Technology & Innovation Ad Hoc Committee
Facial Recognition Technology Research
July 28, 2021

CITY OF LONG BEACH

Facial Recognition Technology Research

Agenda

- Overview
- SWOT
- Best Practice Research
- Recommendations
- Discussion

Overview: Scope

- The City of Long Beach, in order to implement the recommended actions in its adopted Racial Equity and Reconciliation Report, is researching and evaluating Facial Recognition Technology (FRT), which aligns with Goal 3, Strategy 3, Potential Action E of the Report:
    - *"Explore the practice of facial recognition technology and other predictive policing models and their disproportionate impacts on Black people and people of color by reviewing evidence-based practices."*
- For the purpose of this specific action, the Technology and Innovation Commission (TIC) in partnership with Staff from the Technology and Innovation Department (TID) focused specifically on FRT.

Overview: Process

- **January 2021:** An ad hoc subcommittee of the Technology and Innovation Commission was formed to support the FRT aspect of the Racial Equity and Reconciliation Initiative.
- **March 2021:** Research and analysis covering the strengths, weaknesses, opportunities, and threats (SWOT) of FRT was conducted by Commissioner Vinzant. Since March, the subcommittee also began reviewing other city approaches and best practices and lessons learned on FRT.
- **April 2021:** City staff met with the police department to share the subcommittee's initial research. At this meeting, PD informed city staff it was using FRT and had issued its own FRT policy, Special Order on Facial Recognition Technology, in March 2021.
- **April 2021:** At TIC's meeting, a privacy expert from the Future of Privacy Forum provided an overview of the approaches other jurisdictions are taking on FRT.

Overview: Terms

What is Facial Recognition Technology (FRT)?

- It is an automated or semi-automated process that assists in identifying or verifying an individual, or in capturing information about an individual, based on the physical characteristics of an individual's face.
  - Photos, video, and real-time video surveillance are used

- Facial recognition systems use computer algorithms to pick up specific, distinctive details about a person's face.
  - Data about a particular face is often called a face template and is distinct from a photograph because it's designed to only include certain details that can distinguish one face from another

SWOT: Strengths

There are legitimate uses of FRT in policing, including:

- FRT is primarily used to assist police in identifying or eliminating potential suspects of criminal activity
- Use of FRT along with other electronic tools can help police respond quickly to complex events such as terrorism
- It is used to prevent human trafficking and in identifying and reuniting missing children with their families
- FRT can be used as an identifier in helping speed up the identification process for deceased people while ensuring victims are treated with dignity and respect

SWOT: Weaknesses

There are numerous weaknesses of FRT, ranging from demographic differences in accuracy to reliability concerns and human error to bias and privacy concerns:

- Demographic differences in accuracy rates of FRT have been highlighted in academic studies, a NIST study, and other reports
  - MIT Media Lab study researcher Joy Buolamwini found that FRT failed up to 1 in 3 times when classifying the faces of Black women
  - Black men such as Robert Williams have been mistakenly identified by FRT and wrongfully arrested
- Reliability issues of FRT have been raised from police chiefs to ACLU lawyers
- Human error is a common problem, including reviewers' technical use of FRT and innate demographic differences and/or personal biases that may impact use of FRT
- Absence of sufficient human backup identification and policies that rigorously address necessary data, civil liberties, and privacy protections related to FRT

SWOT: Opportunities

If identified gaps or issues related to FRT are addressed, and the necessary new policies, technologies, and resources are implemented, then it may be possible for a police department to deploy FRT in a legal, ethical, and equitable manner

- Due to Europe's strict privacy law (GDPR), a review of FRT vendors operating in that environment may provide useful best practices for building strong data protection practices into police and/or city use of surveillance technologies and potentially FRT
- Taking the time to build trust of the public in police's use of surveillance technology through "communication and transparency" is considered a crucial step
- Police departments can choose to build out the ecosystem needed to support a police department's ethical, equitable, and legal use of surveillance technologies such as FRT, which requires investment of new budget, training, and resources

SWOT: Threats

If identified issues related to FRT are not effectively addressed, it could lead to erosion of public trust and claims that a city or police department is using racially biased and harmful technology

- There are a number of accountability concerns with police use of FRT due to: lack of reporting accountability of sources and methods used by private FRT companies to build their FRT databases (e.g., Clearview AI); and lack of transparency around and independent auditing of police use of surveillance technologies, including FRT
- Even with perfect use of FRT, if a police department has not provided rigorous and ongoing bias trainings, it may lead to negative unintended consequences, including claims of biased policing
- If police use of FRT leads to a mistaken arrest or if the public perceives police have not fully accounted for their privacy concerns, it can worsen police-public relations

Overview: Best practice research

Policy approaches on FRT by local governments are largely split between bans of FRT and surveillance ordinances:

- Roughly 17 bans against FRT that are mainly focused on police and government use with several in tandem with surveillance ordinances
- About 19 surveillance ordinances in place that are technology-neutral frameworks based on expected privacy review, focused on government use
  - All of these surveillance ordinances were based on the ACLU's program, Community Control Over Police Surveillance (CCOPS) guiding principles
- Also, some cities have responded by creating advisory groups, task forces, and studies, which may be tech-specific or general-purpose bodies

Overview: Best practice research

Notable highlights from discussions with other cities about FRT include:

- **Seattle** has a surveillance ordinance with comprehensive staffing to support it, but is now moving towards a ban on FRT
  - FRT is not currently used due to administrative burden and potential liability
- **Portland (OR)** banned FRT with some exceptions due to bias inherent within this technology and the lack of independent entities to certify algorithms and the technology as bias-free
- **Oakland** has a surveillance vetting framework for surveillance technology, an effort led by its Privacy Commission, but the city has also banned FRT
  - Surveillance ordinance focuses on assessment of and approval of technologies with use and impact policies; annual reporting requirement

Summary: Research

Research shows that generally, people are supportive of improved technology for police. The Pew Research Center found in 2019 that:

- 56% of Americans trust law enforcement agencies to use facial recognition responsibly
- 59% of the public says it's acceptable for police to use facial recognition in assessing security threats in public places
- Another Pew study from 2017 found 93% of the public is in favor of the use of body cameras by police to record interactions

Yet, FRT has proven to be inadequately equipped to identify faces, particularly of Native American, Black, and Women groups.

FRT does not yet have the accuracy needed to be an asset to City efforts.

Proposed Recommendations

Current facial recognition technologies lack appropriate accuracy and reliability and pose substantive and unequal risk to BIPOC communities due to inherent algorithmic biases and unaddressed privacy and equity issues.

As such, the subcommittee suggests TIC consider the following proposed recommendations:

- **Short-term Action:** Recommend that City Council ban the use of facial recognition technology by the City with possible consideration of narrowly defined and limited exception(s).*
- **Near-term Action:** Recommend that City Council adopt a surveillance vetting framework ordinance for potential acquisition and use of surveillance technology by the City.

**Please note that the subcommittee gave serious consideration to recommending a moratorium but changed course after conducting best practices research.*

Discussion Questions

The subcommittee looks forward to a robust discussion within TIC and hearing views from members of the public

1. Do you have any questions on the presentation, research and/or memo?
2. How are the suggested recommendations resonating with you? Do you have suggestions? Any changes?
3. How does our understanding of FRT change (if at all) when applying the following lenses:
   - Racial Equity and Justice
   - Privacy
   - Public Safety
   - Civil liberties and civil rights
4. How do we meaningfully capture and center the views, ideas, and solutions from the most impacted community members—BIPOC communities—by FRT?