
NLC
NATIONAL
LEAGUE
OF CITIES
CENTER FOR CITY SOLUTIONS
FACIAL
RECOGNITION
REPORT

NATIONAL LEAGUE OF CITIES
CENTER FOR CITY SOLUTIONS

About the National League of Cities

The National League of Cities (NLC) is the voice of America's cities, towns and villages, representing more than 200 million people. NLC works to strengthen local leadership, influence federal policy and drive innovative solutions.

NLC's Center for City Solutions provides research and analysis on key topics and trends important to cities, creative solutions to improve the quality of life in communities, inspiration and ideas for local officials to use in tackling tough issues, and opportunities for city leaders to connect with peers, share experiences and learn about innovative approaches in cities.

Authors

Lena Geraghty, Program Director of Urban Innovation, Center for City Solutions

Acknowledgements

The authors would like to acknowledge:

William Ossoff and **William Wright**, Harvard Law School Cyberlaw Clinic Students, and Professor **Susan Crawford** for their research and contributions to this report.

Angelina Panettieri, Legislative Director of Information Technology and Communications, for her research and policy guidance.

Cooper Martin, Director of Sustainability & City Solutions, Center for City Solutions, for his guidance and review of the report.

Erin Peterson, Program Specialist for NLC-RISC, for reviewing the report.

Ashleigh Imus for copyediting.

Table of Contents

Facial recognition guide for cities

As cities, towns and villages embrace emerging technologies and determine their use in local government operations, elected officials will have to navigate difficult conversations and decisions, balancing privacy and transparency with efficiency. 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.

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.

Cities are at various stages of regulating use of facial recognition, wrestling with challenging conversations about both government and private-sector use of this technology. This report details 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.

What is facial recognition? How does it work?

Facial recognition technology works by comparing images of an unknown person's face with a database of known individuals' faces in order to find a match and identify an unknown person. Facial recognition systems generally require three elements:

- 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.

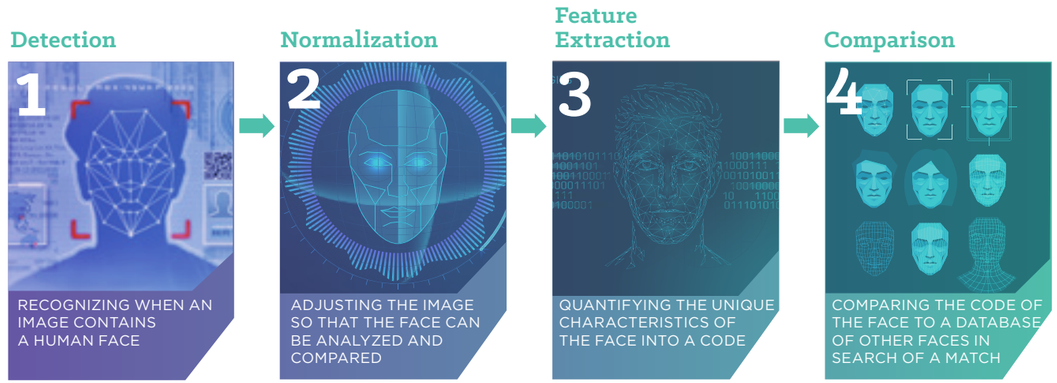
Source of video or photographs

Facial recognition technology identifies unknown people from video footage or photographs. Video surveillance is a frequent source of this imagery. Although widespread video surveillance in cities is not new, it continues to increase. Building-mounted cameras and traffic cameras are common throughout most American cities, operated by both public and private entities. Many police forces use body cameras and vehicle cameras. Law enforcement also routinely deploys surveillance cameras to scan crowds and ensure security during high-profile events. Drone-mounted cameras –– already used by some cities –– provide another source of imagery. Additionally, most personal cellular devices have cameras, allowing the public to record images and video.

Software for algorithmic analysis

A facial recognition system's central component is a set of algorithms that identifies faces within video or photographic images, extracts characteristics unique to those faces and matches these characteristics to known faces in a pre-existing database. Modern algorithms can accomplish this with a high degree of reliability. A 2014 study showed that facial recognition algorithms recognized faces more accurately than humans did within a given data set, distinguishing faces with 98.5% accuracy compared to 97.5% accuracy for the study's human participants.[1] The algorithms have grown steadily more reliable since then, reportedly achieving greater than 99% accuracy in some cases.[2]

Although there are many different algorithms and ways to apply them, the process of facial recognition generally comprises the following steps, each of which entails the application of a distinct algorithm:



Comparison data sets

The comparison phase described above relies on data sets of images of known people against which a captured image of a face can be compared. Many municipalities have access to various such data sets. Police forces generally maintain mug shot databases, and at least 26 states allow law enforcement to run searches against state databases of driver's licenses and ID photos.[3]

In general, the better populated the comparison data set is, the greater likelihood of a match. Even if facial recognition technology worked perfectly, the only way to find a match for every captured face would be to have a comparison data set encompassing the entire world's population.

How do cities, towns and villages use facial recognition?

