TO: Honorable Mayor Phillips and Avon Town Council Members
FROM: Chief Greg Daly
RE: The Avon Police Department's Accountability Report regarding the request to use Facial Recognition Services in accordance with Colorado Revised Statutes (C.R.S.) 24-18-302
DATE: June 13, 2023

SUMMARY: Facial Identification/facial recognition has evolved into a cutting-edge crime solving/ crime fighting investigative tool. Generally, there are two uses of facial recognition- "live view" at some airports for example, where faces from live footage security cameras are compared against an active database, or the more widely used, post incident/event facial identification comparison of "still" photographs against a photo database of known offenders (typically from arrest booking photographs). This accountability report centers around "still photograph" facial identification and **not** live surveillance. The comparison of a still photographic image can provide a selection of possible investigative lead photographs that an investigator can compare with and analyze against. The investigator then builds his/her case with other independent evidence. Importantly, while facial recognition service ("FRS") results are valuable, the results of an FRS comparison cannot serve as the sole basis to establish probable cause in a criminal investigation.

In June 2022, the Colorado State legislature passed Senate Bill 22-113 (SB113), which enacted C.R.S. §§ 24-18-301 through 24-18-309 imposing new requirements on local government agencies, including law enforcement, related to the use of facial recognition services.

Investigative uses of FRS by law enforcement are subject to the statute, C.R.S. § 24-18-301, et seq. SB113 requires that a municipal police department that wishes to use or to continue to use an FRS for investigative purposes must file with its city council a "Notice of Intent" and thereafter an "Accountability Report" related to its proposed use of FRS. The Avon Police Department provided an initial notice of intent, held three community public comment/listening sessions, provided a public comment link on our website and this is the final accountability report from the public process. This final report has been posted to the Town of Avon website and to the Avon Police Department website. We are also required to provide a biannual accountability report to the Avon Town Council.

BACKGROUND: The Avon Police Department has the potential availability of three facial recognition services (FRS).

- The Department of Revenue, Motor Vehicle Investigations Unit, Law Enforcement Communications Center utilizing its database of driver's license photographs.
- The Colorado Bureau of Investigation, utilizing post arrest booking "mugshot" photographs from Sheriff's Offices primarily in the Denver metro area and from the Federal Bureau of Investigation.
- The Colorado Information Sharing Consortium (CISC) Regional Data Warehouse utilizing the Lexis Nexis/Lumen information exchange IT platform. CISC is a consortium of eighty-seven (87) Colorado law enforcement agencies. The mission statement of CISC is "Making data-driven crime solutions available to all Colorado law enforcement agencies." The database comprises of post

arrest booking “mugshot” photographs from all the Colorado member agencies that submit their booking photographs to the consortium (https://cisc.colorado.gov/).

Facial recognition technology must only be used for legitimate law enforcement purposes. Authorized uses of facial recognition technology are limited to the following:

1. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime;
2. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity;
3. To identify a deceased person.
4. To identify a person who is incapacitated or otherwise unable to identify themselves;
5. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else’s identification, or a false identification; or
6. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

Senate Bill 22-113 was passed with an intent to regulate the use of and ensure adherence to many privacy concerns expressed by the legislature at that time. A law enforcement agency shall not apply a facial recognition service to any individual based on the individual's religious, political, 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.

After filing the notice of intent with the Avon Town Council on March 14th and prior to finalizing this accountability report, the Avon Police Department complied with the legislation by:

(a) allowing for a public review and comment period by opening a comment section on our website;
(b) held three public meetings to obtain feedback from our community; and
(c) considered the issues raised by the public through the public meetings.

As a result, our presentation of this accountability report tonight and based on the Town Councils final decision, if approved, we will allow for a ninety-day period before the Avon Police Department utilizes a facial recognition service. As required, we have posted the final adopted accountability report on the agency's public website and submitted it to the agency's reporting authority (Avon Town Council). The reporting authority shall post the most recent version of each submitted accountability report on its public website. The report has been posted to the Town of Avon website. An agency shall update its final accountability report and submit the updated accountability report to the agency's reporting authority at least every two years.

Another major point for consideration from this legislation is that any suspect candidates who are identified by a facial recognition solution are viewed “only” as an investigative lead and should not be viewed as the sole basis for probable cause in a criminal investigation. The results are to be used by officers or detectives merely as possible leads in identifying a suspect in a criminal investigation. The officers and detectives will ensure that their decisions are subject to meaningful human review before proceeding with

the investigation in accordance with C.R.S. § 24-18-303. Use of FRS will follow state law, and the limitations of C.R.S. § 24-18-307 will be respected.

The act prohibits an agency from using an FRS to engage in ongoing surveillance (like at an airport); conduct real-time or near real-time identification; or start persistent tracking unless the law enforcement agency (LEA) obtains a warrant authorizing such use, such use is necessary to develop leads in an investigation, the LEA has established probable cause for such use, or the LEA 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. Avon PD does not have any internal resources that would allow for real-time surveillance using FRS, but if we were to request that resource from an outside agency, we would obtain a search warrant per the statue.

Pursuant to C.R.S. § 24-18-306, an agency must maintain records that are sufficient to facilitate public reporting and auditing of compliance with the agency's facial recognition policies. Accordingly, Avon PD will create an internal database to track when officers submit a photograph to any outside agency for facial recognition, tracking the requesting officers name, the case or event number for the inquiry, the type of investigation, the outside FRS agency that we are requesting to conduct a facial recognition search and if the facial recognition comparison led to any outcomes. This information will be incorporated into a statistical biannual accountability report for the Town Council.

