THE ALGORITHMIC JUSTICE LEAGUE FACIAL RECOGNITION TECHNOLOGY

WHAT IS FACIAL RECOGNITION TECHNOLOGY?

"Facial recognition" refers to a group of technologies that perform tasks on human faces.. It relies on artificial intelligence (AI) to learn the patterns of a human face. The AI system uses a machine learning model to learn from a dataset of human faces. These datasets can be compiled using **data scraped from social media platforms and millions of other websites** and can include anywhere from a few thousand to billions of images.

Facial recognition can be used **by the government and the private sector** in a variety of ways. The process begins with capturing a facial image. Your face can be captured almost anywhere — including by cameras in public and private places (office buildings, streetlamps, traffic lights, gas stations, restaurants). Our faces are the most visible part of our bodies. Unlike fingerprints or DNA testing, facial recognition does not require any physical contact to identify someone.

FIRST: FACIAL DETECTION

The most basic task is detecting the presence of your face in an image or video. Simply detecting that a face is present however does not say anything about that face without some additional steps...

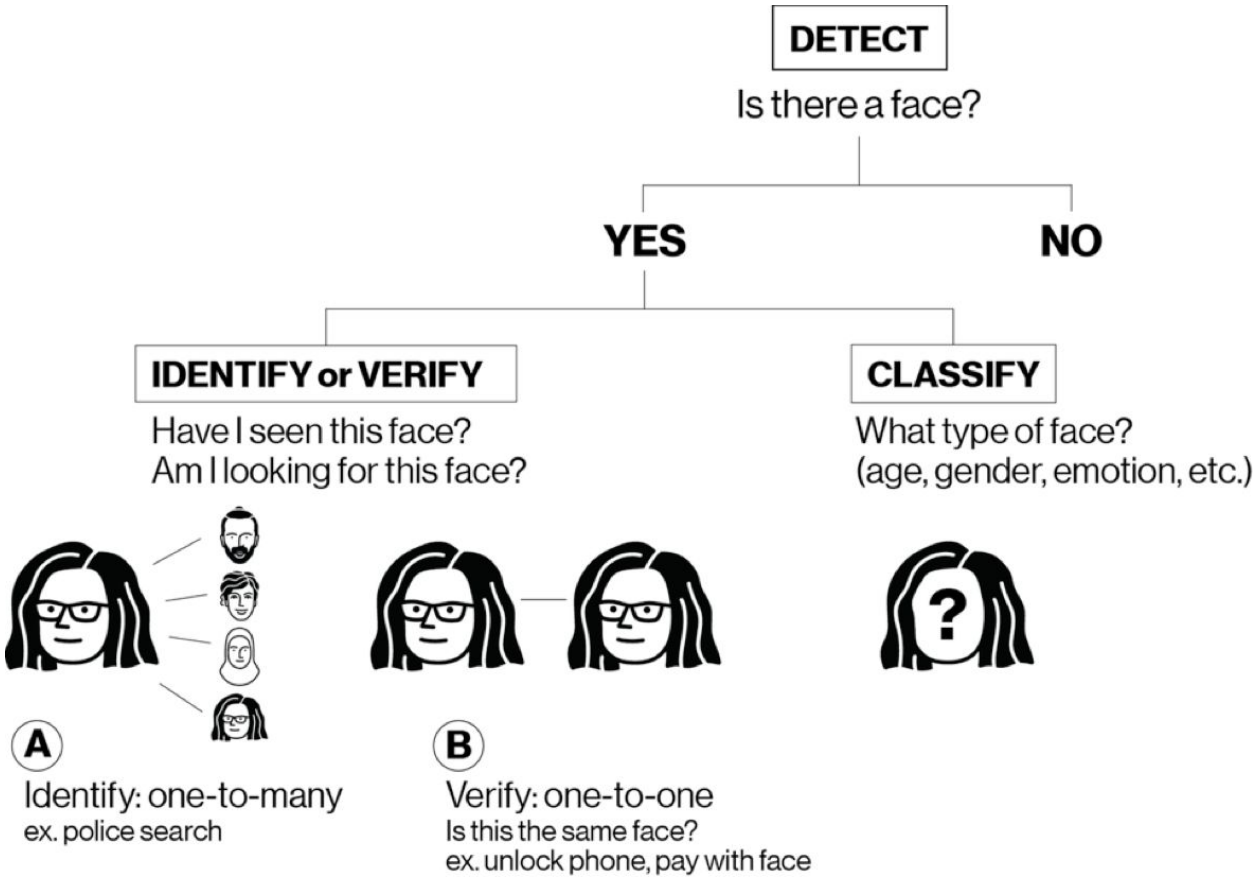
After your face is detected, machines can perform one of several tasks...

Facial Verification
Your face can be compared by a device against a single stored image to determine if it is a match — for example to unlock your phone or to board a plane.