Private vs. public use

Both the public and private sectors in cities across the country use facial recognition. Some apartment buildings have begun to use facial recognition for security purposes.[4] Some airlines use facial recognition for check-in.[5] Sports arenas and concert venues use facial recognition to monitor crowds.[6] Public and private schools around the country, including public schools in Texas City, Texas,[7] and private schools in Seattle, Washington,[8] use facial recognition both for security purposes and to ensure that suspended students do not try to sneak into school events. Boise, Idaho, has plans to use facial recognition to keep banned people out of city hall.[9] Many companies also now offer facial recognition as a central part of their consumer products. The latest version of the iPhone allows users to unlock their phones using facial recognition. Facebook also has used facial recognition for many years to suggest whom to tag in a photo. Google's Nest home security cameras now include facial recognition capabilities.[10] Amazon has also explored the possibility of installing facial recognition into its Ring home security cameras.[11] This could have implications for law enforcement; more than 400 law enforcement agencies have partnerships with Ring in which they can access the video footage captured by Ring cameras installed in private homes.[12]

Facial recognition is commonly used in public safety settings in cities, towns and villages. Many law enforcement agencies at the local, state and federal levels have deployed facial recognition to aid their investigations and more easily identify people. However, there are significant differences in how these facial recognition systems are used across cities and across law enforcement agencies:

Identification vs. surveillance

Some cities limit the use of facial recognition to identification purposes. These municipalities use facial recognition searches of a photo database to identify a suspect whose photo they already have. Some cities use facial recognition to identify a person who has already been arrested or detained in connection with a crime but refuses to identify him or herself.

Other cities conduct real-time facial recognition surveillance, in which cameras can recognize and rapidly compare faces to a database, often in search of a "hot list" of suspects. Los Angeles, California, reportedly has this real-time facial recognition capability.[13]

Driver's license photos vs. mug shots

Cities are also divided regarding the databases they use to conduct facial recognition searches. Cities such as New York City, New York and Detroit, Michigan, only use databases of mug shots, which limits the scope of searches to people previously processed by the criminal justice system. Other cities, including Lincoln, Nebraska, also search driver's license photos from state department of motor vehicle databases.[14]

Evidentiary requirements

Some cities set an evidentiary requirement for police before they can run a facial recognition search. For example, Albuquerque, New Mexico, requires police to demonstrate probable cause before they run a search on a suspect. San Diego, California, police are required to have reasonable suspicion before they run a facial recognition search. By contrast, Lincoln, Nebraska, does not require either of these standards before authorities conduct a search.[15]

Input requirements

The images for use in a facial recognition search range in quality and type. When police fail to obtain a clear photo of a suspect, some departments, including Washington County, Oregon, use sketches or artist renderings as a substitute for the photo.[16] Other departments, including in New York City, have used celebrity doppelgangers as substitutes for suspect photos.[17] Other cities, including Seattle, Washington, have used only actual photos of suspects as inputs.

Type of crime

Some cities have also chosen to limit their use of facial recognition to certain types of criminal investigations. Detroit, Michigan, whose city council approved a new policy in September 2019, now requires that the department use facial recognition only to investigate violent crimes and home invasions.[18]

What are the benefits and risks for local governments' use of facial recognition?

There are benefits and risks for government entities' use of facial recognition. 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.

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.

BENEFIT
Investigative efficiencies

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.

RISK
Bias in facial recognition technology

Facial recognition technology has made great strides in recent years, but the technology in use today tends to make more errors in identifying dark-skinned people and women than light-skinned people and men. A 2018 American Civil Liberties Union (ACLU) study used Amazon's Rekognition, one of the leading facial recognition programs at that time, to search for matches between members of Congress and a database of mug shots.[19] This search produced false positive matches, or incorrectly reported that an unknown picture matched a known picture in a database, for 28 members of Congress, 40% of whom were people of color, even though only roughly 20% of Congressional members are people of color. A 2018 MIT study showed that IBM and Microsoft systems designed to identify a face's gender worked nearly perfectly on White men but had a 20% failure rate on women of color.[20]

The National Institute of Standards and Technology (NIST) is considered the foremost authority on evaluating facial recognition algorithms.[21] Their 2019 test of facial recognition technology vendors assessed how well 189 facial recognition algorithms, submitted by 99 developers around the world, identified people of different demographics. The study found a wide range in accuracy across developers, with many algorithms 10 to 100 times more likely to inaccurately identify people.

When looking at U.S. law enforcement images, the algorithms identified American Indian, Black and Asian American people as false positive identifications more frequently compared to White people. NIST also found that false positives were more likely with women, the elderly and children, compared to men and middle-aged adults, although the effects of these false positives were smaller than the issues with identification based on race.[22]

Why does the technology continue to misidentify people of color and women? The authors of a 2012 Institute of Electrical and Electronics Engineers (IEEE) study state that part of the misidentification problem with women may occur because they tend to wear more cosmetics than men do, decreasing the consistency of images of their face from one capture to the next.[23] Several technologists attributed higher error rates for people of color because there is less contrast in the imagery than for White individuals, making the mapping of facial features inherently less precise.[24] However, the most compelling explanation of these error rates is that facial recognition algorithms reflect the fact that there is a disproportionately higher number of White images in the training image data set. The algorithms optimize their performance on the sets of sample faces used to train them. Training sets tend to overrepresent White men, therefore the algorithms become highly proficient at identifying the faces of White men, to the detriment of people of color. In 2011, researchers evaluated a set of algorithms' accuracy and found that, "the East Asian fusion algorithm is more accurate at recognizing the East Asian faces and the Western fusion algorithm is more accurate on the Caucasian faces."[25]

Ambivalence among facial recognition technology companies perpetuates the problem. Not all facial recognition companies test their algorithms for racial bias.[26] NIST began regularly testing for performance by race only in 2017.[27] There has been some progress in this realm; for example, in January 2019, IBM released a data set of 1 million faces, claiming it better represents the human population than do other less current data sets.[28]

However, cities can still hold facial recognition technology vendors accountable. Many cities seeking vendors for facial recognition technology have minimum thresholds for accuracy overall; they should also have accuracy thresholds with respect to demographic groups.[29] The technology's strong performance regarding White males has masked its shortcomings concerning other groups, especially people of color, giving cities a false impression of reliability.

