Brighton Police Department
Facial Recognition Accountability Report
March 26, 2024

The Brighton Police Department (BPD) has prepared this Accountability Report pursuant to the requirements of Colorado Senate Bill 22-113, as codified in Colorado Revised Statutes (CRS) §§ 24-18-301 through 309. This Accountability Report discusses information required by CRS §§ 24-18-302(2)(a-h). Related references to statutory requirements are noted where applicable.

Technical Description & Intended Use

The BPD will activate the facial recognition functionality (hereafter referred to as the facial recognition service or "FRS"), facilitated by Rank One Computing Corporation, within the LexisNexis Lumen software platform. Lumen is an investigative application that utilizes the criminal justice information shared between the law enforcement member agencies of the Colorado Information Sharing Consortium (CISC). The FRS within the Lumen platform is provided by Denver-based, Rank One Computing Corporation's (ROC) SDK version 2.4 algorithm software *(CRS § 24-18-302(2)(a)(I)).*

This software uses state-of-the-art facial recognition technology to match the face in a user-uploaded image to post arrest "mugshot" images from a database of member agency records. 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 *(CRS § 24-18-302(2)(a)(II)).*

Lumen FRS may be used in an investigation to help identify potential suspects by comparing a single user-uploaded image ("probe image") of an unknown suspect to a collection of gallery facial images provided by the CISC. Lumen FRS 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 by comparing the unique facial structures of the probe image against the gallery of known images *(CRS § 24-18-302(2)(b)(I)).*

The Lumen FRS 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 gallery 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 FRS 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 *(CRS § 24-18-302(2)(b)(II)).*

When provided a probe image to search against a collection of gallery images, Lumen FRS returns multiple results, sorted by the highest match score generated by the ROC SDK's facial recognition algorithms, Once Lumen FRS 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 *(CRS § 24-18-302(2)(b)(III)).*

<u>Purpose and Benefits</u>

Lumen FRS is intended to enhance the BPD's investigative capabilities. 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 a human. The facial recognition algorithm will rank potential matches in a manner that allows for a simplified process of human review *(CRS § 24-18-302(2)(c)(I)).*

The intended benefit of using the Lumen FRS is to generate investigative leads for further investigation with the hope of solving unsolved crimes. By way of example, 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, the NYPD Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, with no known instance which a person was falsely arrested based on a facial recognition match.[1]

The use of FRS will benefit the Brighton Police Department in its efforts to:

- Increase public safety.
- Minimize the threat and risk of injury to specific individuals.
- Minimize the threat and risk of physical injury or liability to law enforcement and others responsible for public protection, safety, and health.

[1] https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

- Provide faster results than fingerprint or DNA as FRS can easily be used in the field with no special equipment.
- Enhance the integrity of criminal investigations and justice system processes and information.

The Lumen FRS helps solve crimes after-the-fact by matching photos obtained by a government customer of suspects, or 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 *(CRS § 24-18-302(2)(c)(II)).*

Approved BPD FRS operators will analyze the suitability of probe images prior to performing an FRS search. Lumen FRS is intended only to support BPD investigations. FRS 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 BPD, not by an automated process. This will be done on an as needed basis and used in conjunction with all other known facts and evidence as dictated by the needs of the case or circumstance. This technology does not facilitate and is not capable of “live tracking” or continuous surveillance *(CRS § 24-18-302(2)(d)(I)).*

Data Management

Access to FRS search results will be provided only to BPD members who are authorized to have access and have completed applicable training. Authorized access to the BPD facial recognition software will be granted only to BPD personnel whose positions and job duties require such access for investigative purposes. The Professional Standards Unit or designee 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 FRS *(CRS § 24-18-302(2)(d)(II)).*

The features and function of the Lumen FRS effectively reduces the risk of inadvertent access to data by BPD personnel. Lumen FRS searches only criminal justice records available to CJIS-certified law enforcement personnel of CISC member agencies.

The Professional Standards Unit or their designee will oversee Lumen FRS permissions for the BPD. The Professional Standards Unit or their designee will have the capability to audit and review any and all usage of FRS 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 *(CRS § 24-18-302(2)(d)(III)).*

All information available within the Lumen investigative platform, including the FRS, is purged according to the retention schedule and policies set by the owner agency. Thus, information made available to other CISC member agencies by the BPD is purged from the Lumen investigative platform when its retention period expires in BPD's record management system. BPD FRS data will be retained in accordance with the retention schedule applicable to the underlying criminal offense in accordance with the Municipal Records Retention Schedule adopted by the City of Brighton, and the evidence preservation requirements applicable to each case *(CRS § 24-18-302(2)(d)(IV)).*