Facial Identification
Your face can be compared against a database of faces — for example a database of drivers license photos or mugshots — to see if it's a match for a potential suspect or another person of interest.

Facial Attribute Classification
Your face can be analyzed in an attempt to guess demographic attributes like your age, gender or ethnicity. This process can also detect accessories and facial hair.

Facial Affect Recognition
Your facial expressions can be analyzed in real-time or on video in *an attempt* to label your emotions or other inner qualities, including personality traits, mental health and intelligence. Your expressions can also be analyzed in *an attempt* to label even more complex characteristics like sexuality, political beliefs or potential criminality.



Below is a simple chart identifying a few ways that facial recognition is being used and the potential harms that are associated with each type of use.

USE CASE	HARMS
LAW ENFORCEMENT Law enforcement officers can use facial recognition to identify potential suspects and conduct mass surveillance, which includes monitoring and tracking people. In Florida, Willie Allen Lynch was identified by facial recognition as a suspect using a cell phone photo. The system returned a low confidence match but was still used to prosecute and convict Lynch in 2016. None of this was revealed by the prosecution to the defense, which could have helped with Lynch's case. He was sentenced to 8 years in prison. Across the country, police departments are using face recognition systems that include over 117 million adults. **These systems have been used to:** • Identify people who have been stopped or arrested • Match ATM photos against a driver's license database and • Scan people walking by a surveillance camera In April 2019, a facial recognition system misidentified Amara Majeed, a Brown University student as a terrorist suspect in Sri Lanka's Easter church bombings. Although the police later issued a statement correcting the error, Ms. Majeed still received death threats, faced additional police scrutiny and lost time at school. *These are examples of facial identification.* Most police agencies do not have a publicly available use policy, have not received legislative approval for the policy and have not audited their facial recognition systems for misuse.	**1. Liberties and Rights** Face **surveillance** poses significant risks to **civil liberties**, and these risks increase as the technology becomes more accurate. Face surveillance threatens rights including privacy, freedom of expression, freedom of association and due process. On a practical level, this affects how we live and work— particularly when it comes to our ability to enter and express our opinions in public spaces. There is a reason why surveillance has been a tool of authoritarian regimes and facial surveillance risks amplifying this effect further in the twenty-first century. The impacts of facial surveillance are also **discriminatory** because they pose a greater risk to civil liberties for underrepresented communities that are already over-policed (immigrants and people of color) and more vulnerable to police targeting. **2. Misidentification** These systems perform with higher inaccuracy rates on underrepresented groups like youth, elderly, women and people with darker skin. This increases the risk that people from these groups will be **misidentified** as a criminal suspects. Misidentification can lead to serious consequences for a person's liberty and livelihood, particularly if someone is forced to go through the criminal justice system and prove their innocence. Even when misidentified suspects are released, they may lose their jobs and still face death threats and online abuse if the arrest becomes known. In addition to being inaccurate (biased) these technologies are **discriminatory** because they disproportionately impact certain groups. "*Facial recognition can be incredibly harmful when it's inaccurate and incredibly oppressive the more accurate it gets.*" - Woodrow Hartzog (Law Professor & Scholar)

EMPLOYMENT Employers are using facial analysis technology that incorporate emotion recognition on videos of job candidates to inform hiring decisions. The system evaluates a job applicant's facial movements, speech patterns and other indicators during the interview. Based on these factors, the system can score candidates on internal measures like confidence, IQ personality type and even criminality, in addition to demographic attributes like age, ethnicity and gender. A company called HireVue provides companies with a platform to interview potential job candidates on camera and use AI to rate their video images according to verbal and nonverbal cues. *This is an example of facial affect recognition.*	**1. Discrimination** Hiring systems are trained on data from top performers. This data often reflects discriminatory hiring and promotion patterns that have favored men over women and have limited racial diversity. If the data favors one group based on gender or race, then the system will generate recommendations in favor of the group in providing recommendations for hiring. **2. Loss of Opportunity** Hiring patterns augmented by the risk of facial recognition negatively impact economic rights and job opportunities for women and people of color. These systems also discriminate against people who have disabilities that affect their facial expressions and speaking voice. **3. Social Inequality** There is no scientific basis for inferring interior characteristics from a person's facial expressions. This was confirmed by a 2019 **survey of over one thousand papers** on the subject. Allowing for these unfounded assumptions increases the power imbalance between employers and applicants and risks interpreting irrelevant physical differences between people as a justification for discriminatory outcomes.
HOUSING Landlords across the country have sought to install facial recognition entry systems for tenants to enter buildings.	Landlords may fail to obtain affirmative consent and fail to ensure that the facial recognition system performs accurately for all groups of tenants, including women, children, elderly and

In May 2019, the Brooklyn Legal Services Tenant Rights Coalition filed (*and won*) an opposition to block the installation of a face recognition entry system at two rent-stabilized apartment buildings. The landlord had failed to obtain consent, failed to evaluate the performance accuracy of the system in consideration and failed to provide the tenants with any guarantee of data privacy of data privacy. *This is an example of facial verification.*	people of color... especially considering the intersectionality of these groups (for example, women of color). Such tech can also be used by the landlord to harass and monitor tenants. There are no laws governing this data use, so there are also risks that the facial data collected could be shared with the government or the police. These risks threaten the privacy, security and other rights of the tenants. **These risks are enhanced because they impact people at their homes,** a sacred and legally protected space where people are most entitled to enjoy their privacy rights and be free from intrusion.
## SCHOOLS Facial recognition is being used in grade schools to take attendance, permit access to facilities and monitor student behavior, attention and other emotional characteristics. *This is an example of facial verification and facial attribute classification.* Facial recognition is being used on college campuses to monitor student movement in shared spaces, track classroom attendance and prevent non-permitted persons from entering campus. At **Duke University** and the University of Chicago, recordings of students in public spaces have been gathered without the students' affirmative consent. Although the dataset has since been taken down, it was previously used to test or improve facial recognition systems across the world including by researchers to improve Chinese government surveillance. *This is an example of facial verification and facial identification.*	**1. Discrimination** There are greater risks that FRTs could **misidentify children of color as being absent or otherwise breaking the rules.** When combined with institutional racism, this could lead to situations where staff disproportionately believe the system over the child. Risks of misidentifying a child include not only disrupting a child's learning environment but also causing serious **psychological harm**. **2. Rights of the child** By making children feel watched, facial recognition discourages children from being spontaneous or playful and associating freely with peers of their choosing.. This effectively creates the conditions of **censorship**, which impact the rights of the child and carry negative consequences for learning and development. Human rights are fundamental for all but especially for children, whose faculties are still developing through self-expression. **3. Surveillance on Campus** Facial recognition threatens academic freedom and civil liberties. It positions government

	surveillance if universities are state-run. Even for private universities, the college still functions as an institution of authority in the students' and faculty lives. As with other use cases, these risks are exacerbated for groups who are more likely to be misidentified or targeted by surveillance.

CALLS TO ACTION

LOCAL LEVEL

In 2019, **San Francisco became the first city in the country to ban local government use of facial surveillance technology**. Oakland, Berkeley and Somerville, Massachusetts soon followed suit. Its neighbor Cambridge has become the latest city to ban facial recognition, which demonstrates **the domino impact of successful advocacy in one city** to influence change in neighboring communities. Legislators have also introduced similar bills in cities across the country, including Portland, Oregon and Portland, Maine.

These cities provide examples of how people can come together and win when it comes to banning facial surveillance. However, these bills do not pass without a fight. To help citizens push forward, the Electronic Frontier Foundation (EFF) created the **About Face** campaign to provide organizing and capacity-building resources for residents throughout the US to call for an end to local government use of face surveillance.

We encourage you to take action by **joining the About Face movement** and connecting with other concerned local residents in your area. Once you have joined, EFF has compiled **a toolkit** that helps citizen groups prepare for meetings with local lawmakers and community partners. This toolkit contains resources that empower community members to fight face surveillance and win.

STATE LEVEL

In October, 2019 the California State Legislature passed **a 3-year moratorium** prohibiting the use of facial recognition in police body cameras. Oregon and New Hampshire have passed similar bans. AJL Founder Joy Buolamwini recently testified in support of **a bill pending in the Massachusetts state legislature** advocating for this approach.

Given the threat to civil liberties posed by face surveillance and the flaws in these systems that disproportionately affect people of color, AJL has called for a moratorium that halts government use of facial recognition unless and until there are appropriate legal limitations and protections in place.

The ACLU of Massachusetts is also supporting this moratorium as part of its **Press Pause on Face Surveillance campaign**. The campaign seeks to educate the public on the civil liberties risks of face surveillance and provides **a platform for MA residents take action** to contact their legislatures in support of the bill.

We encourage you to get involved by contacting your local representatives and voicing your support for laws that would stop the use of face surveillance by government authorities in your state. Efforts in California and Massachusetts demonstrate that progress is possible. The similarities between the two bills highlight that effort in one state can inform legislation and create momentum in others.

FEDERAL LEVEL

There are currently no federal laws that regulate facial recognition technology at either the commercial or government level.

There have been three (3) public hearings since June, 2019 in front of the House Committee on Oversight and Reform to examine how corporate and government use of facial recognition technology impacts civil rights and liberties, privacy rights and other implications mandating the need for oversight and regulation of how this technology is used.

