to ACSOInfo@arapahoegov.com, a public email address designed specifically for questions, comments and feedback. All members also have a phone number on their business cards where members of the public can provide feedback.

ACSO procedures in place for responding to feedback: ACSO's procedures for responding to feedback are oriented to the type of feedback and the manner in which it was received. When complaints are received, individual sections may respond to specific concerns relating to their areas of expertise or the Internal Affairs unit may respond to update citizens on the status and/or results of the agency's investigation into a complaint. ACSO also conducts satisfaction surveys that are sent to members of the community and individuals who have had a contact with one its members. ACSO engages in various community outreach programs, including, for example, National Night Out and Coffee with a Cop, to engage with citizens and respond to feedback.