The first known misidentification and wrongful arrest because of a false positive facial recognition match in the U.S. occurred in Detroit, Michigan. Robert Julian-Borchak Williams, a Black man, was accused and arrested by two Detroit Police Department officers in January 2020 on shoplifting charges, based on store video footage of an October 2018 incident. A review of the investigative process revealed a lack of controls in the process and loose standards for identification. The city has since updated its facial recognition policy.

Hill, K. (2020, June 24). Wrongfully Accused by an Algorithm. New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

It is critical that facial recognition technology companies do all they can to avoid false matches. A false match can lead law enforcement to investigate or arrest an innocent person. Although misidentifications do not always lead to wrongful convictions, a search or arrest itself can be humiliating or trigger trauma, and both entail an increased risk of confrontation or violent escalation. Blacks have a disproportionate number of encounters with police, so they will likely be queried more often in facial recognition searches.[30]

They are also arrested at a higher rate than other groups — in some states, five times as often.[31] They are overrepresented in mug shot databases, meaning that facial recognition technology is more likely to identify a person as a suspect in the U.S. if the person is Black. Because the data sets used for training facial recognition algorithms are distinct from the comparison data sets that these algorithms use in practice, the underrepresentation of Blacks in training data sets and their overrepresentation in mug shot databases make the population for which the technology works least accurately the group most vulnerable to misidentification.

American law enforcement's widespread use of facial recognition technology could negatively and disproportionately affect Black communities. Until commercial companies make training data sets more representative, and cities and the public have processes for holding companies accountable for racial disparities in their algorithms' performance, the use of facial recognition technology will continue to raise significant concerns of racial equity.

The technology's strong performance regarding white males has masked its shortcomings concerning other groups, giving cities a false impression of reliability.

RISK
Constitutional concerns: First and Fourth Amendments

Law enforcement's use of facial recognition technology raises several constitutional issues. The Constitution does not state whether the police can use something like facial recognition technology, and courts have yet to fully deal with this issue. However, the primary concerns are

- whether identifying someone through facial recognition constitutes an unlawful search under the Fourth Amendment and
- whether this could infringe upon First Amendment rights of assembly and free speech.

Ultimately, although government use of facial recognition technology would not per se infringe upon First and Fourth Amendment rights, sufficiently widespread and pervasive deployment of the technology could be interpreted to do so.

Fourth Amendment issues

The Fourth Amendment protects people from unlawful police searches where they have a reasonable expectation of privacy. In *Katz v. United States*, the Supreme Court held that a reasonable expectation of privacy depends on

- whether the person subjectively expected privacy in that circumstance and
- whether society recognizes that expectation of privacy as reasonable.[32]

In theory, the use of facial recognition technology in a public safety context — surveilling public spaces and capturing the image of someone's face — seems to uphold the Fourth Amendment guidelines. Entering a public space generally removes a reasonable expectation of privacy; in *Katz* the Court stated, "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[33] Special cases, such as the act of entering the phone booth at issue in *Katz*, have been treated as exceptions in which it is reasonable for a person to expect some measure of privacy despite being in public.[34] However, the surveillance video that most municipalities use for facial recognition applications is captured in public spaces that would not include any such exception.

The Supreme Court has deemed a person's face to be beyond Fourth Amendment protection. In United *States v. Dionisio*, the Supreme Court refused to recognize an expectation of privacy over certain personal attributes, stating, "Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."[35]

However, the Court has started to expand the expectation of privacy it considers reasonable in cases in which modern technology drastically enhances law enforcement's capabilities. The Court is increasingly willing to find violations of Fourth Amendment rights when new technologies allow the government to track people far more persistently than was previously possible. In *Jones v. United States*, the Court held that a GPS tracker attached to a person's car for several weeks constituted a Fourth Amendment violation.[36]

The Court held that although a driver could not reasonably expect their location at any one instant to be private while they traveled in public, they did have a reasonable expectation that no one would know every location they visited.[37] In *Carpenter v. United States*, the Supreme Court held that warrantless acquisition of data listing the cell towers that a person's phone pinged for 127 days, which gave investigators a map of his movements, constituted a violation of his Fourth Amendment rights, as the knowledge of all of his movements over this period gave the government an excessively intimate and invasive window into his life.[38]

In both cases, although knowledge of the person's location at one instant was not particularly invasive, knowledge of their location at every instant across many days did cross that line. If police use facial recognition technology to track people's whereabouts for an extended period, this could be deemed a violation of Fourth Amendment rights. However, if the police use it in limited fashion to confirm or deny a person's presence at any one time and place, this would likely not be deemed a violation of Fourth Amendment rights, as long as that location is a public place that does not create a reasonable expectation of privacy.