PUBLIC COMMENT AND PUBLIC LISTENING SESSIONS:

Per our Communications Manager Liz Wood, we advertised the public listening sessions via Vail Daily Digital Advertising. We ran three print advertisements in English and three in Spanish - one for each meeting. We spent $1,000 on digital ads on VailDaily.com in two languages that clicked through to the webpage with more information and the public comment form. We received 51,895 impressions (views) of the ads. Twenty-four people clicked on the ads to go to the PD webpage about facial recognition.

We posted information regarding the public comment section and public meetings on both the Town of Avon and Avon PD's Facebook.

We had two public comments through the public comment section on the PD website.

"From Avon Resident. Received 3/24 at 1:54 PM

While I am not in favor of police, law enforcement or anyone utilizing live streaming facial recognition technology for any kind of surveillance. I am in favor of the use of this facial recognition technology for the requested specific uses.

From Avon Resident. Received 4/4 at 3:31 PM

It starts with facial recognition, then it will be digital ids, then social credit scores. As if there is so much crime in Avon that they need facial recognition."

We had the following comments on the PD Facebook post. The individuals did not comment as to whether they were Avon residents;

"Person # 1
Because of such an increase in crime. My personal opinion says, you're warranted to use such a tool. Why not use an appropriate tool to specifically monitor for crime of any kind. Minor to major. Anyone who wouldn't agree just might have

something to hide. Because if you're worried about being identified for something you haven't done in a place you weren't.
You need an evaluation. Good luck.

Person #2 to Person # 1 you may be willing to give up your freedom to privacy, but in my opinion, if this was really about crime, we need a justice system that will actually punishes criminals.
Using AI and databases to fight crime is really just a myth. To prove it, we have finger printing systems, probation and parole systems, ankle monitors and GPS tracking software. Plus, some of the best intelligence agencies and crime fighting techniques but Crime is still prevailing. Why?
Founding fathers have stated those who are willing to sacrifice freedoms for security deserve neither. The nazi proved it.

Person # 1 to Person # 2
I understand where you're coming from, and I agree. "If" identify was the only incident. Everything is connected and if you're soft on crime. This is absolutely unnecessary.
However.
And I don't know. Perhaps law enforcement should be allowed to be tough on crime. Hands being tied?
No doubt, in areas. I don't have their solution. I can see how a tool like this can be useful for what they are talking about."

Example of post to Town of Avon Facebook

We posted a poster at the Avon Library and provided posters to Aspens Property Management for distribution. Additionally, the last public comment meeting was conducted during the April 25th council meeting and the agenda was advertised via the usual channels.

On March 24, Detective A. Herendez completed a Facebook live Spanish interview with the Vail Valley Latino show, answered questions and advertised the three public comment/ listening meetings; https://www.youtube.com/watch?v=JKRmdeiD_4I Minutes 5:00 – 12:03

On April 6, the Vail Daily published a news article about Facial Recognition and our public process; https://www.vaildaily.com/news/avon-police-department-campaigns-for-use-of-facial-recognition-services/

We had three public comments session.

1. March 29th at 7:00pm at the Aspens Mobile Home Park, Community Center, 901 West Beaver Creek Boulevard, Avon, CO 81620- We had 26 attendees.
2. Saturday April 15th at 11:00am at Avon Public Library, 200 Mikaela Way, Avon, CO 81620- No attendees.
3. April 25th at 5:00pm at the Avon Town Council meeting at 100 Mikaela Way, Avon, Co. 81620- Two community members made comments and asked questions and Town Council members had a number of questions and requested some clarifications.

This is a summary of the comments from the Aspens meeting and the Town Council Public comment session.

"Community Input Meeting
Aspens Mobile Home Park
March 29, 2023

Public Questions/Comments:

APD will be using the technology to map a person's face, correct? Yes

Will we be placing the cameras in certain places to get the photos? No

If we (APD) get a photo, we send it in, will we be doing that for every person? No, it can be used on crimes where the suspect is unknown. We can try to identify if we have a photo.

A community member asked if it had worked in Vail during the string of bike/ebike thefts as they recovered many bikes. The Chief stated Vail hasn't gone through this process yet, it was most likely other shared photos and some personal knowledge helped capture the thieves.

Is it going to be more exact to identify person(s) who committed the crime? Technology and photo clarity are improving so hopefully we can get more positive results in the future.

Is it enough probable cause for an arrest if your face matches? No, APD can use the information as a lead only in their investigation but not probable cause for an arrest. We would still have to build a case; this technology is just one tool in an investigation.

Where are the cameras? Avon is not placing cameras for this purpose. Businesses or personal cameras will potentially capture photos and can be shared with the department.

Comment: A great tool to have because it will help eliminate doubt about a suspect and also a good thing if it brings justice for victims of crime.

Comment: Valuable given everything going on with schools and shootings.

Is it a requirement for stores/public places to have cameras? No.

Are there programs that will provide cameras? Not specifically.

Can HOA's and such forbid people to put up cameras (such as Ring) outside their house? If you have a camera installed at your residence you can't pick up privacy matters in someone else's house. Some places may not allow drilling for installation but there are battery operated/wireless cameras available. One resident said he supports it. He also feels like having access and spreading awareness of it may deter people from committing crimes.

