PRESS PAUSE 2.0 ON FACE SURVEILLANCE

ACLU Massachusetts

FACE SURVEILLANCE 101

WHAT IS FACE SURVEILLANCE?

Face surveillance – also known as facial recognition or facial analysis – means using computer programs to analyze images of human faces. Many face surveillance systems are designed to identify and track people, without their knowledge or consent.

HOW DOES FACE SURVEILLANCE WORK?

In most cases, a computer program analyzes an image of a person's face, taking measurements of their facial features to create a unique "faceprint." This faceprint, together with surveillance cameras and databases like the RMV's driver's license images, can be used to identify and track a person wherever they go.

HOW IS FACE SURVEILLANCE USED RIGHT NOW?

Governments can use face surveillance technology in three primary ways:

Identifying: Authorities have a photo, image, or even a drawing of someone they want to identify. Using face recognition, authorities can automatically scan vast databases of labeled images (for example, a driver's license database) to find one or more faceprints that may "match" their photo.

Tracking: Authorities may already know a person's identity, but they want to track that person's real-time or past activities. Authorities can use networks of surveillance cameras to track multiple faceprints, using automation software to build persistent records of every person's movements, habits, and associations. The Chinese government uses this tactic to surveil ethnic minorities, and the Moscow police have used it to target dissidents.

Analyzing: So-called "emotion detection" or "affect recognition" technology is supposed to read emotions based on a person's facial expression. Authorities could attempt to use face surveillance technology to assess people as aggressive or threatening, for example. But an expert review of over 1,000 studies found that there is no scientific basis for this technique.

WHO CREATES FACE SURVEILLANCE PROGRAMS?

Large tech companies such as Amazon, Motorola, and Microsoft — as well as smaller start-ups like Clearview AI — sell face surveillance products, which companies often market aggressively to government agencies and other companies.

WHO USES FACE SURVEILLANCE?

We know federal agencies like ICE and the FBI use face surveillance. We also know that the Massachusetts State Police, the Registry of Motor Vehicles, and some local police use this technology. In some states, school districts are also using the technology. Without adequate regulations in Massachusetts or nationwide, we do not have a complete view of the government's use of face surveillance in our Commonwealth.

IS FACE SURVEILLANCE ACCURATE?

No. The technology is not ready for primetime. For example, a face surveillance manufacturer promoting his technology in Massachusetts admitted it might work only 30% of the time and could result in as many as one false positive "hit" per day. The federal government's own research has also shown that face surveillance technology does not work as well when examining the faces of people with darker skin, women, elderly people, and children.

WHAT IS A "CONFIDENCE THRESHOLD?"

When users perform a scan using face surveillance technology, the program produces results based on a probability score. In other words, the program will tell the user, not whether the faces in different photos match, but how likely it is that they match. Most programs allow users to set a minimum probability that must be reached before images register as a possible match. This is the "confidence threshold." Companies generally provide recommended guidelines for confidence thresholds, but typically, they do not require users to abide by these suggestions. In many systems, users can set whatever thresholds they want.

ARE THERE ANY LAWS GOVERNING FACE SURVEILLANCE?

In the United States, there is no federal law regulating government use of face surveillance technology. A Massachusetts statute putting very limited restrictions on police use of facial recognition will go into effect in July 2021. The law does not require police to obtain a warrant to perform face recognition searches, and does not prevent governments from using the technology to track us as we go about our daily lives.

Seven municipalities in Massachusetts have banned face surveillance in local government: Boston, Brookline, Cambridge, Easthampton, Northampton, Springfield, and Somerville.

WHY IS FACE SURVEILLANCE DANGEROUS?

Face surveillance is dangerous when it works, and when it doesn't work.

It's biased. The federal government has found that many face surveillance programs too often fail when examining the faces of people of color, especially Black women. Other studies have found that face surveillance algorithms often mislabel Black women as men, and falsely assess Black men as angry or contemptuous. Bias in these technical systems exacerbates existing disparities in the policing and criminal legal systems, putting Black people in particular in danger of police harassment or worse. Recently, reporters have covered multiple separate cases of people being wrongfully arrested due to errors in facial recognition systems; in each case the wrongfully arrested person was a Black man.

It facilitates unprecedented and unacceptable government intrusion. Face surveillance hands broad, sweeping power to government agencies, allowing them to track ordinary people wherever we go. You can refuse a search, you can remain silent, but you can't hide your face or leave it at home. In a police state, people are forced to carry and produce ID wherever they go. Face surveillance threatens to make this a reality for everyone in the United States—which is why we must stop it.

WHAT CAN WE DO?

We can demand that our state legislature prohibit the use of face surveillance technology to track us in public and strengthen existing protections in the law. We can also ban the technology at the local level.

TO LEARN MORE OR TAKE ACTION, VISIT ACLUM.ORG/PRESSPAUSE.

PRESS PAUSE 2.0 ON FACE SURVEILLANCE

ACLU Massachusetts