WRPD Facial Recognition Accountability Report for LexisNexis: Lumen

The Wheat Ridge Police Department ("WRPD") submits this accountability report pursuant to the requirements of section 24-18-302 of Senate Bill 22-113. WRPD intends to procure licenses for access to and use of a facial recognition system in support of law enforcement investigations. All use of facial recognition shall be for official law enforcement use only and considered law enforcement sensitive information. Per WRPD Policy 8.32, the Wheat Ridge Police Department will use this technology as an investigative lead only and will use any results in conjunction with other leads and evidence.

I. Purpose

The Wheat Ridge Police Department proposes to procure licenses for LexisNexis's facial recognition service via Lumen. Lumen uses Rank One Computing Corporation's facial recognition technology, an investigative application, to match the face in a user-uploaded image ("probe image") to faces in publicly available images ("candidate images"). It is designed to be used in ways that ultimately reduce violent crime, fraud, and safety risks and to make communities safer.

II. Program Identification and Description

Rank One Computing Corporation's ROC SDK version 2.2.1 provides the core facial recognition algorithms that are utilized in LexisNexis's Lumen product, an integrated platform leveraged by public safety analysts, investigators, patrol officers, and commanders to help solve cases faster.

The facial recognition feature in 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 candidate image.

The facial recognition algorithms depend primarily on the 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 camera, pose of the subject, and occlusions between the camera and the subject's 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.

III. Facial Recognition Data

Candidate facial image data is collected by the CISC from its member agencies, the National Law Enforcement Information Exchange (LInX), and the FBI's N-DEx national information sharing system, which are uploaded to Lumen. Images containing faces are processed into Lumen's facial recognition service.

The probe image is collected throughout the course of the investigation and uploaded by the user. 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.

IV. Proposed Use

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 leads for further investigation with the hope of solving crimes. Through a similar program, the New York Police Department (NYPD) has successfully used facial recognition to identify suspects whose images have been captured by cameras at robberies, burglaries, assaults, shootings, and other crimes since 2011. In 2019 alone, the NYPD Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, including possible matches for leads in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies with no known instances in which a person was falsely arrested on the basis of a facial recognition match.[1]

V. Data Management, Training, and Use Policy

Access to facial recognition service will be provided only to individuals within the WRPD who are authorized to have access and who have completed applicable training. Authorized access to the WRPD facial recognition service will be granted only to personnel whose positions and job duties (investigations, intelligence, and analysis) require such access. The facial recognition program manager shall grant and audit all user access following the required account approval. All facial recognition service users shall be required to have individual access for use of the facial recognition service.

The department may share facial recognition data or requests with any government entity that presents an authorized law enforcement or public safety purpose. External data sharing or requests shall be at the approval of the facial recognition manager or designee documented via the RFI process. Any data sharing or request shall abide by the WRPD facial recognition policy. The department assumes no responsibility or liability for the acts or omissions of other agencies.

Facial recognition data is stored securely on Lumen servers and access is limited to authorized services within Lumen. Images accessed by the WRPD for facial recognition searches not maintained or owned by the WRPD are subject to the retention policies of the respective enrollment databases authorized to

[1] City of New York. (n.d.) *NYPD Questions and Answers Facial Recognition*. https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

maintain those images. Candidate images owned by the WRPD (i.e., WRPD booking photos) are already uploaded to Lumen in connection with CISC. The current data retention policy regarding WRPD booking photos mirrors the retention policy for the level of crime associated.

Training will be provided to all authorized users of the facial recognition service. This training will be arranged and documented by the WRPD 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 the facial recognition service and a specific review and acknowledgment of all elements of the WRPD facial recognition policy.

Approved facial recognition service users will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face, level of detail, illumination, resolution, size of the face image, and other factors affecting a probe image 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. Prior to completing the facial recognition investigation, a peer review process shall be implemented following the development of candidate images. The goal of this review process is to provide an additional level of consistency and control with respect to the application of standardized training practices.

VI. Testing Procedures, Accuracy, and Impact

In accordance with subsection (4) of the Colorado Revised Statutes Section 24-18-304, Rank One Computing submits the ROC SDK for testing in the following ongoing series of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Tests (FRVT):

FRVT 1:1 Verification (https://pages.nist.gov/frvt/html/frvt11.html)

FRVT 1:N Identification (https://pages.nist.gov/frvt/html/frvt1N.html)

FRVT Quality Assessment (https://pages.nist.gov/frvt/html/frvt_quality.html)

FRVT Demographic Effects (https://pages.nist.gov/frvt/html/frvt_demographics.html)

FRVT Paperless Travel (https://pages.nist.gov/frvt/html/frvt_paperless_travel.html)

FRVT Presentation Attack Detection (https://pages.nist.gov/frvt/html/frvt_pad.html)

Following the FRVT 1:1 Verification testing, ROC SDK's version 2.2 ("rankone_013") matched Visa photos with 99.6% accuracy, mugshots with 99.7% accuracy, Visa Border photos with 99.7% accuracy, and Border photos with 99.4% accuracy.

According to the FRVT Demographic Effects testing, ROC SDK'S version 2.2 ("rankone-013") had an FMR (False Match Rate; the probability that a single impostor attempt is incorrectly accepted as a genuine match)[2] range of 0.01% to 3.608%. The lowest FMR, 0.01% (0.00010) was for females, age 12-20, from Eastern Europe and the highest FMR, 3.608% (0.03608) was for females, age 65-99, from West Africa. The algorithm had an FNMR (False Non-Match Rate; the probability that a single genuine attempt fails to match) range of 0.17% to 0.25%. The lowest FNMR, 0.17% (0.0017) was for individuals from Central America and the highest FNMR, 0.25% (0.0025) was for individuals from West Africa.

In the unlikely event of a false match receiving a high match score from the ROC SDK, the false match could appear high on the ranked list of candidate matches. However, the impact of this, including on protected subpopulations, is mitigated by the WRPD policy requiring the person conducting the search to review potential match candidates and closely examine the unique facial characteristics of each potential candidate on the list in comparison with the probe image, as well as the policy requiring peer review of any potential matches identified by the initial examiner. Additionally, as policy states, facial recognition results can only be considered as an investigative lead and must be corroborated with further investigation and evidence. The Center for Strategic and International Studies (CSIS) makes note that "the point is to return a broad range of potential candidates of whom the vast majority, if not all, will be discarded by operators".[3]

As indicated in the policy, an audit shall be conducted annually to identify any unlawful or out-of-policy use of the facial recognition service. As a result, use of the facial recognition service for "fishing expeditions" or the monitoring of persons engaged in lawful activities is curtailed.

Additionally, the WRPD has clear guidelines set forth in Policy 9.36: Biased Based Policing regarding actions against traits involving a particular group.

For the reasons identified above, usage of the facial recognition service in Lumen is unlikely to have a negative impact on the civil rights and liberties of protected subpopulations or marginalized communities.

VII. Facial Recognition Service Complaints and Feedback

To date, Rank One Computing Corporation has not received a complaint or report of bias regarding any version of the ROC SDK. As mentioned previously, NIST FRVT testing has explored demographic performance differentials with the results made publicly available on its website.

The Wheat Ridge Police Department held three public meetings to solicit feedback from the community. Ongoing community concerns and feedback will be welcomed through the Professional Standards Unit.

[2] Tilton, C (2015, January 12). *Biometric Authentication*. National Institute of Standards and Technology. https://www.nist.gov/system/files/applyingmeasurementscienceworkshopjan12_13_2016.pdf

[3] Crumpler, William (2020, April 14). *How Accurate are Facial Recognition Systems – and Why Does It Matter?* Center for Strategic & International Studies. https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it