The Court has also held that use of non-publicly available technology to conduct otherwise impossible searches violates Fourth Amendment rights. In *Kyllo v. United States*, the Supreme Court held that police use of a thermal imaging device to determine whether a man was growing marijuana in his apartment was an unlawful search.[39] The police did not physically enter the suspect's home; nonetheless, the lack of widespread public use or knowledge of devices that could remotely penetrate the home in that manner created a reasonable expectation of privacy that the Court was willing to recognize.

However, the thermal scanner was not widely available, and the way the police used it — scanning the exterior wall of a person's home to provide information about what was occurring inside — was not something the public generally knew was possible. Facial recognition technology is available in enough applications that the public cannot be said to be unaware of it. A 2019 Pew Research Center survey found that most American have heard of facial recognition technology (86%), with 25% having heard a lot about it.[40] In the vein of new technology enabling violations of privacy, *California v. Ciraolo* is more relevant to facial recognition technology than is *Kyllo*.[41] In *Ciraolo*, the Supreme Court held that police use of a plane to conduct aerial surveillance on a suspected marijuana grower's property was not unlawful, as the routine practice of commercial flight in public airways at that point in history made any expectation of privacy unreasonable regarding objects plainly visible from the sky.[42]

These cases both turn on whether law enforcement uses the technology to gain information about people in a way that the public could reasonably expect. As public video surveillance is not a new concept and facial recognition technology is also now widespread, the latter's use to identify individuals in public would likely not raise the same Fourth Amendment concerns as did *Kyllo*.

First Amendment issues

Law enforcement's use of facial recognition technology can potentially infringe on First Amendment rights of free speech and assembly. Some argue that facial recognition technology can do this by depriving people of their ability to speak and gather anonymously, because the knowledge that they are being tracked could deter people from engaging in speech or assembly in which they otherwise would engage.[43]

The Supreme Court has held that the First Amendment right of free speech includes the right to speak anonymously.[44] In *NAACP v. Alabama*, the Court held that the NAACP could not be compelled to disclose its members' identities, as doing so would hinder their ability to express their ideas.[45] In *Talley v. Alabama*, the Court held that the First Amendment protected the right to distribute pamphlets anonymously, stating, "[t]here can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[46] The Supreme Court's recognition that a degree of anonymity is necessary for free expression runs contrary to facial recognition technology's capacity to essentially end anonymity in public spaces.

Judicial treatment of police surveillance of public gatherings is mixed. In *Laird v. Tatum*, the Supreme Court held that the military's surveillance of a public gathering did not inhibit the group's ability to express their views, absent any danger of a direct injury stemming from the surveillance.[47] However, at some point, surveillance can cross the line. In 2015, the Third Circuit ruled in *Hassan v. City of New York* that extensive police surveillance of Muslim Americans following the September 11 attacks did harm a group that was singled out for its religious affiliations, and was thus constitutionally impermissible.[48]

Facial recognition technology may entail more passive surveillance than in *Hassan*. However, the technology also goes far beyond simply photographing a gathering as in *Laird*, when it means not only photographing but also immediately identifying people. In 2016 the police used facial recognition technology on pictures in social media posts to identify and arrest protestors in Baltimore after Freddie Gray's death.[49] The ACLU stated that this raised significant First Amendment concerns.[50]

Police use of facial recognition technology as another investigative tool is unlikely to be held categorically impermissible under the First Amendment. However, certain uses, such as using the technology to monitor specific gatherings or to track specific groups over extended time periods, could inhibit free expression and assembly rights and be held to violate the First Amendment. Although continued improvements to facial recognition technology could remedy many of the other problems stemming from it, the threat that facial recognition technology poses to constitutionally protected rights will only increase as the technology grows more accurate.

RISK
City liability

The doctrine of sovereign immunity traditionally protects governments and government officials from lawsuits. However, both states and the federal government have carved out exceptions allowing government officials to be held liable in certain situations.

Liability for violations of constitutional rights

In a 2017 report, the Bureau of Justice Assistance in the U.S. Department of Justice warned that "misuse of face recognition information may expose agencies participating in such systems to civil liability."[51] One of these sources of liability stems from 42 U.S.C. § 1983, a statute giving people the right to sue a "person" acting under government authority who deprives them of their constitutional rights, such as those discussed above under the First and Fourth Amendments. People can directly sue individual government officials in their personal capacities. However, given that governments can pay more money in damages or in a settlement than individuals can, plaintiffs will often try to sue the government.

In the 1978 case *Monell v. Department of Social Services*, the Supreme Court held that a city is a "person" for the purposes of § 1983 liability, opening cities to liability for constitutional violations. Cities can either be sued directly, or they can be held liable for their employees' actions.[52] Cities can only be held liable for their employees' actions if the employees act under the color of authority and the violation resulted from an official policy that is the "moving force" of the constitutional violation. Courts have determined several specific categories of city actions that can result in a violation under § 1983:

- **A formal policy established by the city or an informal policy or custom that is so pervasive as to constitute a de facto policy of the city.** For example, a police department policy of using deadly force absent probable cause of an imminent threat of harm would amount to a violation of citizens' Fourth Amendment rights.[53] In the context of facial recognition, if courts were to determine that facial recognition surveillance in public areas violates the Fourth Amendment, a city that officially deploys this surveillance would be at risk of liability under § 1983.
- **A failure to train or supervise employees to such an extent as to demonstrate "deliberate indifference" toward constitutional rights.**[54] For example, if cities deploy facial recognition technology without training officers in how to use it and these officers subsequently falsely arrest numerous people, the cities could be held liable for Fourth Amendment violations. The doctrine of "qualified immunity" may protect officers from liability under § 1983 when they are sued as individuals. Officers are liable for violations of constitutional rights only if a "reasonable officer" would know that his or her conduct was unlawful in the situation in question.[55]
- **A single decision by a "final policymaker" for the government.** This "final policymaker" would be an official with authority to decide on a policy for a given subject matter. This could be a mayor or an official delegated to make decisions in a certain area. State courts have different approaches to determining who constitutes a "final policymaker" for the purposes of this rule.[56] In the facial recognition context, if there is no public discussion about the use of facial recognition during official duty but a chief executive approves it unilaterally, cities could be held liable for unintended or improper consequences.
- **A higher-ranking official knows and approves of a subordinate's decision that violates a citizen's constitutional rights.** A mere failure to overrule a subordinate does not amount to an affirmative endorsement.57 However, without a policy that provides proper checks and balances for the use of facial recognition technology, city officials could be liable for improper actions of its public safety department.

Municipal tort liability

Apart from considering federal § 1983 constitutional claims, cities could also face municipal liability for torts such as negligence or battery. Most states have passed tort claims laws, which allow people to sue state and local officials for certain torts. These laws are often modeled on the Federal Tort Claims Act (FTCA) of 1946, which enables people to sue the federal government for similar violations. Under the FTCA and most state tort claims acts, governments are liable for tort violations committed by their employees only if those officials acted within the scope of their employment.

However, the types of claims for which cities are liable vary widely depending on the state. Some states waive immunity only for certain types of claims. No claims have yet been brought against a government under tort law for the misuse of facial recognition. However, a pending

claim against Apple in a federal court in New York could indicate how courts will handle this issue. Apple accused Ousmane Bah of stealing from one of its stores after the company's facial recognition algorithm misidentified him as the perpetrator.[58] Bah claims that the actual perpetrator presented as identification Bah's learner's permit, which does not include a photo and which Bah lost on the street in the months prior. As a result, Apple's facial recognition software linked the perpetrator's face, captured on surveillance footage, with Bah's name and address. Bah is now suing Apple for negligence, claiming that it carelessly used its facial recognition software to wrongfully identify him, seeking $1 billion in damages.[59] The litigation is ongoing. The outcome of this lawsuit will indicate how courts may treat similar claims against cities or companies for the negligent use of facial recognition technology resulting in misidentifications.

State biometric privacy laws

A few states (e.g., Oregon, California, Illinois, Texas and Washington) have passed biometric privacy laws that hold private companies liable for privacy violations resulting from the collection of biometric data. These laws regulate companies' retention and protection of biometric data, and they require individual consent for collection of biometric data.[60] None of these laws hold governments directly liable, but the laws could have implications for cities seeking to acquire facial recognition technology. Vendors may be more reluctant to operate in states that have strict biometric privacy laws, as they may face greater liability. Alternatively, to mitigate this liability risk, vendors may seek to shift liability to cities. If cities agree to indemnify facial recognition vendors in their contracts with these vendors, they could face greater legal and monetary risk.

Shifting of liability in contracts

Contracts between cities and vendors demonstrate various approaches to liability. In some contracts, cities have agreed to assume much of the liability for claims resulting from the misuse of facial recognition technology, agreeing to indemnify the vendor and pay for damages that may result from lawsuits. Article XI of the San Diego Association of Government (SANDAG) contract with FaceFirst states, "FaceFirst shall not be responsible, and shall have no liability to Customer or any third parties allegedly aggrieved in connection with the use of the product by Customer." Under Article XII of the contract, SANDAG agrees to "defend at its expense any legal proceeding brought by a third party…against FaceFirst," provided that the claim against FaceFirst is connected with SANDAG's failure to comply with "any applicable law."[61] Under this contract, if SANDAG collects data in a way that violates a state data privacy law, it could be liable to pay for damages assessed against FaceFirst.

A Detroit, Michigan, contract with DataWorks Plus reflects an alternative approach, under which the vendor assumes much of the liability risk. Under Article 2.04 of that contract, DataWorks Plus agrees to "remain liable in accordance with applicable law for all damages to the City caused by the Contractor's negligent performance or nonperformance of any of the Services furnished under this Contract." DataWorks Plus also agrees to fully indemnify Detroit for any claims asserted against the city that arise from DataWorks Plus's own negligence.[62] By contrast, FaceFirst agrees to fully indemnify SANDAG only for intellectual property claims, that is, claims that FaceFirst's technology violated another company's patents or copyrights.[63]

Before the City and County of San Francisco, California, banned facial recognition, its contract with Cogent struck a middle ground between these two cases. As in the Detroit contract with DataWorks Plus, Cogent agreed to indemnify the city and its employees from claims "arising directly or indirectly from Contractor's performance of this Agreement." However, unlike the DataWorks Plus contract, Cogent included a limitation in this indemnification clause: it disclaimed all responsibility in cases resulting from the "active negligence or willful misconduct" of San Francisco.[64] As these cases illustrate, minor changes in the language of a city's contract with a facial recognition vendor can have substantial implications for the city's risk of liability.

How are cities regulating facial recognition?

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. Most cities regulating facial recognition focus solely on governmental use. To date, only the City of Portland, Oregon, has restricted private use of facial recognition. This section highlights a few cities and their experiences with facial recognition technology.

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

Regulating surveillance technology

Guided by the ACLU's Community Control Over Police Surveillance framework, at least 15 cities across the country have passed surveillance technology ordinances. Most of these ordinances indirectly govern the use of facial recognition and require community oversight over any use of surveillance technology.[65] For example, Oakland's surveillance ordinance, considered one of the strictest in the country, requires law enforcement to create a "technology impact report" on new surveillance technologies that covers issues such as data storage and civil liberties.[66]

CITY OF SEATTLE, WASHINGTON

Policy limiting use of facial recognition, but technology no longer used

The City of Seattle, Washington, began using facial recognition technology in 2014. With the help of a $1.5 million grant from the Department of Homeland Security, Seattle, Washington, purchased a facial recognition system from NEC. The Seattle City Council voted on a facial recognition use policy that allowed law enforcement to use the technology in limited circumstances. Specifically, Seattle permitted the use of facial recognition to identify people taken into custody when they could not be identified by other means. The Seattle City Council approved funding for the system under a policy created in consultation with the ACLU of Washington. Seattle Sound 911, a public safety agency covering three counties in the Seattle region, operated the system.[67]

Seattle required that the vendor achieve a 96% identification accuracy rate.68 Police used the system in a limited capacity to identify people who had been taken into custody but could not be identified. According to city officials, police conducted fewer than 50 searches in four years. Recognizing the system's limited utility, Seattle Police stopped using the technology in 2018. Also motivating this decision was the difficulty of receiving approval for the system's use through the city's new surveillance oversight ordinance, passed in 2017, because of the overly bureaucratic process for approved use and public calls to ban the use of facial recognition.

CITY OF DETROIT, MICHIGAN

Policy limiting use of facial recognition

Initiating a three-year contract with the facial recognition vendor DataWorks Plus, Detroit, Michigan, purchased a facial recognition system in July 2017 for $1 million. Under Detroit's public-private partnership Project Green Light, businesses and organizations could purchase and install facial recognition cameras that feed captured images to the police.

These images could then be compared to a database of mug shot photos maintained by Detroit police.[69] After a series of public debates, the Detroit Board of Police Commissioners, a civilian oversight body composed of officials either elected or appointed by the mayor, adopted a new policy in September 2019.

This policy prohibits the use of real-time surveillance and allows the use of facial recognition only during investigations of violent crimes and home invasions. The policy also requires that at least two officers verify matches produced by the facial recognition system. It imposes harsh penalties for officers who abuse the technology, including termination of employment.[70]

SAN FRANCISCO BAY AREA, CALIFORNIA

Policies banning facial recognition

Many cities in the San Francisco Bay Area have banned city officials' use of facial recognition. The San Francisco Police Department used facial recognition for nine years prior to the Board of Supervisors' decision to ban the technology in May 2019. San Francisco purchased a system from 3M Cogent and, like Seattle, required the vendor to regularly test the accuracy of its algorithm. San Francisco Police could search between half a million and one million mug shots. San Francisco's use policy was not publicly available before the Board of Supervisors voted to ban use of the technology.71 San Francisco Supervisor Aaron Peskin, who introduced the bill, argued that a ban was necessary because the technology is "so fundamentally invasive" that it should not be used at all.[72]

The City of Oakland followed suit in banning facial recognition in July 2019. City Council President Rebecca Kaplan explained her rationale for introducing her bill banning the technology: "I welcome emerging technologies that improve our lives and facilitate city governance, but when multiple studies show a technology is flawed, biased, and is having unprecedented, chilling effects to our freedom of speech and religion, we have to take a stand."[73]

After discussing facial recognition in 2018 and much of 2019 at city council meetings and the council's Public Safety Committee, the City of Berkeley Council became the fourth U.S. city to ban facial recognition, in October 2019, citing concerns about both privacy and racial bias.[74]

How can cities better approach the topic of facial recognition publicly?

Cities have a responsibility to their communities to thoughtfully explore emerging technologies that can aid the greater good. The conversation concerning facial recognition is particularly sensitive given the technology's imperfections and how it is frequently implemented and used behind closed doors. By following these recommendations, cities can better facilitate public discussions about facial recognition technology 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.

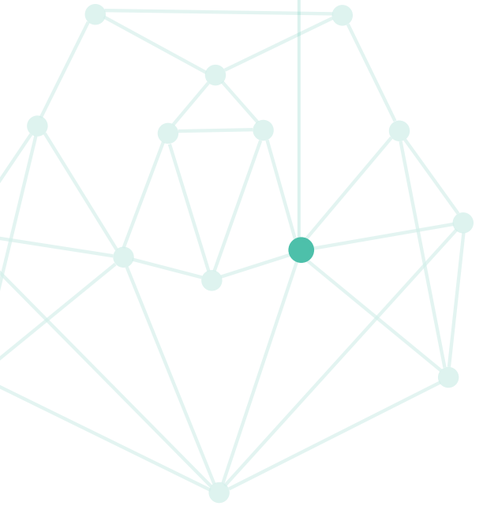
- Require that all officers who are cleared to use the technology be extensively trained on how to use it. Make sure that officers are aware of the probabilistic nature of the technology.
- Establish a high probability threshold for matches before the technology can be used in an investigation.
- Require 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.[75]
- 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.[76] 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.[77]
- 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.

Endnotes

[1] Whitehead, N. (2014, April 23). *Face Recognition Algorithm Finally Beats Humans.* Science. Retrieved from https://www.sciencemag.org/news/2014/04/face-recognition-algorithm-finally-beats-humans?r3f_98.

[2] Brownlee, J. (2019, May 31). *A Gentle Introduction to Deep Learning for Face Recognition.* Machine Learning Mastery. Retrieved from https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/.

[3] Garvie, C. et al. (2016, October 18). *The Perpetual Line-up. Georgetown Center on Privacy and Technology.* Retrieved from https://www.perpetuallineup.org/.

[4] King, K. (2019, October 7). *New York City Lawmakers Look To Regulate Facial Recognition Tools.* Wall Street Journal. Retrieved from https://www.wsj.com/articles/new-york-city-lawmakers-look-to-regulate-facial-recognition-tools-11570485799.

[5] Steele, K. (2018, November 29). *Delta Unveils First Biometric Terminal in U.S. in Atlanta; Next Stop: Detroit. Delta Press Release.* Retrieved from https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.

[6] Draper, K. (2018, March 13). *Madison Square Garden Has Used Face-Scanning Technology on Customers.* New York Times. Retrieved from https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

[7] Simonite, T. & Barber, G. (2019, October 17). *The Delicate Ethics of Using Facial Recognition in Schools.* WIRED. Retrieved from https://www.wired.com/story/delicate-ethics-facial-recognition-schools/.

[8] Mikkelsen, D. (2018, October 31). *Two Seattle Schools Among First To Use Facial Recognition Software in US.* King5 News. Retrieved from https://www.king5.com/article/news/education/two-seattle-schools-among-first-to-use-facial-recognition-software-in-us/281-609937626.

[9] Harding, H. (2019, July 9). Boise Will Spend $52,000 on Facial Recognition To Keep "Banned" People Out of City Hall. Idaho Statesman. Retrieved from https://www.idahostatesman.com/news/local/community/boise/article232411592.html.

[10] Crist, R. (2019, September 9). *Google's Got a New Face-Tracking Camera for Your Home. We've Got Questions.* Cnet. Retrieved from https://www.cnet.com/news/google-nest-hub-max-a-new-face-tracking-camera-for-your-home-weve-got-questions/.

[11] Nguyen, N. & Mac, R. (2019, August 30). *Ring Says It Doesn't Use Facial Recognition, But It Has "A Head Of Face Recognition Research."* Buzzfeed. Retrieved from https://www.buzzfeednews.com/article/nicolenguyen/amazon-ring-facial-recognition-ukraine.

[12] Siminoff, J. (2019, August 28). *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map.* Ring Blog. Retrieved from https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/.

[13] Garvie, C. & Frankle, J. (2016, April 7). *Facial-Recognition Software Might Have a Racial Bias Problem.* The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[14] Garvie et al., *The Perpetual Line-up.*

[15] Garvie et al., *The Perpetual Line-up.*

[16] Garvie, C. (2019, May 16). *Garbage In, Garbage Out. Georgetown Center on Privacy and Technology.* Retrieved from https://www.flawedfacedata.com/.

[17] Garvie, *Garbage In, Garbage Out.*

[18] Cwiek, S. (2019, September 19). *Detroit Police Commissioners Approve Facial Recognition Policy. Michigan Radio.* Retrieved from https://www.michiganradio.org/post/detroit-police-commissioners-approve-facial-recognition-policy.

[19] Snow, J. (2018, July 26). *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots.* American Civil Liberties Union. Retrieved from https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[20] Buolamwini, J. et al. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.* Proceedings of Machine Learning Research, 81, 1–15. Retrieved from

[21] Simonite, T. (2019, July 22). *The Best Algorithms Struggle to Recognize Black Faces Equally. Wired.* Retrieved from https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

[22] National Institute of Standards and Technology. (2019, December). *National Institute of Standards and Technology Interagency or Internal Report 828.* Retrieved from https://doi.org/10.6028/NIST.IR.8280.

[23] Klare, B. et al. (2012). *Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Information Forensics and Security, 7, 1789–1802.* Retrieved from http://openbiometrics.org/publications/klare2012demographics.pdf.

[24] Garvie et al., *The Perpetual Line-up.*

[25] Phillips, P.J. et al. (2011). *An Other-Race Effect for Face Recognition Algorithms. ACM Transactions on Applied Perception*, 8(2), 1–11.

[26] Garvie et al., The Perpetual Line-up.

[27] Garvie et al., The Perpetual Line-up.

[28] Smith, J. (2019, January 29). *IBM Research Releases 'Diversity in Faces' Dataset to Advance Study of Fairness in Facial Recognition Systems.* IBM Research Blog. Retrieved from https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

[29] Garvie et al., The Perpetual Line-up.

[30] Garvie et al., *The Perpetual Line-up.*

[31] Garvie et al., *The Perpetual Line-up.*

[32] Katz v. United States, 389 U.S. 347 (1967).

[33] Katz v. United States, 389 U.S. 351 (1967).

[34] Katz v. United States, 389 U.S. 348 (1967).

[35] US v. Dionisio, 410 US 1 (1973).

[36] United States v. Jones, 565 U.S. 400 (2012).

[37] United States v. Jones, 565 U.S. 404 (2012).