If Crime occurs in Avon, can we send to other agencies before we fully investigate in hopes to catch criminals? We already do this (depending on the crime) in hopes of finding people more quickly (surrounding Law Enforcement agencies, Facebook etc.)

It was asked if it can be shared to the community in general (we cannot currently use ECalert/Everbridge for this purpose) and if people can share this information and the answer was yes.

One resident stated they receive amber alerts through the phone, is this different technology or similar? Different.

Do we think technology will help speed up identifying a suspect? It may be one of many tools that will help.

A resident was wondering if we can utilize it anywhere in Eagle County or just Avon? The County (and other towns) will have to go through the same public input process as Avon is in order to use it.

APPLAUSE from the crowd because Avon likes to be a leader!

As a community what can we do to help get this approved? Provide comments on Avon PD's Facebook page and on the website, whether for or against. Comments can be in English or Spanish."

We received a follow up email from Augustina Del Hoyo, Resident Manager for the Aspens;

"Thank you for last night's conference. Thank you for your concern for the safety and well-being of our community, families and children.

The Aspens community will be supporting the Facial Recognition Project.

Best regards

Agustina Del Hoyo, Resident Manager, The Aspens Mobile Home Village"

These were the two public comments/questions at the April 25th public comment session at that Avon Town Council Meeting.

A resident of Wildridge raised questions related to how often Avon PD expects to use the technology and under what kind of circumstances, is it 100 times, are they for murders or is it five times and they are for jaywalk offenses.

Chief Daly responded that he could not see it happening very often because it will be down to the quality/resolution of the photographs submitted. He discussed an internal debate over whether facial recognition should be used only for serious crimes or felonies, and he shared a little story that he mentioned at the first meeting (at the Aspens Community Center) regarding an example of an event at Walmart, where a person had their handbag stolen from Walmart, should the Police Department be limited using this technology where that person had their last $300 in their life in that handbag (stolen), and whether it was as important to pursue justice for that person versus a more serious crime. Chief Daly shared that a lady came up to him after the meeting to say that it was her and that she had her last rent money in her bag. The Avon Police Department was able to track that individual down and repatriate the money back to her. Chief Daly confirmed that the PD would not be using facial recognition for jay walking, but yes on thefts, assaults, and more serious crimes. Chief Daly didn't want to put a limit on the types of crimes that the PD utilizes facial identification technology, because to one person $300 may not be a big deal but that the aforementioned lady came up and said that it was her last rent money. That was why Chief Daly did not want to put a restriction on it. However, we would not waste their time (the facial recognition services) with simple cases, and Chief said that we already do community facial identification/recognition by our Facebook posts with nearly a 70% success rate when asking the community if they recognize a person of interest.

Another resident of Avon raised a couple of questions; what constitutes a basis that such individual has committed, is committing or will commit a crime. What assurances are there that Avon PD will abide by the six authorized uses and what are the repercussions if an officer were to violate the terms of service?

Chief Daly shared that in terms of has, is or will commit a crime comes out of the statute book. Chief Daly said that most incidents would be post incident where the PD would try to use facial recognition. In terms of will commit, Chief Daly gave an example of individual making threatening remarks on a Facebook post or other social media where we would want to identify that individual to see if a future violent crime may be committed against a person or an institution. Chief Daly confirmed that it is in the statute book that we can only use it for the aforementioned reasons, and we would be subject to violation of a crime if we were not to. The Police Department is required to come back every two years with an accountability report and the plan is to keep a log for every instance of use. Chief Daly shared that misuse of this technology by an officer could lead to disciplinary repercussions for an officer up to including termination and or criminal charges.

Additional councilmember questions included whether we could access photographs from outside of Colorado. Chief Daly confirmed that through the Colorado Bureau of Investigation, they can pull from the Federal Bureau of Investigations booking mugshot photograph database. The question of costs came up. Chief Daly confirmed that there was no specific additional cost for the facial recognition services as we were already paying an annual subscription service fee for Lumen services to include the database

exchange between law enforcement agencies throughout Colorado and facial recognition. However, there would be a new training cost of $150 per officer for a four-hour training course for nineteen officers and $550 each for two detectives for a 24-hour training course for a total new training cost of $3,950.

A subsequent council question revolved around the crime rates in Avon, types of crimes, misdemeanors/felonies, and the frequency of those crimes in Avon. The following table gives a quick summary of crimes from 2017 to 2022.

Avon Police Department
2006-2022 Activity Statistics

	2017	2018	2019	2020	2021	2022
Total Crimes Reported	798	827	668	530	564	536
Group A Crimes	313	359	201	285	287	264
Group B Crimes	487	468	426	245	277	272
Clearance Rate	.43	.51	.48	.46	.44	.37
Total Reports	901	855	703	662	664	693
Calls for Service	22,890	20,632	20,213	26,741	20,253	18,236
Dispatched calls	4,712	4,996	4,850	4,274	4,728	4,610
Traffic Accidents	159	154	155	139	127	147
Traffic Accidents Alcohol/Drug Impaired	7	7	12	5	13	11
Total Arrests	392	392	345	273	321	258
Adult Arrests	365	354	318	251	309	248
Juvenile Arrests	27	38	27	22	12	10
Felony Arrests	53	71	45	31	45	38
Sexual Offenses	11	14	7	10	10	9
Robbery	2	0	0	3	0	1
Burglary	7	13	1	3	3	13
Larceny	109	113	83	73	71	72
Motor Vehicle Theft	7	5	10	10	11	7
Assault	43	67	47	59	59	52
Arson	0	0	0	1	0	0
Forgery/Counterfeiting	3	5	4	2	2	5
Fraud	27	20	17	17	37	31
Vandalism	63	65	36	70	55	46
Weapon Offense	4	6	4	4	3	3
Narcotics	34	41	26	21	17	11
DUI	133	108	97	69	91	100
Liquor Laws	14	15	24	13	12	10
Disorderly Conduct	20	27	21	19	26	24
Domestic Violence	33	43	41	31	37	24
Traffic Stops	2281	1985	1949	1770	1680	1523
Total Traffic Warnings	1620	1561	1508	1266	1192	1110
Written Traffic Warnings	1463	1378	1423	1299	1212	1146
Traffic Summons	508	309	302	308	307	228

Chief Daly subsequently responded on 05/07/2023 to an email question from an Avon resident regarding his estimate of how many times he foresees this technology being used. The question was ""In how many cases over the year would you have used facial recognition had it been available to you, and what kind of cases were those?"

"Mr.???, to answer your *previous question, these are examples of the instances that my detective could remember that we may have submitted photos for facial identification comparison. If this process is*

approved by the council, going forward we will keep a log of every photo that we submit for facial identification comparison.

2022: *4 Total Cases*

- *Fraud/Identity Theft/Theft from the Westin*
- *Theft from Rec Center*
- *Theft from Walmart*
- *Theft from Walmart*

- ***2023:*** *4 Total Cases (From the start of the year till now)*
  - *Theft from Avon Truck and Auto*
  - *Hit and Run at Avon Center*
  - *Ski Theft from the Westin*
  - *2nd Degree Assault & Disorderly*

Respectfully,"

PRIVACY CONCERNS: As discussed, Senate Bill 22-113 was specifically created to ensure that privacy concerns are met by statewide law enforcement agencies. The Avon Police Department will adhere to the criteria set out by this bill. This system is designed as a crime prevention/investigative tool, to aid officers/detectives in solving crimes against Avon citizens resident and guests and to bring justice for victims of crimes.

FACIAL RECOGNITION SERVICES: Attachments A-C contain the responses to questions posed in C.R.S. §§ 24-18-302 from the three facial recognition services that are available to the Avon Police Department.

TRAINING: Avon PD will provide periodic training to its officers educating them on the statutory requirements regarding the use of facial recognition services, it's capabilities and limitations, image comparison principles, the procedures for using FRS, ensuring meaningful human review and the method of logging the FRS search on the department official FRS record keeping database. We have explored training through Ideal Innovations Incorporated for facial identification training courses (recommended by General Counsel of one of the FRS) The basic four-hour introductory course costs $150 per officer and the more advanced 24-hour course will provide the participant with a system-agnostic foundation for Facial Examination. Participants will have the opportunity to conduct comparisons; learn key definitions, the stability of facial features, and contributions to facial uniqueness. Challenges within the discipline and agencies/organizations that are influencing the discipline are discussed. The 24-hour training costs $550 per officer. We intend that all officers will complete the four-hour course and the Department's two detectives will complete the 24-hour courses. Officers who use the FRS will consult with a detective on the images before they use the information as investigative leads.

FINANCIAL CONSIDERATIONS: There is no cost to use FRS though Colorado Department of Motor Vehicles or the Colorado Bureau of Investigation. The Avon Police Department is a member of CISC, and we pay a subscription of $2,163 per year to use the Lexis/Nexus Lumen database (cost is already included in our budget). This covers our twenty-one commissioned officers. The LexisNexis/Lumen investigative tool covers many investigative database resources and within these resources is their facial recognition

service. If approved by Avon Town Council, nineteen officers will complete the four-hour course and two detectives will complete the 24-hour course, 19 x $150= $2,850 and 2 x $550= $1,100 for a total of $3,950 (to be taken out of professional development/training budget).

STAFF RECOMMENDATION: The majority of public comment has been supportive in the Avon Police Departments request to use facial recognition/identification resources. In the 90-day waiting period before utilizing Facial Recognition resources, Avon PD officers will complete a 4-hour familiarization training and our two detectives will complete a 24-hour training. We recommend that the Avon Town Council authorize the Avon Police Department's use of the facial recognition/identification services as a crime solving investigation tool. Avon PD will create a database for FRS use to facilitate public reporting. Finally, the Avon Police Department will complete a biannual Facial Recognition Service accountability report to the Avon Town Council.

PROPOSED MOTION: "I move to authorize the Avon Police Department's use of facial recognition/facial identification services, as a crime solving tool, with the understanding that the Avon Police Department will ensure proper legal use, adherence to policy and provide proper training in its use. Additionally, the Avon Police Department will produce, as legislatively required, a biannual accountability report on facial recognition/identification use, to its reporting authority, the Avon Town Council."

Thank you, Chief Greg Daly

# # #

ATTACHMENTS:
Attachment A Lumen Rank/ One Computing
Attachment B Colorado Bureau of Investigation
Attachment C Department of Revenue, Motor Vehicle Investigations Unit, Law Enforcement Communications Center

Required data from the three facial recognition services that Avon PD would like to utilize:

Attachment A

Lumen/ Rank One Computing

After filing the notice of intent described in subsection (1) of this section, and prior to developing, procuring, using, or continuing to use a facial recognition service, an agency shall produce an accountability report for the facial recognition service. An accountability report must include:

(a)

(I) The name, vendor, and version of the facial recognition service; and Rank One Computing Corporation's ROC SDK version 2.2.1 provides the core facial recognition algorithms that are utilized in LexisNexis Risk Solutions' Lumen product, an integrated data platform leveraged by public safety analysts, investigators, patrol officers and commanders to help solve cases faster.

(II) A description of its general capabilities and limitations, including reasonably foreseeable capabilities outside the scope of the agency's proposed use; 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.

(b)

(I) The type of data inputs that the facial recognition service uses; The Lumen facial recognition service accepts images as data inputs.

(II) How data is generated, collected, and processed; and [LexisNexis] 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 Any images containing faces are processed into Lumen's facial recognition service. The probe image is collected in the course of an investigation.

(III) The type of data the facial recognition service is reasonably likely to generate; 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.

(c) A description of the purpose and proposed use of the facial recognition service, including: 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. (See https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page)

(I) What decision will be used to make or support the facial recognition service; and

(II) The intended benefits of the proposed use, including any data or research demonstrating those benefits;

(d) A clear use and data management policy, including protocols for the following:

[DEFER TO ARAPAHOE COUNTY – see NYPD and CISC models]

(I) How, when, and by whom the facial recognition service will be deployed or used; to whom data will be available; the factors that will be used to determine where, when, and how the technology is deployed; and other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances;

(II) If the facial recognition service will be operated or used by an entity on the agency's behalf, a description of the entity's access and any applicable protocols;

(III) Any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose for which the facial recognition service will be used;

(IV) Data integrity and retention policies applicable to the data collected using the facial recognition service, including how the agency will maintain and update records used in connection with the service, how long the agency will keep the data, and the processes by which data will be deleted; [LexisNexis] The agency determines retention and collections policies. On the FaceRec side we sync all data the agency has in Lumen into the FaceRec service; therefore, their current data retention policies apply to FaceRec as well.

(V) What processes will be required prior to each use of the facial recognition service;

(VI) Data security measures applicable to the facial recognition service, including:

(A) How data collected using the facial recognition service will be securely stored and accessed; and [LexisNexis] Facial recognition data is stored securely on Lumen servers, and access is limited to authorized services within Lumen

(B) If an agency intends to share access to the facial recognition service or the data from that facial recognition service with any third party that is not a law enforcement agency, the rules and procedures by which the agency will ensure that the third party complies with the agency's use and data management policy;

(VII) The agency's training procedures, including those implemented in accordance with section 24-18-305, and how the agency will ensure that all personnel who operate the facial recognition service or access its data are knowledgeable about and able to ensure compliance with the use and data management policy before using the facial recognition service; and

(VIII) Any other policies that will govern use of the facial recognition service;

(e) The agency's testing procedures, including its processes for periodically undertaking operational tests of the facial recognition service in accordance with section 24-18-304;

In accordance with subsection (4) of Colo. Rev. Stat. Section 24-18-304, 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).

(f) Information concerning the facial recognition service's rate of false matches, potential impacts on protected subpopulations, and how the agency will address error rates that are determined independently to be greater than one percent;

On the NIST 1:1 leaderboard, available here: 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 top 7 among vendors overall. The 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), a Russian company that is seeking to rebrand as a Dutch subsidiary of a Luxembourg fund, which in turn is a subsidiary of Russia's largest telecom (Intema fka VisionLabs and a subsidiary of Mobile TeleSystems PJSC) and Korean providers Samsung and Kakao.

	FALSE NON-MATCH RATE (FNMR)								
	Constrained, Cooperative							Unconstrained, Non-Coop	
Algorithm	FMR	≤ 0.000001	≤ 0.00001	≤ 0.00001	≤ 0.000001	≤ 0.000001	≤ 0.000001	≤ 0.00001	≤ 0.00001
	Submission Date	VISA	MUGSHOT	MUGSHOT AT≥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.

FALSE NON-MATCH RATE (FNMR)

Algorithm	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 AT≥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%.

In the NIST Demographic Effects series (available here: https://pages.nist.gov/frvt/html/frvt_demographics.html), the ROC SDK shows accuracy of less than 4% FMR with less than 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 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 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. In the absence of additional evidence, 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 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.

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]

(g) A description of any potential impacts of the facial recognition service on civil rights and liberties, including potential impacts to privacy and potential disparate impacts on marginalized communities, including the specific steps the agency will take to mitigate the potential impacts; and

DEFER TO ARAPAHOE COUNTY

(h) The agency's procedures for receiving feedback, including the channels for receiving feedback, from individuals affected by the use of the facial recognition service and from the community at large, as well as the procedures for responding to feedback.

DEFER TO ARAPAHOE COUNTY

(3) Prior to finalizing an accountability report, an agency shall:

(a) Allow for a public review and comment period;

(b) Hold at least three public meetings to obtain feedback from communities; and

(c) Consider the issues raised by the public through the public meetings.

(4) At least ninety days before an agency puts a facial recognition service into operational use, the agency shall post the final adopted accountability report on the agency's public website and submit it to the agency's reporting authority. The reporting authority shall post the most recent version of each submitted accountability report on its public website.

(5) An agency shall update its final accountability report and submit the updated accountability report to the agency's reporting authority at least every two years.

(6) An agency seeking to procure a facial recognition service must require each vendor to disclose any complaints or reports of bias regarding the vendor's facial recognition service.

Rank One Computing Corporation has not received a complaint or report of bias regarding any version of the ROC SDK. Rather, in operational environments, the ROC SDK has shown a high degree of accuracy across all demographic sub-populations without statistically significant error differentials due to demographic bias. NIST FRVT testing has explored demographic performance differentials, with the results made publicly available on its website. In addition to the Demographic Effects series data noted above, which involves data from foreign visa applications, there are also demographic performance results available in the 1:1 Verification series that show the receiver operating characteristic curve error tradeoff between FMR and FNMR for four subpopulations – white male, white female, black male and black female – based on data from US mugshot photos (see Figures 157-179 of the February 2, 2023 report).

Attachment B

Colorado Bureau of Investigation Facial Recognition Accountability report

December 2022

Agency and Vendor Information

Agency Name	Colorado Bureau of Investigation
Agency Contact	Investigations
Agency Phone Number	303-239-4201
Vendor Name	Idemia

Software Information

Name of Software	Idemia MBIS Module – MorphoBis Face
Version of Software	4.4
General Capabilities	Create a template of an unknown person's face image, to then compare it to a known mugshot database to determine whether there is a likely match. The comparison is achieved through a multi-stage architecture with successive algorithms and is then assessed by human analysis.
Limitations	The system is only as good as the mugshot photos law enforcement agencies submit to the CBI/FBI.
Reasonably foreseeable Capabilities outside the scope of the agency's proposed use	While there are no plans to use it for such at this time, it could help identify a deceased person, or a victim of a crime if there is a photo available.
Is the software/service live surveillance or mugshot based?	Mugshot based. There is no live component to this system. A photo must be manually uploaded into the system of mugshots to be searched.
What decision was used to make or support the Facial Recognition Software?	The CBI believes having the technology available for use will help solve crimes

Purpose and Proposed Use of Facial Recognition Services

The purpose of using Idemia's MorphoBis Face software is to generate an investigative lead based on a photograph, or image pulled from a video to help solve an investigation into a crime. This is not a live surveillance system so there is no real time surveillance being used, it is strictly used on a case-by-case basis. An agency must be actively investigating a crime, with a case number, and have a usable photograph or image pulled from a video feed in order for the CBI to use the software. The photo will be entered into the software and run against the CBI and FBI mugshot databases only. Once the software returns its results, a CBI analysist who has been trained in Forensic Facial Comparisons will perform a manual analysis of the results and see if it is a possibility the generated results could be a lead of LEO. If the analysist determines it is a possibility, that lead is given to the requester as an investigative lead only. The leads generated cannot be used for probable cause and are not considered to be a positive identification of a person.

Data Information and Security

Type of Data inputs used	Photograph, or a still image taken from a video
How is the data generated, collected, and processed?	The search photo is generated and collected from a surveillance video or camera, or taken by a witness etc. It is scanned into the computer and
What type of data the system is reasonably likely to generate?	The system may produce an investigative lead for law enforcement. The system is not to be used as a form of positive ID and cannot be used as a basis for probable cause. It is to be used as an investigative tool for the LEO to pursue as their investigation continues.
How will data collected be securely stored and accessed?	The software resides on the CBI secure network and can only be accessed from that secure connection.
What, if any measures are taken to minimize the inadvertent collection of data beyond the amount necessary for the specific purpose the facial recognition software/service will be used?	This does not apply; it is not a surveillance type system.

Agency's Procedure to Include Periodically Undertaking Operational Tests per 24-18-304	Query the face recognition system with images whose exact binary copies have already been enrolled in the database. Ensure the Rank-1 match candidate has the same image as the probe. Continue to perform the first two steps with additional images as often as availability of computing resources and human effort allow. Testing is performed to ensure Gallery images are properly enrolled, and their corresponding templates are both valid and accessible. The Face Recognition (FR) system's network access is not interrupted for any distributed resources. Software running on local and network resources is not exhibiting any failures.

Data Integrity and Retention Policies

How will the agency maintain and update records?	The searched photo is not retained in the database after its search; therefore, it is never searched again. A copy of the report generated will remain within the record management system indefinitely for retention and audit purposes.
How will the agency address error rates that are determined independently to be greater than 1%?	Idemia is verified by the National Institute of Standards and Technology (NIST), who is quoted as saying "One important exception is that some developers supplied identification algorithms for which false positive differentials are undetectable. Among those is Idemia…" Idemia has been in the top ten for both Demographic differentials and vendor accuracy in the NIST tests for several years.
How long will the agency keep the data?	The CBI's mugshot database is permanent, so all mugshots submitted to the CBI with an arrest will remain in the database. The search photo (probe) is never inserted or kept in the database. It is a simple search and purge function that takes place when searching against the database.
What is the process by which data will be deleted, if applicable?	A search and purge function is in place, as soon as a search image (probe) is done with its search of the database, it is purged from the system, it is not inserted into the database ever.

Intended Benefits

Benefits	To aid in the investigation process to help identify potential subjects of a crime.

Any data or research demonstrating these benefits:	Not addressed

Policies and Procedures

Training Procedures	Users must have training in both the Facial Software, as well as an FBI approved face comparison and identification training. CBI Standard Operating Procedure SOP#
facial recognition Use Policy	CBI Facial Identification Directive 4.30
What processes will be required prior to each use of the facial recognition software/service?	Photo in question must be of usable quality. There must be an active case number and ongoing investigation that involves the person in question in the photo. User will Login with a secure username/password.

Use Cases

When and why will facial recognition Software/services be used?	After a written request has been made to the CBI. The CBI requires that the request come from a Law Enforcement Agency email address, and that they provide an active case number, and description of the crime. CBI will then perform a Quality Control check to determine if the photo is of usable quality.
How will the facial recognition software/service be used?	By CBI employees who are trained on the Idemia Software and have successful completed Forensic Facial Training Programs.
To whom will the data be available?	Only the law enforcement agency that requested the search and retained by the CBI.
Is the technology constant or only under specific circumstances?	Not constant, it is not a live feed surveillance system. It requires a person to manually upload a photo into the system in order for it to be used. It will only be used when a crime has been committed and a law enforcement agency has a good quality photo of the suspect to search.
Where is the technology deployed or used?	The software is not deployed to a location. It is used from CBI computers to search the CBI and FBI database. It is not a surveillance system.

Outside Agency Use

If the facial recognition software/service will be used or operated by an entity on the agency's behalf, provide a description of the entity's access and all applicable protocols:	No other agency will have use of The CBI's system. They can request searches be performed; however, a CBI staff member will complete these searches.
Does the agency Intend to share access to the facial recognition software/service or the data with any third party that is not law enforcement?	No
If the answer above is yes, describe the rules and procedures by which the agency will ensure that the third party complies with the agency's use policy:	N/A

Potential impacts

Information concerning rate of false matches, potential impacts on protected subpopulations	There will never be a positive identification made, the CBI will give an investigational lead if it is believed there are enough similarities between the searched photo and the result from the database. A LEO must not use the results as more than an investigative lead.
What are the potential impacts on Civil Right & Liberties, and potential impacts to privacy and marginalized communities?	According to NIST, Idemia has the lowest variance (bias) in match rates for different genders, age, and ethnic groups and is ranked first in the 2022 NIST demographic differentials summary report.

Feedback

What is the procedure for receiving feedback from individuals and communities?	Not addressed
Procedure for Response to Feedback?	Not addressed

Attachment C

Department of Revenue, Motor Vehicle Investigations Unit, Law Enforcement Communications Center

FR: Colorado DMV

(i) the name, vendor, and version of the facial recognition service; and
Thales' Facial Comparison Solution (FCS), Biometric Investigation Workstation

(ii) a description of its general capabilities and limitations, including reasonably foreseeable capabilities outside the scope of the agency's proposed use;

Facial recognition (FR) is a fraud prevention, fraud detection, business integrity, and risk mitigation tool used by the majority of U.S. and Canadian credential issuing authorities. FR software automates the process of photo image matching and is designed to determine whether the person shown in one photograph is likely to be the same person shown in another photograph.

Facial recognition technology automates the process of comparing one photograph to other photographs to find potential matches. Facial recognition is a software application capable of potentially identifying or verifying the identity of a person by analyzing patterns based on a person's facial feature locations and contours and comparing them to those features in other photographs.

(b) (i) the type of data inputs that the facial recognition service uses;

FR software is based on the ability to recognize a face and measure the various features of the face. Every face has numerous distinguishable features that enable electronic matching. The following are examples of such features:

1. Distance between the eyes
2. Length or width of the nose
3. Depth of the eye sockets
4. Shape of the cheekbones
5. Dimensions of the mouth
6. Length of the jaw line

These features are measured to create a numerical value that represents the characteristics of the facial structure, which can be efficiently evaluated by software to produce comparison results. Templates are one such method used by some FR systems to represent the characteristics of the facial structure.

(ii) how data is generated, collected, and processed; and

Data is collected each time a customer applies for a credential within the Colorado DMV. A photograph and fingerprint are taken on most instances when getting a credential. Within the DMV system, there are potentially numerous photographs taken during previous credential issuances and stored in the system. As an example, a person can have a picture in the DMV system as a 15 or 16 year old, one when he turned

18, another at age 21 and then a picture taken every 4 years, resulting in numerous photographs taken for one person.

The FR system itself does not contain any specific applicant PII. The only PII is in the Central Server application of the DMV's system.

FR is a type of biometric software application that can identify a specific individual in a digital image by analyzing and comparing patterns.

(iii) the type of data the facial recognition service is reasonably likely to generate;

Data collected is for the sole purpose of identifying possible matches in the system with previous photographs taken, then against other photographs to determine if a person has more than one identity.

(c) a description of the purpose and proposed use of the facial recognition service, including:

A core responsibility of the credential issuing authority is to ensure that each applicant has only one identity on record. This is commonly referred to as the one person/one record principle. An FR program assists jurisdictions in ensuring that an individual has only one identity and is a proactive approach to identifying fraud before the issuance process is complete. FR systems are designed to combat identity fraud and identity theft.

(i) what decision will be used to make or support the facial recognition service; and
(ii) the intended benefits of the proposed use, including any data or research demonstrating those benefits;

Facial recognition assists credential issuing authorities in identifying suspicious activities, including:

1. An individual holding more than one credential under different names (identity fraud or multiple fictitious identities)
2. Different individuals holding a common identity and credential number (identity theft)
3. Clerical or data errors, such as attaching a photo to the wrong driver record
4. Patterns of clerical error that may indicate collusion or internal fraud

(d) a clear use and data management policy, including protocols for the following:
(i) how, when, and by whom the facial recognition service will be deployed or used;
The FR system is used by the Colorado DMV-Motor Vehicle Investigations Unit (MVIU) on a daily basis to prevent identity theft and or to help identify/compare a photograph with previously known photographs.

to whom data will be available; the factors that will be used to determine where, when, and how the technology is deployed; and other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances;
FR requests for assistance are considered for law enforcement agencies with higher profile or more serious criminal investigations, often crimes against persons or serious crimes against property. MVIU has a Law Enforcement request for assistance form, affidavit of intended use:

Offenses such as national security violations, homicide, kidnapping, sexual assault, robbery, aggravated assault, threats of bodily harm, extortion or threat to injure a person, sex offenses, crimes against children

or spouse, resisting an officer, and weapons offenses. MVIU may also assist with property crimes if/when appropriate and time allows.

(ii) if the facial recognition service will be operated or used by an entity on the agency's behalf, a description of the entity's access and any applicable protocols;

No one other than the MVIU will be conducting evaluations using the FR system.

(iii) any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose for which the facial recognition service will be used;

No one other than MVIU personnel will have access to the FR system, therefore no additional information or data will be provided.

(iv) data integrity and retention policies applicable to the data collected using the facial recognition service, including how the agency will maintain and update records used in connection with the service, how long the agency will keep the data, and the processes by which data will be deleted;

MVU keeps the following information:
Request type
Status (no match, match found)
Agency type
Requesting agency
Assignee (who worked the case from MVIU)
Type of case/Classification or reason for request (type of crime being investigated)
Compliance with interagency data sharing agreement (no assistance is provided for an immigrations related request)

These records have been kept since 2016, and are tracked by fiscal year. No records have been deleted at this time.

Any information provided by the MVIU to a law enforcement agency that makes a request for FR assistance will be a possible lead in an investigation.

(v) what processes will be required prior to each use of the facial recognition service;

LE agencies making requests for assistance will complete an affidavit for request, it will be approved if it meets the established requirements. (Offenses such as national security violations, homicide, kidnapping, sexual assault, robbery, aggravated assault, threats of bodily harm, extortion or threat to injure a person, sex offenses, crimes against children or spouse, resisting an officer, and weapons offenses. MVIU will assist with property crimes on a case by case basis, also.)

(vi) data security measures applicable to the facial recognition service, including:

(a) how data collected using the facial recognition service will be securely stored and accessed; and

(b) if an agency intends to share access to the facial recognition service or the data from that facial recognition service with any third party that is not a law enforcement agency, the rules and procedures by which the agency will ensure that the third party complies with the agency's use and data management policy;

MVIU does not share information with agencies that are not considered law enforcement. As previously stated, data collected as to LE agencies that make requests are kept by MVIU. If results of a request are shared with a law enforcement agency, that agency can only share the information with a prosecutor's office, similar to police reports that are part of an investigation.

(vii) the agency's training procedures, including those implemented in accordance with section 24-18-305, and how the agency will ensure that all personnel who operate the facial recognition service or access its data are knowledgeable about and able to ensure compliance with the use and data management policy before using the facial recognition service; and

MVIU training procedures:

Training emphasizes that FR is an investigative tool that allows the investigator to potentially identify a subject via photo image capture and image gallery development.

Users understand the basics of the security protocols in place that limit access to the FR system. Securing the system is fundamental to the protection of the PII contained in the system.
Users complete AAMVA's Fraudulent Detection and Remediation (FDR) course, along with several weeks of fraud prevention and fraudulent document review. These training classes take approximately three to six weeks of training.

Users then receive one-on-one training with the FR system which includes the review of photographs through facial characteristics and the FR system.

Training includes learning the FR system, review of the Biometric Investigative Platform User Guide, limitations on its use, ethical use and privacy, processes and procedures, application usage, and facial and fingerprint identification.

Investigators are trained in knowing that FR is an investigative tool and does not provide generate match/no match results. The results are a "possible match" that need to have a facial identification examination completed by at least one qualified staff member to make a determination as to the probability of a match.

Once trained, investigators use the FR system on a daily basis, spending at least one hour per day reviewing photographs and making decisions on those reviews.

(viii) any other policies that will govern use of the facial recognition service; (e) the agency's testing procedures, including its processes for periodically undertaking operational tests of the facial recognition service in accordance with section 24-18-304;

MVIU conducts tests on a regular basis (often several tests per week) to test the system to verify its effectiveness. Those tests include running known photographs through the FR system under an "alias name" to verify if the system yields any possible matches.

(f) information concerning the facial recognition service's rate of false matches, potential impacts on protected subpopulations, and how the agency will address error rates that are determined independently to be greater than one percent;

Results from FR are always reviewed to see if they are correctly identifying a second record under a different identity. The system is set up to show possible leads, and the human element of comparing the two photographs and fingerprints is then done to verify a potential match. It is then up to the investigator(s)/review to determine if it is a possible match.

(g) a description of any potential impacts of the facial recognition service on civil rights and liberties, including potential impacts to privacy and potential disparate impacts on marginalized communities, including the specific steps the agency will take to mitigate the potential impacts; and (h) the agency's procedures for receiving feedback, including the channels for receiving feedback, from individuals affected by the use of the facial recognition service and from the community at large, as well as the procedures for responding to feedback.

By relying on the FR system and the training involved and daily use of the system followed by human review and investigation, potential impacts to a person's civil rights and liberties is greatly reduced, if not completely eliminated. Results from the FR system are always a first step in the investigation and are never considered the final result. It is a basic tenet that potential matches from Facial Recognition will generate human examination and no other action, such as an arrest or corrective action, should be taken solely on the basis of a FR result.