There are bi-partisan efforts underway in Congress to restrain the federal government's use of facial recognition technology. Proponents from Alexandria Ocasio-Cortez (D-NY) to Jim Jordan (R-OH) have joined together in calls for legislative reform. While certain advocates are pressing on the concerns to our civil rights and liberties, others are focused on our right to privacy. Despite variance in the approach, *there is a real concern on both sides.*

Currently, **The House is exploring a moratorium** on government funding for any new uses of facial recognition technology by federal agencies. In keeping with our position at the state level, we believe that calls for such legislation do not go nearly far enough. Given what we know about the lack of oversight and safeguards in place, known abuses and disproportionate impact on vulnerable and darker skinned groups, we reiterate the need for a moratorium at the federal level that would prohibit all government use of these technologies unless and until adequate regulations are in place.

We also need to seriously consider the **growing evidence in front of Congress as of January 2020** calling for a moratorium on company use of facial recognition in sensitive contexts like hiring and education, where rights and opportunities concerning work and our children are at risk.

COMPANIES AND THE PRIVATE SECTOR

AJL has created the **SAFE Face Pledge** (in partnership with the Centre on Technology & Privacy at Georgetown Law) as an opportunity for companies to make public commitments when it comes to

limiting the abuse of facial recognition technology. The SAFE Face Pledge provides actionable steps that companies can take as developers to turn AI ethics principles into practice:

- **S**how Value for Human Life, Dignity, and Rights
- **A**ddress Harmful Bias
- **F**acilitate Transparency
- **E**mbed Safe Face Pledge into Business Practices

Companies that sign the pledge demonstrate that there is a better way to do business by agreeing to be held accountable to the steps in the pledge. Equally notable are the companies who have been called upon and yet refuse to sign. **We are calling on all companies** who develop, deploy or use facial recognition technologies across industries to come forward and **sign the SAFE Face Pledge**.

If you are an executive, partner or person of influence within your organization, we urge you to take steps to build consensus amongst your colleagues and/ or company decision-makers to move forward with making the pledge.

Please do not hesitate to contact us if you have any strategic questions about how to move forward with supporting the Pledge.

EDUCATION

Grade Schools

In Massachusetts, a coalition of twenty-four advocacy organizations led by the ACLU **sent a joint letter** urging the Massachusetts Board of Elementary and Secondary Education to ensure that schools around the state do not implement face surveillance technology. **We encourage parents** to use this letter as a template for contacting their own school board representatives or building a coalition amongst local education and advocacy organizations in your state.

College Campuses

Fight for the Future in partnership with Students for Sensible Drug Policy **just launched a campaign this month** to ban facial recognition on college campuses across the US. Whether you are a student, alumni, professor or employee you can use this platform to contact your school and take a stand against face surveillance on campus.

The campaign has also **created a toolkit** for student groups to introduce resolutions in student government and lobby administrators, including many additional resources on the subject. **If you are a student on campus today, we call on you** to leverage these resources to push back and prevent face surveillance on college campuses from continuing to spread.

HOUSING

In 2019, the Brooklyn Legal Services Tenants Rights Coalition successfully filed a motion to block efforts by the landlord to install a face recognition entry system. This is an example of how a dedicated group of people can come together to push back on the encroachment of facial recognition on their rights in their communities and homes.

We hope that the Brooklyn tenants victory can serve as a model for other tenant groups to push back against landlord installation of facial recognition until these technologies are banned from residential spaces. This fight is hitting home for people across the country as landlords continue to implement these systems on the proposed grounds of security and convenience without any protection or oversight.

Tenants can:

1. Begin by contacting **a local legal aid provider,** many of whom who may follow the example set by Brooklyn Legal Services in this case and offer subsidized services to tenants looking to challenge landlord installation of facial recognition.

2. Attend local city council meetings to inform officials about the dangers of this technology. Tenants can cite the example of the victory in Brooklyn and the steps followed by lawyers and tenants in the process.

3. Contact the Brooklyn tenants that were involved in this victory, who made express efforts to gather documentation throughout their case for the purpose of helping others:

   "That's why we're so on top of thinking about official documentation and official legislation so no one has to go through the same fight again like we did." Fabian Rogers, tenant at Atlantic Plaza Towers, Brooklyn NY

In November, 2019 Senator Cory Booker (D-NJ) introduced **The No Biometrics Barriers to Housing Act** to prohibit the use of facial recognition in *public housing* units. While this legislation is critical to prevent harmful impact on accessing fair and affordable housing for vulnerable communities, it is important to note that the bill only covers federally funded housing and therefore would not have protected groups such as the Brooklyn tenants even if it had been in place.

This highlights the need for continued vigilance as to the scope of proposed and enacted laws when it comes to the many different uses of facial recognition by the government and companies. Areas where the law falls short will require additional community and citizen-led efforts to prevent harmful use.