Facial Recognition Use and Accountability Report

605.1 PURPOSE

Agency Content

The **Mead Police Department** considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are not considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric 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, and help in the identification of persons unable to identify themselves or deceased persons. The Mead Police Department has established access and use of a face recognition to support the investigative efforts of law enforcement and public safety agencies both within and outside Mead Police Department.

It is the purpose of this policy to provide Mead Police Department personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will insure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals. Further, this policy will delineate the manner in which requests for face recognition are received, processed, cataloged, and responded to.

The Mead Police Department ("MPD") adopts this Policy as its Accountability Report required pursuant to the requirements of CO SB113. MPD intends to activate the facial recognition functionality within Lumen software platform and to use such services in support of its law enforcement investigations.

MPD proposes to use facial recognition services facilitated by Rank One Computing Corporations versions 2.21, within LexisNexis' Lumen software platform ("Lumen"). Lumen is an investigative application that utilizes criminal justice information shared between 87+ law enforcement agencies of the Colorado Information Sharing Consortium ("CISC"). The software uses state-of-the-art facial recognition technology to match the face in a user-uploaded image to mugshot images from CISC member agency records. The software is designed to be used in ways that ultimately reduce violent crime, fraud, and to make communities safer.

All use of facial recognition technology shall be only for law enforcement purposes and will be considered law enforcement sensitive information. Per C.R.S. § 24-18-307, MPD will use this technology only for investigative leads and must use any results obtained in conjunction with other leads and evidence.

This policy also applies to:

- Images contained in a known identity face image repository and its related identifying information.
- The face image searching process.
- Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, and disseminated.
- Lawfully obtained probe images of unknown suspects that have been added to unsolved image files, pursuant to authorized criminal investigations.
- Any use of a facial recognition service shall result in the creation of a record documenting the use of the service sufficient to facilitate public reporting and auditing of compliance with the agency's use and data management policies developed as part of the agency's accountability report pursuant to section 24-18-302 (2)(d)

This policy assists **Mead Police Department** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Reducing the opportunities for bias and prejudice to impact the criminal justice process.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

605.2 DEFINITIONS

Agency Content

Facial Recognition - the algorithmic process of rating the number of similarities between facial photos.

CISC - Colorado Information Sharing Consortium.

Lumen - Vendor of facial recognition software that is supplied through CISC.

Mobile Image - an image captured by an officer in the field for the purpose of being used for a facial recognition identification.

In addition the definitions provided in C.R.S. 24-18-301 are included.

605.3 FACIAL RECOGNITION SOFTWARE INFORMATION

Agency Content

605.3.1 TECHNICAL DESCRIPTION AND INTENDED USE

Agency Content

Lumen may be used in an investigation 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 match score generated by the ROC SDK's facial recognition algorithms.The match 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.

605.3.2 CAPABILITIES AND FUNCTION

Agency Content

The Lumen facial recognition tool helps solve crimes after-the-fact by matching photos obtained by a government customer, of suspects, persons of interest to a law enforcement investigation, and victims or possible victims of crimes against images of known persons contained within the CISC member-agencies records. Specifically, the Lumen facial recognition tool uses a machine-learning facial recognition algorithm to initiate a search between the face in probe image against the images contained within the criminal justice records available only to members of the CISC. At that point, law enforcement personnel make independent assessments to determine if there is a match between the probe image and images scored high within Lumen. Each decision about a possible match is made by a member of the MPD.

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.

605.3.3 DECISION MAKING

Agency Content

The Lumen facial recognition tool is only intended to support investigations and does not make any decisions as to whether the probe image is a match to a database image. Each decision about identification is made by a member of the MPD and not by an automatic process. Law enforcement personnel must review the results for every search to enable human review and independent verification. Probable Cause determinations may not be based solely on these identifications. In addition, all results will be peer reviewed by other sworn members prior to utilizing any information obtained.

605.3.4 INTENDED USE AND BENEFITS

Agency Content

The Lumen facial recognition tool is intended to enhance the investigative abilities of the MPD. This type of facial recognition technology automates the process necessary to locate potential matches between a probe image and thousands of criminal justice record images that would otherwise require a manual search by human. The facial recognition algorithm will rank potential matches in a manner that allows for a simplified process of human review.

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 unsolved crimes. 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 have been 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 which a person was falsely arrested on the basis of a facial recognition match.

605.3.5 DATA INPUTS AND GENERATION

Agency Content

The Lumen facial recognition tool uses the following types of data inputs:

- User submitted probe images and associated information identifying the purpose of the search (such as case number and type of crime).

- The candidate facial image data is collected by the CISC from its member agencies, the national NCIS Law Enforcement Information Exchange (LInX) and the FBI's N-DEx national information sharing system.

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

605.4 DATA MANAGEMENT, TRAINING, AND USE POLICY

Agency Content

The MPD will follow statutory requirements described in Colorado Revised Statutes 24-18-301 through 309, in conjunction with an approved department directive. As such, the department will follow the below guidelines regarding data management, training and the authorized use of the facial recognition service.

605.4.1 DATA MINIMIZATION

Agency Content

The features and function of the Lumen facial recognition tool effectively reduces the risk of inadvertent access to data by MPD personnel. As noted above, the Lumen facial recognition tool searches only criminal justice records available to CJIS-certified law enforcement personnel of CISC member agencies. The criminal justice records available in the facial recognition tool are subject to the retention policies of the owner agencies.

605.4.2 DATA INTEGRITY AND RETENTION

Agency Content

The Patrol Commander will be designated as the Facial Recognition Administrator overseeing all Lumen facial recognition tool permissions for the MPD. This person will have the capability to audit and review any, and all usage of this facial recognition software by any authorized member of the department. 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.

All information obtained from the Lumen facial recognition tool by any member of the police department will be collected in a formal report and retained in accordance with guidelines set forth in the record management system.

Without the express permission of MPD, or as required by law, such as a judicial order, LexisNexis employees will not review MPD search history within the Lumen facial recognition tool, ensuring that sensitive investigative data will remain confidential.

All information available within the Lumen investigative platform, including the facial recognition tool, is purged according to the retention schedule and policies set by the owner agency. For example, any information made available to other CISC member agencies by MPD is purged from the Lumen investigative platform when its retention expires inside MPD's record management system.

605.4.3 USAGE RULES AND REQUIREMENTS

Agency Content

Access to facial recognition search results will be provided only to individuals within the MPD who are authorized to have access and have completed applicable training. Authorized access to the MPD facial recognition software will be granted only to personnel whose positions and job duties (Investigations, Intelligence and Analysts) require such access. The facial recognition administrator shall grant and audit all user access, following the required account approval. All facial recognition users shall be required to have individual access for use of the facial recognition software/technology.

Approved facial recognition operators will analyze, review, and evaluate the quality and suitability of probe images, to include 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.

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 on copies, saved as a separate image, and documentation will indicate what enhancements were made, including the date and time of change. The resulting images, if any, shall be manually compared with the probe image by the person conducting the comparison.

Any upload of a probe image, query, or request shall include 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. This information will be logged, tracked and available for auditing and review.

Per Colorado Revised Statutes §24-18-303, members shall disclose the use of facial recognition technology to a criminal defendant in a timely manner prior to trial.

Use of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The use must be limited to the following situations:

- There exists 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.
- To support law enforcement in critical incident responses and special events.
- To assist in the identification of potential witnesses and/or victims of violent crime.
- For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.

- To investigate and/or corroborate tips and leads.
- To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).
- To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.
- There is an active or ongoing criminal or homeland security investigation.

Facial recognition data is stored securely on Lumen servers, and access is limited to authorized users within Lumen.

Lumen is a web-based software and not an application which needs to be downloaded to any Town of Mead computers. Any records exported by MPD members shall be immediately uploaded to the department's record management system (Versadex). Versadex is CJIS compliant and maintained by the City of Mead's Information Technology department.

605.4.4 TRAINING PROCEDURES

Agency Content

Training will be provided by the MPD to all authorized users of facial recognition services. This training will be arranged and documented by the facial recognition program manager and account access will not be created or provided until training has been completed. Training will cover both the use of facial recognition software/technology as well as a specific review and acknowledgment of all elements of this policy.

Per Colorado Revised Statute Section 24-18-305, the training will at a minimum include:

- The capabilities and limitations of the facial recognition service.
- Procedures to interpret and act on the output of the facial recognition service; and
- 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.

