Why Ban Facial Recognition?

Law enforcement use of facial recognition poses a profound threat to personal privacy, political and religious expression, and the fundamental freedom to go about our lives without having our movements and associations covertly monitored and analyzed.

safety not surveillance
SNSMN.org

This technology can be used for identifying individuals in photos or videos, and law enforcement and other government agencies can use it to conduct dragnet surveillance of entire neighborhoods. Face surveillance technology is also prone to error, implicating people for crimes they haven't committed.

It has been well documented by MIT, the Georgetown Center for Privacy and Technology, and the ACLU that these error rates – and the related consequences – are far higher for women and people with darker skin.

Regardless of your race or gender – and even if these disparate error rates were addressed – face surveillance must be stopped. **Facial recognition surveillance presents an unprecedented threat to our privacy and civil liberties.** It gives governments, companies, and individuals the power to spy on us wherever we go: tracking our faces at protests, political rallies, places of worship and more.

Table of Contents

Why Ban Facial Recognition?

#1: Blanket, indiscriminate, widespread surveillance of civilian population

- It enables the automated and indiscriminate live surveillance of people as they go about their daily business, giving authorities the chance to track your every move.

#2: Inaccuracies and racial bias

- The technology is inaccurate, leading to consequences like false arrests.
- Bias on racial and gender lines leading to discrimination of minorities
    - Error rate of 0.8 percent for light-skinned men but **up to 34.7 percent** for dark-skinned women

#3: Can target and identify vulnerable groups

- Can be used to round up immigrants and refugees
- Facial Recognition can aid the efforts of controversial organizations like ICE
- Leads to more brutal detention and deportation of vulnerable communities

#4: No legal or regulatory framework

- There is no standard policy ensuring the tech can be fairly applied.
- This regulatory gap leads to abuses of power.

#5: Violates right to privacy and civil liberty protections

- Removes rightfully expected anonymity in public spaces
- Indiscriminate and large-scale surveillance whittles away right to privacy

#6: Facial recognition does not follow principle of necessity and proportionality

- A human right recognized by the United Nations is that surveillance should be necessary and proportionate. Large-scale, blanket surveillance is not proportional to finding a few criminals.

#7: Chilling effect on democracy

- Constant, indiscriminate surveillance changes and restricts behavior
- Stifles democratic culture
    - Discourages protests, encourages retaliation and punishment by the state on those who protest or dissent
- Infringes on Freedom of Assembly, Association and Expression

#8: Citizens denied consent

- Citizens often have no say in how their image is used, recorded, stored, analyzed or shared.
- Creates distrust in state, law enforcement and institutions.

#9: Automation bias

- If it's accepted that the technology is infallible, it can lead to bad decisions.
- This "automation bias" must be avoided. Machine-generated outcomes should not determine how state agencies or private corporations treat individuals.
- Trained human operators must exercise meaningful control and make decisions based in law.

#10: Private use

- The overwhelming majority of facial recognition tech is developed, sold and used by private corporations and entities.

Counterarguments and Rebuttals

Why use Facial Recognition Technology?

#1: Useful tool for identification

- Facial recognition can serve as both a forensics tool for solving crime and as a passive safety tool to scan crowds and look for wanted suspects.
- In addition, the technology can and has been used as a form of biometric identification to help streamline an authentication process.
- Certain safeguards can be put in place to protect against abuse

#2: Additional civic purposes

- Locating missing persons
- Medical emergencies
    - Example: A lone individual collapses on an empty street. A camera is recording, and it uses facial recognition to identify the individual as someone who has a serious medical condition. If the camera is also paired with a computer vision algorithm to detect when someone has involuntarily fallen over, an alert can be sent for someone to make an assessment as to whether or not emergency services need to be called.

Rebuttals

#1: Technology outpaces legislation

- Absent a broader regulatory framework, technology advances and changes faster than the government's ability to regulate it.
- Many governments lack the expertise to understand the technology, and fail to properly implement policy safeguards. This holds especially true at the municipal level, where the technology is usually provided by corporations with interests misaligned with the public good

#2: Cost-benefit analysis

- Regardless of how useful it may be in the future the technology is not mature enough to live up to the hype, and has resulted in individuals being falsely arrested. The more it's used, the more people will be falsely arrested.
- Even when it eventually becomes mature, the technology is ripe for abuse.
- The goods brought by facial recognition are better accomplished by tools and techniques we already have.

Technology Overview

Facial recognition technology is a form of computer vision, which seeks to understand and automate tasks that the human visual system can do. Computer vision tasks include methods for acquiring processing, analyzing, and understanding digital images and videos, and then extracting data from them. Computer Vision includes shape recognition, optical character recognition and more.