FRS users will analyze, review, and evaluate the quality and suitability of probe images prior to performing a facial recognition search. To protect the integrity of the image, original probe images shall not be altered, changed, or modified. Any enhancements made to a probe image shall be saved as a separate image, and documented to indicate what enhancements were made, including the date and time of the modification(s). Resulting candidate images, if any, shall be manually compared with the probe image by the person conducting the comparison. In accordance with training, any candidate image that is incompatible with a probe shall be removed from the candidate image list. The user shall write a supplemental report detailing their search and results *(CRS § 24-18-302(2)(d)(V).*

Lumen is web-based software and not an application which needs to be downloaded to any City of Brighton computers. Any records exported by BPD members shall be immediately uploaded to the department's CJIS-compliant records and/or evidence management system. All information obtained from the Lumen FRS by a member of the BPD will be documented in the related investigative case report and retained in accordance with BPD records management policies. Facial recognition data is stored securely on Lumen servers, and access is limited to authorized users within Lumen. *(CRS § 24-18-302(2)(d)(VI)(A)).*

FRS data will not be shared with non-law enforcement agencies. LexisNexis/Lumen employees will not have access to and will not review BPD search history within the Lumen FRS without the express permission of BPD, or as required by law or court order. This ensures that FRS investigative data will remain confidential. BPD FRS data will not be shared with non-law enforcement agencies *(CRS § 24-18-302(2)(d)(VI)(B)).*

Training

The BPD will provide training to all authorized FRS users. This training will be arranged and documented by the Professional Standards Unit. FRS account access will not be created or provided until training has been completed. Training will include the use of

FRS technology as well as a specific review and acknowledgment of all elements of BPD policy and this Accountability Report.

In accordance with CRS § 24-18-305, FRS training will at a minimum include:

a. The capabilities and limitations of the facial recognition service.
b. Procedures to interpret and act on the output of the facial recognition service; and
c. To the extent applicable to the deployment context, the meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals.

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

a. each authorized user will access only their individual account;
b. the authorized user shall document in a case report all required information to support the authorized use of facial recognition satisfying an official law enforcement purpose;
c. how a lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system;
d. the software automatically compares the probe image to gallery images within the repository;
e. results of the comparison are returned and provide a potential investigative lead.

Updated training shall be identified with any policy revisions or updates to the FRS *(CRS § 24-18-302(2)(d)(VII)).*

The BPD will follow statutory requirements described in CRS §§ 24-18-301 through 309, in conjunction with BPD Policy 707 *(CRS § 24-18-302(2)(d)(VIII)).*

<u>Testing Procedures</u>

As required by CRS § 24-18-304(4), Rank One Computing has previously submitted the ROC SDK for testing in the following series of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) *(CRS § 24-18-302(2)(e*)):

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

The ROC SDK algorithm is regularly submitted for testing by the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT)[2]. In the NIST test for 1:N verification (probe image:multiple known images), the ROC SDK facial recognition algorithm v2.4 ranked in the top 10 globally in all investigative search accuracy results, and #8 out of 388 algorithms for frontal mugshot accuracy[3]. In the demographic effect series, the ROC SDK v2.4 ranked 11th 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)[4] *(CRS § 24-18-302(2)(f))*.

The potential impact of a false match is mitigated by a BPD investigator who must develop additional supporting evidence prior to making an arrest. With any ranked match return of possible candidates, the investigator would apply their skills, training, and experience to closely review the unique characteristics of each candidate. The investigator could then select from the list of candidates and make a possible match based on similarity of facial characteristics between the candidate and the probe image. Or the investigator may instead determine that none of the candidates from the list of results are a match *(CRS § 24-18-302(2)(g)).*

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. By way of example, statistics provided by the NYPD (the largest PD in the nation) show that the agency uses facial recognition tens of thousands of times each year without a known instance of false arrest[5].

Public Feedback

An online public comment section was established on the City of Brighton Police website on March 6, 2024. This webpage allows members of the community to access the accountability report and leave feedback and comments about the facial recognition software. This webpage can be found at the following web address https://www.brightonco.gov/CivicAlerts.aspx?AID=2466.

[2] Please see full report at https://pages.nist.gov/frvt/html/frvt11.html
[3] https://roc.ai/2023/03/08/roc-ai-dominates-latest-nist-face-recognition-benchmarks/
[4] Please see full report at https://pages.nist.gov/frvt/html/frvt_demographics.html
[5] https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

Three public meetings were held to obtain feedback from the community. These meetings were advertised via social media and held at the following locations:

1. March 6, 2024 – Brighton Police Department, in person
2. March 7, 2024 – Brighton Recreation Center, in person
3. March 25, 2024 – Virtual Meeting via Zoom/Facebook Live

Community members were present for both in-person meetings, as well as the virtual meeting. Comments, feedback, and questions were accepted from both groups.

The BPD will continue to receive and consider any community feedback on its use of FRS through any method of communication, including but not limited to, US Mail, the BPD citizen comment line, or any other means of in-person or electronic communications. All comments and/or complaints will be existing performance management software as facilitated by the Professional Standards Unit *(CRS § 24-18-302(2)(h)).*