Lovely-Frances Domingo
lovely.f.domingo@gmail.com
UC Berkeley Information School PhD Applicant Fall 2021
Sample Writing – Written for Urban Design & Planning "Tech in Cities" course

Use of "Facial Recognition" Analysis Software by Law Enforcement in Seattle and San Diego

Executive Summary

The appetite for technology-driven solutions in law enforcement has grown over the years, coinciding with the increasing demand for operational efficiency combined with lower overhead costs for implementation. With recent advances in artificial intelligence technology, this is now possible (O'Brien and Har 2019). According to Grandview Research, a market research firm, the "facial biometrics" market is expected to grow from $136.9 million in 2018 to $375 million by 2025 (Schuppe 2019). Unlike DNA analysis, the ease of operation enables law enforcement officials to incorporate the use of facial biometric technology in their daily workflow, including solving routine crimes rather than saving the analysis tool for high-profile cases (Schuppe 2019).

Municipal law enforcement agencies have begun implementing the use of facial biometric analysis systems, such as the Seattle Police Department (2014) and the San Diego Police Department (2013). Both the design and implementation of facial biometric analysis tools vary per vendor, institution, and state which makes it difficult for the public and policy makers to understand, therefore has largely been unregulated (Garvie, Bedoya and Frankle 2016). As a result, the lack of regulation and oversight can lead to misuse and risks of violating privacy, civil liberties, and civil rights (Garvie, Bedoya and Frankle 2016).

The purpose of this document is to compare and contrast publicly accessible policies for the Seattle Police Department (SPD) and the San Diego Police Department (SDPD) regarding facial biometric analysis systems. Both SPD and SDPD employ facial biometric analysis technology "after-the-fact," (Garvie, Bedoya and Frankle 2016) which means that the analysis is done using preexisting artifacts, such as a digital image, rather than in "real-time," (Garvie, Bedoya and Frankle 2016) which analyzes facial biometrics while capturing live video footage of an individual(s). Each policy will be analyzed to determine whether there are any statements to indicate appropriate measures to minimize misuse and violations of privacy, civil liberties and civil rights against communities of color. This analysis will look at each of the policy's approach on:

- Access Control – who can access the facial biometric technology
- Auditability – ability to trace request to a particular individual, statements about compliance requirements
- Data Management – referring to data lifecycle, length of data retention, destruction of data after use, etc.
- Privacy – mentions of privacy, data obfuscation (as necessary), minimization of data collection, limitation of access

- Bias training and equity – Referring to training that introduce the possibility of personal biases informing and/or influencing the use of the system that may negatively impact specific subset of populations

Seattle Police Department: 12.045 Booking Photo Comparison Software

The Seattle Police Department (SPD) began using facial biometric analysis technology in 2014. The *SPD Title 12 – Department Information Systems - 12.045 Booking Photo Comparison Software* policy regulates the use of any biometric analysis software by SPD while protecting privacy (Seattle Police Department 2019). The policy broadly defines biometric analysis to include "facial or human recognition" (Seattle Police Department 2019). In doing so, the definition broadly captures other features that can be used to identify individuals, which includes tattoos, gait, etc.

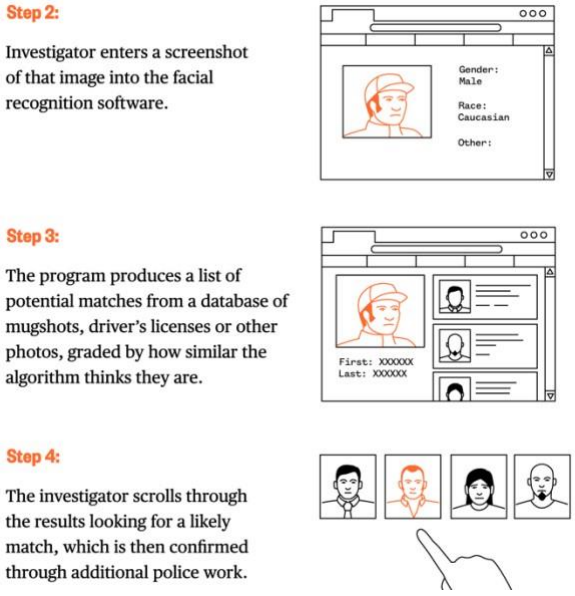

Figure 1. Example of how a BPCS trained personal may use the system (Schuppe 2019)

Access Control

Only department trained personnel are authorized to use BPCS at designated BPCS workstations (See Figure 1). BPCS personnel are required to maintain logs of all inquiries. Officers/Detectives do not have direct access to BPCS workstations. They must follow standard operating procedures of filing inquiries and describing incident in order to establish reasonable basis for the request. Criteria for requests must be satisfied in order for inquiries to be performed.

Auditability

Logs of inquiries are maintained at BPCS workstations. Usage of BPCS is audited on an annual basis. The policy mentions that Compliance Personnel is responsible for auditing all BPCS usage. However, based on this policy, it is not clear whether auditing and compliance is subject to internal auditor or if SPD will bring in a third-party auditor to ensure compliance, or both. It is also not evident in the policy as to what compliance framework or criteria will be used to evaluate the auditing process and whether or not there are any significant repercussions involved. BPCS is likely subject to comply with federal information security policy (Seattle Police Department 2019).