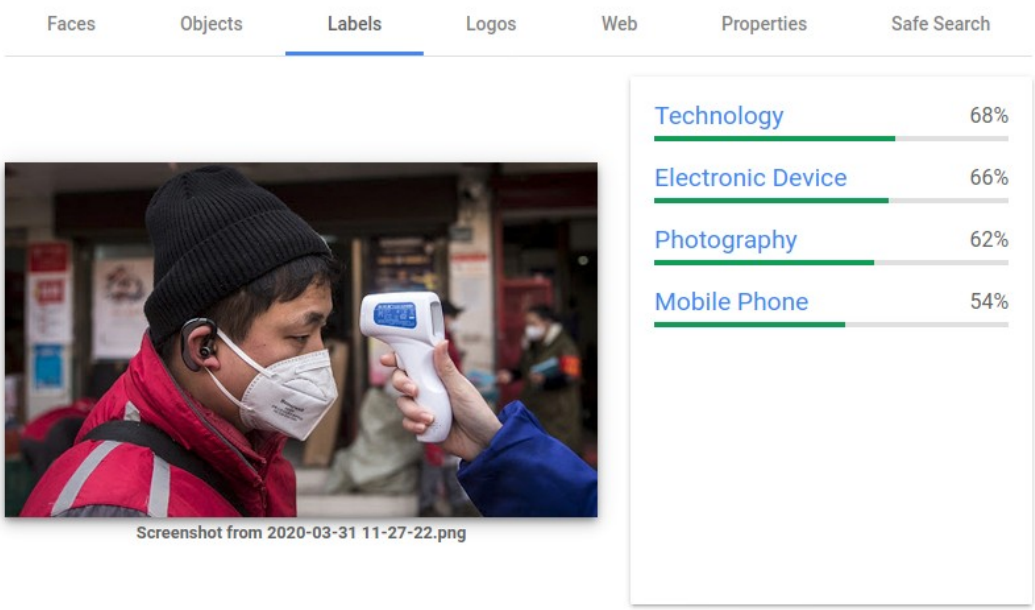


Figure 1: Example of Computer Vision

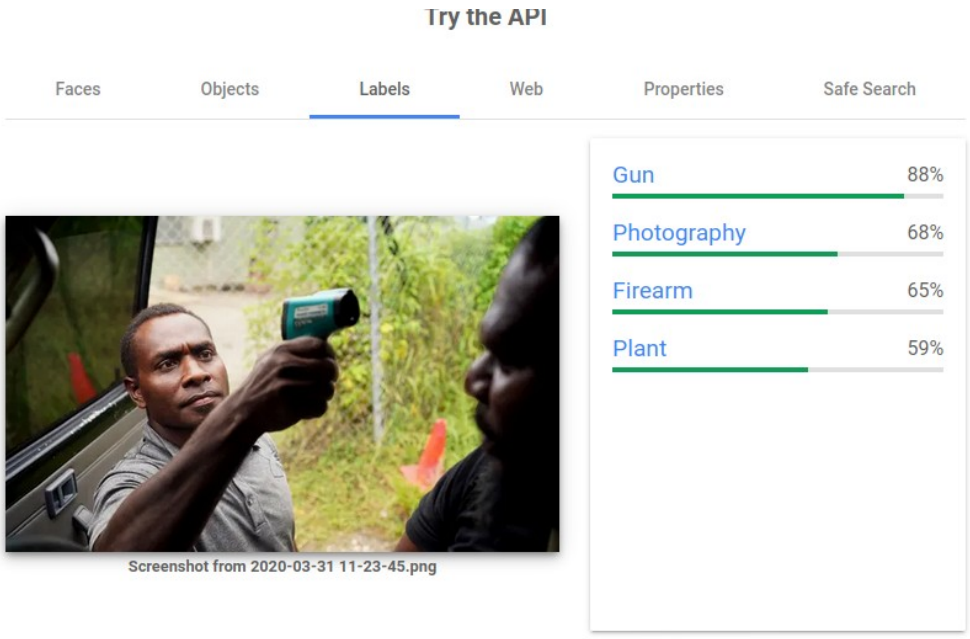


Figure 2: Example of Computer Vision

Two categories of Facial Analysis technologies:

Facial Recognition Technology (FRT) aims to both recognize and authenticate individuals with a positive identification of identity. This is achieved by extracting a feature set from a face image or video and comparing against a database.

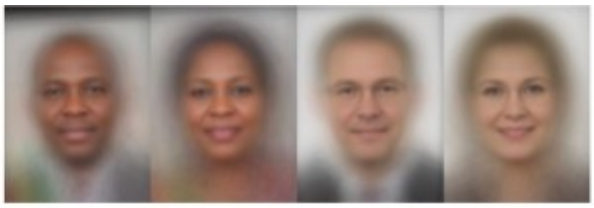
Estimation or Predictive Analysis refers to systems that rely on estimate algorithms that attempt to output a categorical quantity such as the age, emotional state or the degree of fatigue.

Both present significant civil liberty violations as well as disproportionate harms for black and minority populations.

Figure 3: Example of simple facial identification, which is the computer vision identifying that a “face” is present. *Recognition* goes further to confirm the identity.

Racial and Gender Bias

This MIT Study examined facial-analysis software from IBM, Microsoft and Face++ and uncovered an error rate of 0.8 percent for light-skinned men but **up to 34.7 percent** for dark-skinned women. Researcher Joy Buolamwini presented this research In a **United States House Committee on Oversight and Government Reform** hearing on facial recognition:



Gender Classifier	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
Microsoft	94.0%	79.2%	100%	98.3%	20.8%
FACE++	99.3%	65.5%	99.2%	94.0%	33.8%
IBM	88.0%	65.3%	99.7%	92.9%	34.4%

Figure 4: An excerpt from Joy Buolamwini's research, showing that even the most sophisticated facial analysis and facial recognition systems are markedly unreliable on darker women. Notice the gap between the lighter individuals on the right.

Zooming in on the hand and thermometer from Figure 2, we find that modifying the image so that the hand is lighter-skinned removes “gun” from the computer-generated predictions. **While such divergent outcomes may happen only occasionally, these occasional manifestations of algorithmic bias against darker-skinned people could be the decisive factor in performing a wrongful arrest.**

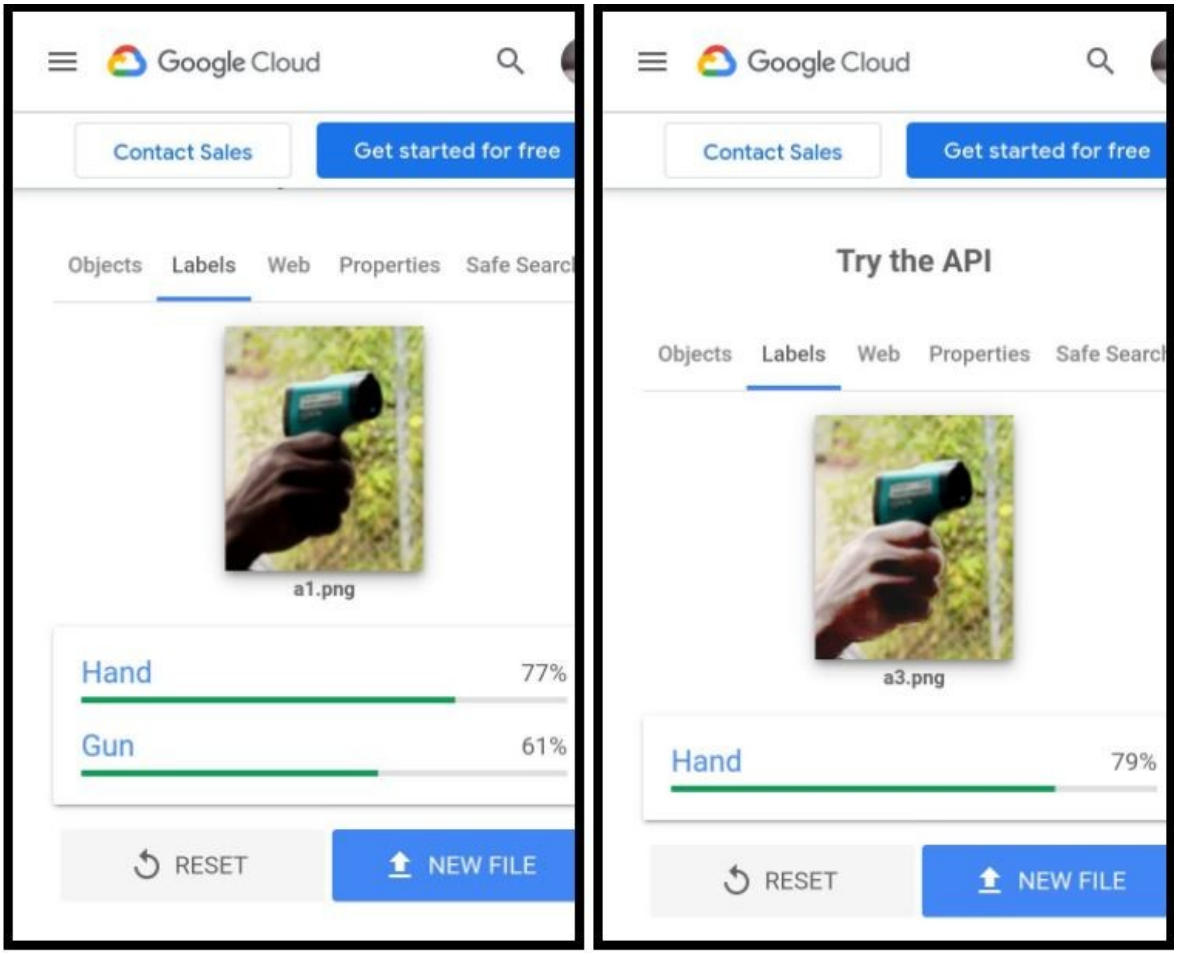


Figure 4: Impact of augmented pigmentation on computer-vision predictions.

