NLC NATIONAL LEAGUE OF CITIES
CENTER FOR CITY SOLUTIONS

FACIAL RECOGNITION GUIDE FOR CITIES

EXECUTIVE SUMMARY

Facial recognition, the process by which peoples' faces captured in video footage or photographs are compared to a database of known individuals to find a likely match and identify an unknown person, is an emerging technology that warrants careful consideration, balancing privacy and transparency against potential effectiveness and efficiency. Facial recognition technology is becoming more common in both the private and public sectors in the U.S. Grocery stores use it to track customers' shopping habits. Many people use it to unlock their cellphones. Police departments use it to determine the identity of suspects from video camera footage.

> Like many other emerging technologies, facial recognition technology has become widespread before public policy discussions have occurred in communities across the country.

Facial recognition systems will generally require a source of video footage or photographs to be analyzed, software to process captured images for comparison using algorithmic analysis and databases against which those images can be compared. The effectiveness of facial recognition systems is dependent on a good quality image of an unknown individual, an algorithm that has been trained on a wide variety of human faces and a strong definition of what the software should consider as a match between the unknown face and the database.

Although there are a variety of applications for facial recognition technology, it is commonly deployed in public safety settings in cities, towns and villages. However, there are significant differences in how these facial recognition systems are used across cities and across law enforcement agencies when it comes to factors like use for investigative purposes or real-time surveillance, the source of comparison databases and evidentiary requirements before use.

There are benefits and risks for government entities' use of facial recognition. Public safety officials state that facial recognition systems create efficiencies and provide investigative leads that would not exist otherwise. With the proper guardrails in place and sufficient checks and balances guiding the confirmation process, facial recognition technology can identify suspects with fewer policing resources. This could be particularly helpful when local governments face reduced revenues, funding and resources due to COVID-19.

> Facial recognition can bring efficiencies into the investigative process.

However, facial recognition systems also reflect racial, gender and age bias in the data sets on which they are trained. Misidentifying people from information generated by a facial recognition system can have real-life negative effects. As with any emerging technology, the lack of legal guidance can make it difficult for cities to ensure that organizations use facial recognition technology in the best way and do not risk legal action or liability.

A few states have passed legislation limiting the scope of facial recognition usage, including three states that have banned law enforcement from using facial recognition on body cameras (California, New Hampshire and Oregon). In its 2019–2020 session, the U.S. Congress held hearings and proposed bills related to facial recognition, but none of these proposed laws would directly impact local law enforcement. Federal or state legislation may eventually preempt or nullify local legislation. However, cities are taking the lead in shaping facial recognition policy. Not every city that now uses facial recognition has voted on a policy to govern its use. Some cities have developed policies that limit the scope of law enforcement's permitted uses. Several cities have banned the technology entirely.

HOW SOME CITIES REGULATE FACIAL RECOGNITION FOR GOVERNMENT USE

☑ LIMITED SCOPE OF USE

New York, New York
Detroit, Michigan
Seattle, Washington
Lawrence, Massachusetts
Davis and Palo Alto, California
Nashville, Tennessee
Pittsburgh, Pennsylvania

☒ BAN

San Francisco, Oakland and Berkeley, California
Boston, Brookline, Cambridge, Northampton, Easthampton and Somerville, Massachusetts
Portland, Oregon
Portland, Maine
Jackson, Mississippi
New Orleans, Louisiana
Madison, Wisconsin
Minneapolis, Minnesota

*Only includes examples with publicly available policies

Cities have a responsibility to their communities to thoughtfully explore emerging technologies that have the potential to aid the greater good. The conversation around facial recognition is a particularly sensitive one given the imperfections with the technology itself and the way in which it is frequently being implemented and used behind closed doors. By following these recommendations, cities could better facilitate facial recognition technology discussions publicly in their communities.

1. Engage with residents to develop policies, and be transparent about facial recognition use.

- Require elected officials to vote on any decision to use facial recognition technology before law enforcement can implement it.
- Insist on community input in a public forum (e.g., by hosting town hall meetings) before voting on a decision to use facial recognition.
- Collaborate with a diverse group of non-governmental organizations and stakeholders when designing a policy, in order to achieve broader community buy-in.
- Consider establishing a citizen overview board, with real authority and budget, that regularly reports on the state of biometric surveillance in the city.
- Make any facial recognition use policies publicly available online.
- After a facial recognition policy has been adopted, establish a public awareness campaign in order to educate citizens on the scope of the technology and the city's use policy.
- Ensure that the public can submit complaints about any issues they encounter related to the government's use of facial recognition.
- Disclose to the public the locations of cameras deployed in public areas if those cameras provide imagery to be used in facial recognition.
- Require regular internal auditing by independent ombudsmen to ensure that the system is working as intended and not discriminating against certain groups.
- Consider requiring recurring votes to reauthorize a facial recognition use policy annually or biannually.
- Conduct an annual or biannual review of the facial recognition system's effectiveness, and ensure elected officials' access to the review (e.g., how often it is used and assists investigations).