Data Management

Only specific personnel will have access to BPCS work stations and all data associated with BPCS request will be kept in the system for 42 months. Within this policy, there is no clear definition for what constitutes 'data.' There is reason to believe, perhaps, that 'data' mentioned in the policy is related to Criminal Justice Information (CJI) which is outlined in 12.111 – Use of Cloud Storage Services, which

defines 'data' as "biometric, identity history, biographic, property, and case/incident history data" (Seattle Police Department 2017).

Privacy

The policy provides no direct access to the BPCS for detectives/officers and there are set access controls to ensure that only a small subset of trained personnel have access to sensitive personal information.

Bias Training or any reference to reducing bias in usage

While not directly mentioned in the policy, 12.045 Booking Photo Comparison Software, the SPD manual refers to Title 5 – Employee Conduct – 5.140 on Bias Policing.

San Diego Police Department DP 1.50 Facial Recognition

The San Diego Police Department employs a procedure document governing the use of facial recognition technology, DP 1.50 – Facial Recognition (dated June 19, 2015), which defines purpose, scope, definitions, procedures and restrictions related to the use of facial recognition software by SDPD officers. The procedure applies to all members of the SD Police Department. According to DP 1.50, the purpose of facial recognition technology is to assist law enforcement officers identify individuals who have been "lawfully detained or otherwise subject of a criminal investigation" (Muckrock 2015) if they cannot provide proof of their identity.

Unlike the Seattle Police Department's Booking Photo Comparison Software, which is limited to specific workstations and only accessed by trained personnel, San Diego's facial recognition system is comprised of a mobile, cloud-based application, called Face First, used by SDPD officers directly. It's accessible, convenient, and powered by cellular network. A police officer submits an inquiry through the Face First application using an image taken of an individual, or "probe image" (Muckrock 2015). The application queries the Tactical Identification System (TACIDS) for potential matches based on "enrolled images" (Muckrock 2015) or images present in various regional databases such as booking images (or mug shots), existing warrants, driver's license image, etcetera (See Figure 2).

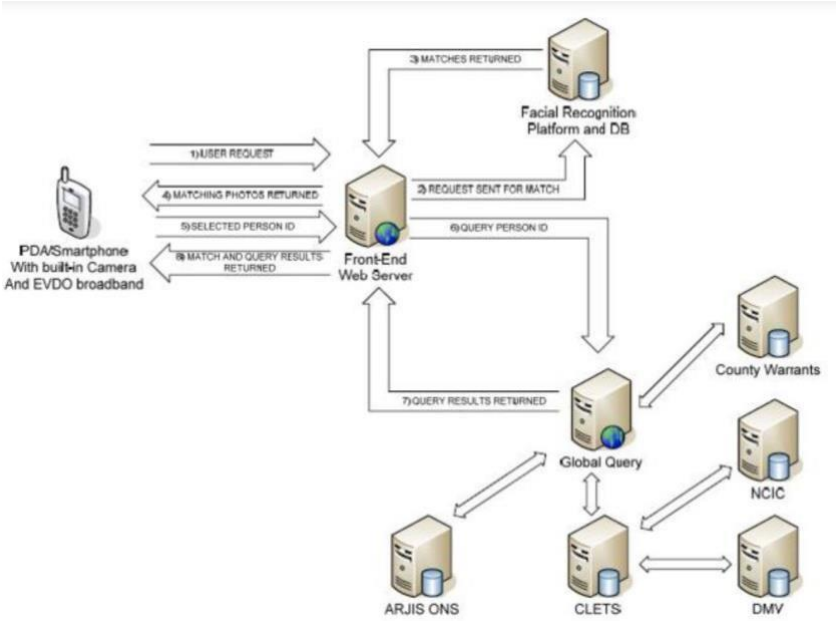

Figure 2. Process for when an officer submits a photo into the TACIDS Facial Recognition Platform or database in San Diego (Schuppe 2019)

The use of Face First technology has increased since SDPD implemented the technology in 2013. There were 134 devices among 67 certified law enforcement personnel. In 2016, there were 433 devices used by 991 law enforcement personnel in San Diego County (Schuppe 2019).

Access Control

The "Face First" application is based on the Android operating system. With mobile devices and applications, there is some concern for device security and visibility on who is able to access the software. There are currently no specific statements in place to ensure that only authorized personnel are capable of accessing information, nor is it possible to vet the purpose of each individual inquiry done through the application.

Auditability

The current policy at the time of this analysis shows no statement or mention of how inquiries may be audited or reviewed.

Data Management

Once the analysis request for facial recognition has been completed, the image used for comparison ("probe image") is manually deleted from the device that was used to capture the image. However, there is no mention of time frame for data retention and data destruction, enforcement or compliance to this procedure in the policy.

Privacy

There is no statement about privacy in the policy. If an individual is unable to procure personal identification (ID, driver's license, and other identifying documentation), is under arrest for a crime or is being detained as a suspect or for criminal investigation, the officer involved may take the photograph without any mention of consent.

Bias Training or any reference to reducing bias in usage

While the purpose of the document can be construed as an example of an 'acceptable use policy,' it does not provide specific statements or procedures for gaining consent or mention of training or connected policies to minimize personal bias and how it may influence reasonable suspicion to use the facial recognition application.

Recommendations

Privacy advocates, civil liberties and civil rights organizations such as the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) for both Washington state and California have raised concerns about the use of facial biometric analysis technology. The EFF have published extensive research and white papers illuminating the implications of the use of facial biometric analysis software on privacy and the impact it has on communities of color. The EFF noted that a combination of "misidentification of African Americans and other minorities [by face recognition] … with well-documented racially-biased police practices mean that people of color will likely shoulder the burden of face recognition inaccuracies" (Lynch 2018). Imperfect and already racially informed policing can promote a very chilling effect for residents in both Seattle and San Diego, particularly for communities of color.

The Seattle Police Department *Title 12 – Department Information Systems - 12.045 Booking Photo Comparison Software* policy establishes reasonable controls for the use of facial biometric analysis technology; however, the policy must explicitly mention the risks in which this technology may be informed by already existing racially-biased police practices. The Seattle Police Department has had a history of disproportionate policing against communities of color compared to white subjects [through the use of] Propensity Score Matching, which is "an imperfect method that matches situations seen as similar in an attempt to account for confounding factors" (Kroman 2019). Propensity Score Matching combined with facial biometric analysis software can exacerbate an already "imperfect method" at a much larger scale.

The same can be said for current policing practices in San Diego that is now at risk of being perpetuated using Face First application technology but much higher risk due to its mobility and convenience (using a smartphone or networked device). There is currently no oversight on how this mobile application should be used while in the field. A San Diego State University study reported that SDPD blacks, Hispanics, and Pacific Islanders were more likely to be subject of searches and field interviews than white subjects (City News Service 2016). As such, there needs to be mechanism to determine if the technology is being disproportionately used against one subset of the population. Appropriate set of access controls, audit & compliance, and setting data management procedures in the policy must be adopted to minimize risks of misuse and violations.

Bibliography

City News Service. 2016. *KPBS.* November 25. Accessed May 11, 2019. https://www.kpbs.org/news/2016/nov/25/san-diego-police-more-likely-to-search-blackand/.

Garvie, Claire, Alvaro Bedoya, and Jonathan Frankle. 2016. *Perpetual Line Up: UNREGULATED POLICE FACE RECOGNITION IN AMERICA.* October 18. Accessed May 11, 2019. https://www.perpetuallineup.org.

Jones, Tom, and Lynn Walsh. 2016. *Use of Facial Recognition Software By San Diego Law Enforcement Increasing.* May 5. Accessed May 11, 2019. https://www.nbcsandiego.com/investigations/Use-of-Facial-Recognition-Software-BySan-Diego-Law-Enforcement-Increasing--378006081.html.

Kroman, David. 2019. *Crosscut.* May 1. Accessed May 11, 2019. https://crosscut.com/2019/05/report-shows-seattle-police-enforcement-still-disparatealong-racial-lines.

Lynch, Jennifer. 2018. *Face Off: Law Enforcement Use of Face Recognition Technology* . February 12. Accessed May 2019. https://www.eff.org/wp/law-enforcement-use-facerecognition.

2015. "Mobile Biometric Technologies Records Request (San Diego Police Department)." *Muckrock.* August 9. Accessed May 11, 2019. https://www.muckrock.com/foi/san-diego56/mobile-biometric-technologies-san-diego-police-department-20388/.

Muckrock. 2015. "Mobile Biometric Technologies (San Diego Police Department) Records Request." *Muckrock.* August 9. Accessed May 11, 2019. https://www.muckrock.com/foi/san-diego-56/mobile-biometric-technologies-san-diegopolice-department-20388/.

O'Brien, Matt, and Janie Har. 2019. May 13. Accessed May 11, 2019. https://abcnews.go.com/Technology/wireStory/san-francisco-ban-police-city-facialrecognition-62997265.

Schuppe, John. 2019. *NBC News.* 11 May. Accessed 12 May, 2019. https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routinepolicing-tool-america-n1004251.

Seattle Police Department. 2019. "12.045 - BOOKING PHOTO COMPARISON SOFTWARE." *Seattle Police Department Manual.* May 7. Accessed May 11, 2019. http://www.seattle.gov/police-manual/title-12---department-information-systems/12045--booking-photo-comparison-software.

—. 2019. "12.050 - CRIMINAL JUSTICE INFORMATION SYSTEMS." *Seattle Police Department Manual.* May 7. Accessed May 12, 2019. http://www.seattle.gov/police-manual/title-12--department-information-systems/12050---criminal-justice-information-systems.

—. 2017. "12.111 - USE OF CLOUD STORAGE SERVICES." *Seattle Police Department Manual.* March 1. Accessed May 11, 2019. http://www.seattle.gov/police-manual/title-12--department-information-systems/12111---use-of-cloud-storage-services.