These inaccuracies are broadly due to two factors:

1. **Unrepresentative training data:**
    1. Training data is the tool that allows machine learning technologies like facial recognition to be so powerful, allowing large datasets to be quickly analyzed.
    2. Because these tools “learn” from the training data they are given, they inherit any biases that went into the creation of those data sets
    3. So if a facial recognition algorithm is only shown faces of white men while being trained, it will be less able to identify anyone who is not a white man.

2. **Encoded bias in algorithms**
    1. Technology inherits the biases of the people who design it, and can not evolve or learn in a meaningful way beyond the parameters set by engineers.
    2. The overwhelming majority of software developers are middle-aged white men living in Silicon Valley.
    3. This lack of diversity means that errors will inevitably be introduced when these technologies interact with people and communities that exist outside the life experiences of Bay Area technologists.
    4. The way software in general is developed, starting with a "minimum viable product" and patching fixes as they are developed inevitably results in biases, bugs, and other "edge cases" not being addressed or fixed until the system is being deployed and impacting people.

History of Abuse of Private Information

Abuse of confidential databases by Police Departments in Minnesota has been widely reported:

> *"A 2013 report by the state's legislative auditor estimated more than half of Minnesota's 11,000 law enforcement users of the Driver and Vehicle Services website made questionable searches in fiscal year 2012."*
>
> *"The auditor's report came after several high-profile cases, including that of a former Department of Natural Resources employee charged with illegally viewing the driver records of at least 5,000 people, mostly women. A Minnesota police officer who sued several agencies after her driver's license information was snooped received more than $1 million in settlements."*

Even when not being actively malicious and abusing confidential information, a combination of the culture of secrecy and technical ineptitude has led to *accidental* breaches of private information.

Nationwide, the Associated Press reports that nationally, hundreds of offices receive reprimands each year for abusing private information,

> *"Among those punished: an Ohio officer who pleaded guilty to stalking an ex-girlfriend and who looked up information on her; a Michigan officer who looked up home addresses of women he found attractive; and two Miami-Dade officers who ran checks on a journalist after he aired unflattering stories about the department."*

Given unfettered access to facial recognition software will certainly expose vulnerable citizens to the asymmetrical power of officers and agents of the government.

Sources and Additional Reading

Facial Recognition Ban Ordinances:

Model bill from the Electronic Frontier Foundation. Direct Links to ordinance language (you can download copy's of the language from our nextcloud):

- Alameda, (CA)
- Boston (MA) ordinance;
- Berkeley (CA) ordinance;
- Brookline (MA) ordinance
- Cambridge (MA) ordinance;
- Easthampton, (MA)
- Jackson, (MS) ordinance direct link to language
- Madison, (WI)
- Minneapolis, (MN) ordinance
- New Orleans, (LA) ordinance
- Northampton (MA) ordinance
- Oakland (CA) ordinance
- Pittsburgh, (PA) ordinance
- Portland (ME) ordinance
- Portland (OR) ordinance;
- San Francisco (CA) ordinance;
- Santa Cruz, (CA) ordinance
- Somerville (MA) ordinance;
- Springfield M Ordinance

News Stories and Sites

- "How the Police Use Facial Recognition, and Where It Falls Short" from *The New York Times*
- Ban Facial Recognition website from Fight for the Future
- "About Face" Campaign from the Electronic Frontier Foundation

Videos and Blogs

- The Coded Gaze: Bias in Artificial Intelligence | Equality Summit with Joy Buolamwini
- "We Must Fight Face Surveillance to Protect Black Lives" by Joy Buolamwini
- "Ban Facial Recognition" Overview from Fight for the Future

Papers

- Buolamwini, Joy and Timnit Gebru. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. 2018
- Fidler, Mailyn. Local police surveillance and the administrative Fourth Amendment. 2020.
- Ho, Daniel E. et al. Evaluating Facial Recognition Technology: A Protocol for Performance Assessment in New Domains. 2020.

- Lynch, Jennifer. Face Off: Law Enforcement Use of Face Recognition Technology. 2019.
- Reisman, Dillon et al. Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability. 2018.
- United States House Committee on Oversight and Government Reform. 2019.