[38] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

[39] Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

[40] Smith, A. (2019, September 5). *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly.* Pew Research Center. Retrieved from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/09/09.05.19.facial_recognition_FULLREPORT_update.pdf.

[41] California v. Ciraolo, 476 U.S. 207, 213 (1986).

[42] California v. Ciraolo, 476 U.S. 207, 215 (1986).

[43] Hamann, H. et al. (2019, Spring). *Facial Recognition Technology: Where Will It Take Us? The American Bar Association, Criminal Justice Magazine*. Retrieved from https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

[44] Nat'l Ass'n for Advancement of Colored People v. State of Ala. Ex rel. Patterson, 357 U.S. 449 (1958).

[45] Nat'l Ass'n for Advancement of Colored People v. State of Ala. Ex rel. Patterson, 357 U.S. 449 (1958).

[46] Talley v. California, 362 U.S. 60, 63 (1960).

[47] Laird v. Tatum, 408 U.S. 1 (1972).

[48] Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015).

[49] Brandom, R. (2016, October 11). *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*. The Verge. Retrieved from https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.

[50] American Civil Liberties Union. (2016, October 18). *Letter to Principal Deputy Assistant Attorney General Vanita Gupta*. Retrieved from https://www.aclu.org/sites/default/files/field_document/coalition_letter_to_doj_crt_re_face_recognition_10-18-2016_1.pdf.

[51] U.S. Department of Justice. (2017, December). *Face Recognition Policy Development Template*. Bureau of Justice Assistance, U.S. Department of Justice. Retrieved from https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf.

[52] Monell v. Dep't of Soc. Servs., 436 U.S. 658 (1978).

[53] Tennessee v. Garner, 471 U.S. 1 (1985).

[54] City of Canton v. Harris, 489 U.S. 378 (1986).

[55] Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982). The Supreme Court has further clarified that officers are to receive broad deference when the law is unsettled, and that only those officers who are "plainly incompetent" or "knowingly violate the law" will not be covered by qualified immunity. See Kisela v. Hughes, 138 S. Ct. 1148, 1152 (2018).

[56] City of St. Louis v. Praprotnik, 485 U.S. 112 (1988).

[57] Lytle v. Carl, 382 F.3d 978, 987 (9th Cir. 2004).

[58] Shaban, H. & Flynn, M. (2019, April 23). Teen Sues Apple for $1 Billion, Blames Facial Recognition at Stores for His Arrest. *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2019/04/23/teen-sues-apple-billion-blames-facial-recognition-stores-his-arrest/.

[59] Bah v. Apple, Inc., 19-cv-03539, Complaint (S.D.N.Y., Apr. 22, 2019). Retrieved from https://www.scribd.com/document/407291893/Bah-v-Apple-Inc-19-cv-03539-U-S-District-Court-Southern-District-of-New-York.

[60] Seyfarth Shaw LLP. (2020, June 9). *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*. JDSupra. Retrieved from https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/.

[61] Garvie et al., *The Perpetual Line-up*.

[62] Lipton, B. (2019, August 27). *Rep. Rashida Tlaib and Detroit Police Spar Over City's Milion-Dollar Facial Recognition Contract. Here It Is*. Muckrock. Retrieved from https://www.muckrock.com/news/archives/2019/aug/27/rep-rashida-tlaib-detroit-facial-recognition/.

[63] Garvie et al., *The Perpetual Line-up*.

[64] Garvie et al., *The Perpetual Line-up*.

[65] American Civil Liberties Union. Community Control Over Police Surveillance. Retrieved from https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

[66] Tadayon, A. (2018, May 2). Oakland To Require Public Approval of Surveillance Tech. *East Bay Times*. Retrieved from https://www.eastbaytimes.com/2018/05/02/oakland-to-require-public-approval-of-surveillance-tech/.

[67] Garvie et al., *The Perpetual Line-up*.

[68] Miletich, S. (2016, October 18). Seattle Police Win Praise for Safeguards With Facial-Recognition Software. *Seattle Times*. Retrieved from https://www.seattletimes.com/seattle-news/crime/seattle-police-wins-praise-for-safeguards-with-facial-recognition-software/.

[69] Garvie, C. & Moy, L. (2019, May 16). *America Under Watch. Georgetown Center on Privacy and Technology*. Retrieved from https://www.americaunderwatch.com/.

[70] Cwiek, Detroit Police Commissioners Approve Facial Recognition Policy.

[71] Garvie et al., *The Perpetual Line-up*.

[72] Metz, R. (2019, May 14). *San Francisco Just Banned Facial-Recognition Technology*. CNN. Retrieved from https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html.

[73] Ravani, S. (2019, July 17). Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns. *San Francisco Chronicle*. Retrieved from https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

[74] McKay, T. (2019, October 16). *Berkeley Becomes Fourth U.S. City To Ban Face Recognition in Unanimous Vote. Gizmodo*. Retrieved from https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651.

[75] Cwiek, Detroit Police Commissioners Approve Facial Recognition Policy.

[76] Friedman, B. & Ferguson, A. (2019, October 31). Here's a Way Forward on Facial Recognition. *New York Times*. Retrieved from https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html.

[77] Bala, N. & Watney, C. (2019, June 20). *What Are the Proper Limits on Police Use of Facial Recognition?* Brookings. Retrieved from https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/.

NLC NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER