10 reasons you should be worried about facial recognition technology

August 22 2019, by Birgit Schippers

Credit: AI-generated image (disclaimer)

Facial recognition technology is spreading fast. Already [widespread in China](China), software that identifies people by comparing images of their faces against a database of records is now being adopted across much of the rest of the world. It's common among police forces but has also been used at airports, railway stations and shopping centers.

The rapid growth of this technology has triggered a much-needed debate. Activists, politicians, academics and even police forces are expressing serious concerns over the impact facial recognition could have on a political culture based on rights and democracy.

Human rights concerns

As someone who researches the future of human rights, I share these concerns. Here are ten reasons why we should worry about the use of facial recognition technology in public spaces.

(1) It puts us on a path towards automated blanket surveillance

CCTV is already widespread around the world, but for governments to use footage against you they have to find specific clips of you doing something they can claim as evidence. Facial recognition technology brings monitoring to new levels. 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) It operates without a clear legal or regulatory framework

Most countries have no specific legislation that regulates the use of facial recognition technology, although some lawmakers are trying to change this. This legal limbo opens the door to abuse, such as obtaining our images without our knowledge or consent and using them in ways we would not approve of.

(3) It violates the principles of necessity and

proportionality

A commonly stated human rights principle, recognized by organizations [from the UN](#) to the [London Policing Ethics Panel](#), is that surveillance should be necessary and proportionate. This means surveillance should be restricted to the pursuit of serious crime instead of enabling the unjustified interference into our liberty and fundamental rights. Facial recognition technology is at odds with these principles. It is a technology of control that is symptomatic of the state's mistrust of its citizens.

(4) It violates our right to privacy

The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from [private companies](#). Facial recognition technology's indiscriminate and large-scale recording, storing and analyzing of our images [undermines this right](#) because it means we can no longer do anything in public without the state knowing about it.

Credit: AI-generated image ([disclaimer](#))

(5) It has a chilling effect on our democratic political culture

Blanket surveillance can deter individuals from attending public events. It can stifle participation in political protests and campaigns for change. And it can discourage nonconformist behavior. This chilling effect is a serious infringement on the right to freedom of assembly, association, and expression.

(6) It denies citizens the opportunity for consent

There is a lack of detailed and specific information as to how facial recognition is actually used. This means that we are not given the opportunity [to consent](#) to the recording, analysing and storing of our

images in databases. By denying us the opportunity to consent, we are denied choice and control over the use of our own images.

(7) It is often inaccurate

Facial recognition technology promises accurate identification. But numerous studies have highlighted how the algorithms trained on racially biased data sets misidentify people of color, especially women of color. Such algorithmic bias is particularly worrying if it results in unlawful arrests, or if it leads public agencies and private companies to discriminate against women and people from minority ethnic backgrounds.

(8) It can lead to automation bias

If the people using facial recognition software mistakenly believe 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 take decisions based in law.

(9) It implies there are secret government watchlists

The databases that contain our facial images should ring alarm bells. They imply that private companies and law enforcement agencies are sharing our images to build watchlists of potential suspects without our knowledge or consent. This is a serious threat to our individual rights and civil liberties. The security of these databases, and their vulnerability to the actions of hackers, is also cause for concern.

(10) It can be used to target already vulnerable groups

Facial recognition technology can be used for blanket surveillance. But it can also be deployed selectively, for example to identify migrants and refugees. The sale of facial recognition software to agencies such as the controversial US Immigration and Customs Enforcement (ICE), which has been heavily criticized for its tactics in dealing with migrants, should worry anyone who cares for human rights. And the use of handheld mobile devices with a facial recognition app by police forces raises the spectre of enhanced racial profiling at the street level.

Debate sorely needed

With so many concerns about facial recognition technology, we desperately need a more prominent conversation on its impact on our rights and civil liberties. Without proper regulation of these systems, we risk creating dystopian police states in what were once free, democratic countries.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation