**FACE SURVEILLANCE 101**

WHAT IS FACE SURVEILLANCE?

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

HOW DOES FACE SURVEILLANCE WORK?

In most cases, a computer program will analyze 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 records, can be used to identify and track a person wherever they go.

HOW IS FACE SURVEILLANCE USED RIGHT NOW?

Governments are currently using face surveillance technology in three ways:

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

**Tracking:** Authorities may already know a person’s identity, but they want to track that person in real time and retroactively. 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.

**Analyzing:** So-called “emotion detection” or “affection recognition” technology purports to be able to read emotions based on a person’s facial expression. This means that authorities can attempt to use face surveillance technology to assess people as aggressive or threatening, for example. 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, IBM, and Microsoft — as well as smaller start-ups — have face surveillance products, which they market aggressively to governments and private buyers alike.

WHO USES FACE SURVEILLANCE?

We know that 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. Without any oversight laws or 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. This 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. Academic research has also shown that face surveillance technology frequently misclassifies darker-skinned faces and women.

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 you, 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 match. This is the “confidence threshold.” Companies will provide recommended guidelines for confidence thresholds, but nothing requires 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 are no laws or regulations governing the sale, acquisition, use, or misuse of face surveillance technology by government agencies. As of August 2019, the only exceptions are municipal bans on face surveillance in San Francisco and Oakland, California, as well as Somerville, Massachusetts. Cambridge, Massachusetts is currently considering a face surveillance ban, and a proposal to establish a statewide moratorium is currently before legislators on Beacon Hill.

WHY IS FACE SURVEILLANCE DANGEROUS?
Face surveillance is dangerous when it works, and when it doesn’t work.

It’s biased. Research, including studies at MIT, has shown that some of the most popular face surveillance programs fail to correctly classify people of color, especially Black women. For example, these programs will often mislabel Black women as men, or falsely assess Black men as aggressive. This threatens to exacerbate the already serious problems of racial bias in our criminal justice system, where police are prone to treat Black men as hostile, even when they are attempting to cooperate with officers. Philando Castile was shot and killed while trying to produce his ID.

It facilitates unprecedented government intrusion. Face surveillance hands broad, sweeping power to government agencies, allowing them to track ordinary people wherever they 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.

WHAT CAN WE DO?
We can demand that our state government pass a moratorium on face surveillance, so that we can establish safeguards to protect our basic constitutional rights.

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