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

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

605.4.5 TESTING PROCEDURES

Agency Content

In accordance with CRS 24-18-304(4), Rank One Computing submitted 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
Presentation Attack Detection -	https://pages.nist.gov/frvt/html/frvt_pad.html

605.4.6 MINIMIZATION OF RISK OF FALSE MATCH

Agency Content

The potential impact of a false match, including on protected subpopulations, is mitigated by the human investigator review requirement as well as by the requirement to develop additional evidence prior to making an arrest. While an erroneously high match score from the facial recognition software would potentially result in a candidate ranking higher on a list of results, 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 candidate 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 facial recognition software and the human investigation, such false match could become an investigative lead which would require additional investigation and may be ruled out due to additional investigation.

However, studies have shown that erroneous investigative leads do not result in a false arrest. As shown by the NYPD statistics, facial recognition is used tens of thousands each year by a single agency without a known instance of false arrest (see https://www.nyc.gov/site/nypd/about/about-nypd/ equipment-tech/facial-recognition.page). Across the nation, automated facial recognition has been used on the order of millions of times by law enforcement agencies, and there are only three known false arrests involving automated facial recognition. Each of these false arrests is attributable to violation of applicable policies and procedures, particularly the requirement to develop independent evidence to support probable cause prior to making an arrest.

605.4.7 RESTRICTIONS OF USE

Agency Content

The MPD and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

MPD will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:

- Non-law enforcement (including but not limited to personal purposes).
- Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
- Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- Harassing and/or intimidating any individual or group.
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

MPD does not connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system will not be configured to conduct face recognition analysis on live or recorded video.

MPD will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

MPD shall not use the results of a facial recognition service 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 law enforcement officer to establish probable cause in a criminal investigation.

Any member of MPD using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals shall ensure that those decisions are subject to meaningful human review. (CRS 24-18-303)

Facial recognition services shall not be used to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless:

- MPD obtains a warrant authorizing such use;
- Such use is necessary to develop leads in an investigation;
- MPD has established probable cause for such use; or
- MPD 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. A court may issue an ex parte order under this subsection (1)(d) if a law enforcement officer certifies and the court finds that the information likely to be obtained is relevant to locating or identifying a missing person or identifying a deceased person.

Facial recognition services shall not be applied 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.

Facial recognition services shall not be used to create a record depicting any individual's exercise of rights guaranteed by the first amendment of the United States constitution and by section 10 of article II of the state constitution.

MPD 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.

This policy is closely associated with policy 337 Public Safety Video Surveillance System. The provisions in policy 337 for media collection and storage are applicable to the media collected and maintained for facial recognition purposes. Nothing in this policy is meant to conflict or override policy 337.

605.4.8 OFFICER RESPONSIBILITIES

Agency Content

Members of the MPD will only use facial recognition tools in the manner prescribed by the associated training and this policy.

All uses of facial recognition tools will be thoroughly documented in the respective official report to include;

- The crime being investigated OR the reason for exigency in identifying a person without a criminal nexus.
- The source of the comparison photo.
- The nexus between the photo being compared and the crime being investigated.
- The results of the comparison using the facial recognition tool.
- Any corroborating evidence that associates the suspect to the crime being investigated.

Members are reminded of the following concerns surrounding the use of facial recognition;

- No charges or arrest will be pursued based solely on the results of a facial recognition comparison.
- Corroborating evidence should be thoroughly documented.
- A probable cause assessment should be made and documented.
- Only when sufficient probable cause exists to pursue charges, should the officer pursue an arrest.

605.4.9 SUPERVISOR RESPONSIBILITIES

Agency Content

The supervisor shall review all uses of the facial recognition tool to insure compliance with this policy.

The supervisor will review cases where facial recognition tools were used to insure that sufficient probable cause existed prior to the filing of charges or arrest of the suspect.

Supervisors will use examples of facial recognition uses to provide updated training to officers.

Supervisors shall insure that officers receive facial recognition training prior to utilizing the facial recognition tools.

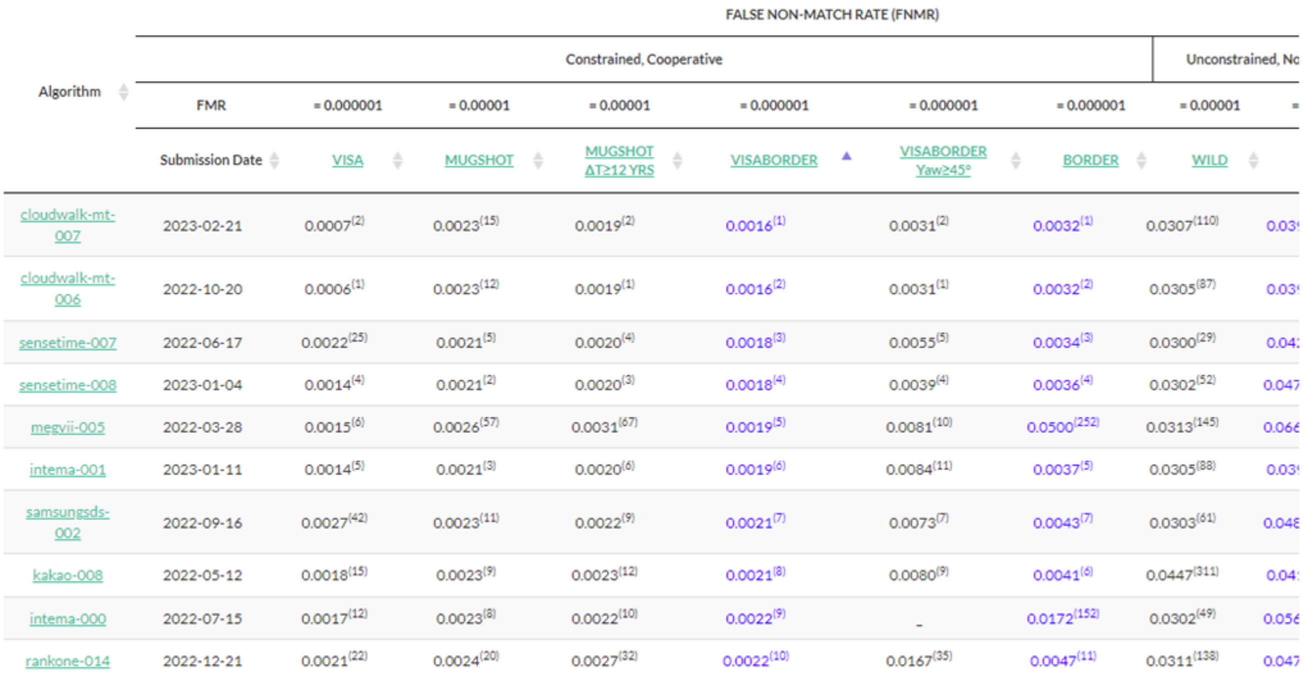
605.5 ACCURACY AND IMPACT

Agency Content

605.5.1 TEST RESULTS

Agency Content

Rank One Computing's SDK facial recognition algorithm was submitted to the National Institute of Standardization and Technology (NIST) Face Recognition Vendor Test (FRVT) for 1:1 Verification. In that test, ROC's SDK facial recognition algorithm ranked No. 10 in the world out of 478 total entries and was the top entry from the United States



Algorithm	FALSE NON-MATCH RATE (FNMR)								
	Constrained, Cooperative							Unconstrained, No	
	FMR	= 0.000001	= 0.00001	= 0.00001	= 0.000001	= 0.000001	= 0.000001	= 0.00001	=
	Submission Date	VISA	MUGSHOT	MUGSHOT ΔT≥12 YRS	VISABORDER	VISABORDER Yaw≥45°	BORDER	WILD	
cloudwalk-mt-007	2023-02-21	$0.0007^{(2)}$	$0.0023^{(15)}$	$0.0019^{(2)}$	$0.0016^{(1)}$	$0.0031^{(2)}$	$0.0032^{(1)}$	$0.0307^{(110)}$	0.03
cloudwalk-mt-006	2022-10-20	$0.0006^{(1)}$	$0.0023^{(12)}$	$0.0019^{(1)}$	$0.0016^{(2)}$	$0.0031^{(1)}$	$0.0032^{(2)}$	$0.0305^{(87)}$	0.03
sensetime-007	2022-06-17	$0.0022^{(25)}$	$0.0021^{(5)}$	$0.0020^{(4)}$	$0.0018^{(3)}$	$0.0055^{(5)}$	$0.0034^{(3)}$	$0.0300^{(29)}$	0.04
sensetime-008	2023-01-04	$0.0014^{(4)}$	$0.0021^{(2)}$	$0.0020^{(3)}$	$0.0018^{(4)}$	$0.0039^{(4)}$	$0.0036^{(4)}$	$0.0302^{(52)}$	0.047
megvii-005	2022-03-28	$0.0015^{(6)}$	$0.0026^{(57)}$	$0.0031^{(67)}$	$0.0019^{(5)}$	$0.0081^{(10)}$	$0.0500^{(252)}$	$0.0313^{(145)}$	0.06
intema-001	2023-01-11	$0.0014^{(5)}$	$0.0021^{(3)}$	$0.0020^{(6)}$	$0.0019^{(6)}$	$0.0084^{(11)}$	$0.0037^{(5)}$	$0.0305^{(88)}$	0.03
samsungsds-002	2022-09-16	$0.0027^{(42)}$	$0.0023^{(11)}$	$0.0022^{(9)}$	$0.0021^{(7)}$	$0.0073^{(7)}$	$0.0043^{(7)}$	$0.0303^{(61)}$	0.048
kakao-008	2022-05-12	$0.0018^{(15)}$	$0.0023^{(9)}$	$0.0023^{(12)}$	$0.0021^{(8)}$	$0.0080^{(9)}$	$0.0041^{(6)}$	$0.0447^{(311)}$	0.04
intema-000	2022-07-15	$0.0017^{(12)}$	$0.0023^{(8)}$	$0.0022^{(10)}$	$0.0022^{(9)}$	-	$0.0172^{(152)}$	$0.0302^{(49)}$	0.05
rankone-014	2022-12-21	$0.0021^{(22)}$	$0.0024^{(20)}$	$0.0027^{(32)}$	$0.0022^{(10)}$	$0.0167^{(35)}$	$0.0047^{(11)}$	$0.0311^{(138)}$	0.047

605.5.2 BIAS AND INACCURACY

Agency Content

In the NIST Demographic Effects series the ROC SDK ranked 8th worldwide across all 70 sub-populations of the NIST test data, with the lowest scoring demographic being West African females aged 65-99 years old (0.01871% false match rate).

605.5.3 CIVIL RIGHTS IMPACT

Agency Content

The potential impact of a false match, including on protected subpopulations, is mitigated by the human investigator review requirement as well as by the requirement to develop additional evidence prior to making an arrest. 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 their skills, training, and experience in the facial examination to closely review the unique 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 based on the 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 eludes both the ROC SDK and the human investigator, it could become an investigative lead, triggering additional investigation into the relevant candidate. In the absence of additional evidence, erroneous investigative leads do not result in a false arrest. NYPD statistics show that their agency uses facial recognition tens of thousands of times each year without a known instance of false arrest.

MPD personnel with access to the Lumen facial recognition tool are required to input a case number and crime type prior to initiating a search, affirmatively representing that the search is conducted for the purpose of investigating a crime that has been committed. As a result, the use of the Lumen facial recognition tool for "fishing expeditions" or monitoring persons engaged in lawful activities is curtailed. This information will be verified by ongoing scheduled audits of user inputs into the facial recognition service.

Usage of the Lumen facial recognition tool by the MPD is unlikely to have a negative impact on the civil rights, liberties, privacy, or on marginalized communities of the people of the State of Colorado. ROC's SDK algorithm achieved greater than 99% accuracy across all demographic groups on NIST's FRVT Demographic Effects in Face Recognition test program; thus, disparate impact on marginalized communities is likely to be negligible.

The MPD has clear guidelines prohibiting investigations into individuals based in whole or in part on a person's actual or perceived race, ethnicity, gender, national origin, language preference, religion, sexual orientation, gender identity, age or disability, unless that investigation is based on a reliable suspect-specific description of the individual that includes other non-demographic identifying characteristics.

605.6   PUBLIC FEEDBACK

Agency Content

The Mead Police Department will seek approval from its elected body prior to the implementation and utilization of the Lumen facial recognition tool. As is statutorily required by C.R.S 24-18-302, consideration and public comment will be heard at a Public Safety Committee Meeting, Council Study Session, and Council Regular meeting should the item be moved forward at each meeting respectively.