2. Establish a training program for law enforcement and other users of a facial recognition system.

- Require that all officers who are cleared to use the technology be extensively trained on how to use it. Make sure that officers are aware of the probabilistic nature of the technology.

- Establish a high probability threshold for matches before the technology can be used in an investigation.

- Require double-blind confirmation before a match is determined. Two different officers must independently review and confirm the match. Retain thorough records of use of the system and approvals.

- Prohibit officers from making an arrest based solely on a facial recognition match.

- Set a high standard for the quality of photos that officers can run through a facial recognition search.

- Forbid officers from using police sketches or celebrity doppelganger photos in lieu of real photos of suspects.

- Require implicit bias training to ensure that bias does not influence the ways in which officers use the technology.

- Educate officers on the legal consequences of misusing the technology, including violations of constitutional rights and, depending on the state, tort violations.

- Require that officers who deliberately misuse the technology be swiftly held accountable by the department or city, including through suspensions or firings, regardless of outside lawsuits.

3. Limit the scope of facial recognition use to reduce the risk of misidentifications and privacy violations.

- Require that officers have at least individualized, reasonable suspicion of a crime before running a suspect's photos through a facial recognition database for identification purposes.

- Limit the use of facial recognition to investigations of violent offenses

- Limit the use of real-time public surveillance to a narrow set of situations involving life-threatening emergencies or major violent crimes such as terrorism, and ensure that law enforcement obtains a warrant based on probable cause before conducting such surveillance. If feasible, consider installing a system that alerts law enforcement only when surveillance cameras capture a suspect's face, which will reduce privacy violations of innocent people.

- Consider the pros and cons of using either mug shot photos or driver's license photos as the source of a facial recognition database.

  - A database of driver's license photos includes more people and, thus, may be more likely to include a suspect. Furthermore, it is not skewed toward subsections of the population, particularly people of color, that are overrepresented in mug shot databases. However, every driver in a state will be vulnerable to a false identification. If a city wants to use driver's licenses as the source of a photo database, consider waiting for state legislature approval so that citizens are aware that their photos are used in this way.

  - Mug shot databases are smaller and may be less likely to include a suspect. Certain population groups, particularly people of color, are overrepresented in these databases. However, if properly updated to remove people found to be innocent, these databases include only people convicted of a crime and who have, thus, already lost some liberties. If a city wants to use mug shots as the source of a photo database, ensure that the database includes only people convicted of a crime and not those who were exonerated or never charged.

4. Institute rigorous standards for data storage and cybersecurity to ensure protection of citizens' biometric data.

- Delete any photo or video footage that has been analyzed with facial recognition technology and is not pertinent to an ongoing investigation.

- Regularly scrub databases of mug shot photos to exclude people found innocent or against whom charges were dropped.

- Restrict the length of time that data is stored to reduce the risk of a data breach.

- Restrict storage of biometric data to a single database to minimize the number of entry points potentially vulnerable to hackers.

- Require all employees who access the system to follow basic cybersecurity hygiene practices, including, at a minimum, establishing two-factor authentication on their accounts. Restrict permitted access both in written policies and as a technical matter.
- Ensure state-of-the-art forensic tracking of any use of a facial recognition system before it is deployed.
- Create policies and systems governing and constraining sharing of facial recognition results within city hall or police departments, to limit opportunities for non-approved uses of the technology.

5. Follow best practices for drafting contracts to ensure accuracy and reduce legal risk.

- Contracts with facial recognition vendors should require the vendors to regularly test their algorithms for both accuracy and racial bias.
- Require vendors to certify that their technology's algorithms use a demographically representative training set. These certifications should be updated regularly.
- Organizations using cameras provided by contractors should require the cameras to meet high photo-quality standards.
- Remove contract language in which a vendor disclaims responsibility for the facial recognition algorithm's accuracy.
- Pay close attention to the wording of indemnification clauses, to ensure that the city does not adopt too much liability for the vendor and that the vendor is held accountable for its errors. This is particularly important in states that have biometric privacy laws under which private companies can be held liable.
- Before signing a long-term contract with a vendor for a full facial recognition program, consider signing a short-term contract for a pilot program to determine whether facial recognition is useful and worthwhile.

You can find more information on what facial recognition is, how cities are using it, how cities are regulating it and how city officials can best approach public conversations about facial recognition use in their communities in NLC's Facial Recognition Report.