Regulate facial-recognition technology

Until appropriate safeguards are in place, we need a moratorium on biometric technology that identifies individuals, says **Kate Crawford**.

Earlier this month, Ohio became the latest of several state and local governments in the United States to stop law-enforcement officers from using facial-recognition databases. The move followed reports that the Immigration and Customs Enforcement agency had been scanning millions of photos in state driver's licence databases, data that could be used to target and deport undocumented immigrants. Researchers at Georgetown University in Washington DC used public-record requests to reveal this previously secret operation, which was running without the consent of individuals or authorization from state or federal lawmakers.

It is not the only such project. Customs and Border Protection is using something similar at airports, creating a record of every passenger's departure. The technology giant Amazon is building partnerships with more than 200 police departments to promote its Ring home-security cameras across the United States. Amazon gets ongoing access to video footage; police get kickbacks on technology products.

Facial-recognition technology is not ready for this kind of deployment, nor are governments ready to keep it from causing harm. Stronger regulatory safeguards are urgently needed, and so is a wider public debate about the impact it is already having. Comprehensive legislation must guarantee restrictions on its use, as well as transparency, due process and other basic rights. Until those safeguards are in place, we need a moratorium on the use of this technology in public spaces.

There is little evidence that biometric technology can identify suspects quickly or in real time. No peer-reviewed studies have shown convincing data that the technology has sufficient accuracy to meet the US constitutional standards of due process, probable cause and equal protection that are required for searches and arrests.

Even the world's largest corporate supplier of police body cameras — Axon in Scottsdale, Arizona — announced this year that it would not deploy facial-recognition technology in any of its products because it was too unreliable for police work and "could exacerbate existing inequities in policing, for example by penalizing black or LGBTQ communities". Three cities in the United States have banned the use of facial recognition by law-enforcement agencies, citing bias concerns.

They are right to be worried. These tools generate many of the same biases as human law-enforcement officers, but with the false patina of technical neutrality. The researchers Joy Buolamwini at Massachusetts Institute of Technology in Cambridge and Timnit Gebru, then at Microsoft Research in New York City, showed that some of the most advanced facial-recognition software failed to accurately identify dark-skinned women 35% of the time, compared to a 1% error rate for white men. Separate work showed that these technologies mismatched 28 US members of Congress to a database of mugshots, with a nearly 40% error rate for members of colour. Researchers at the University of Essex in Colchester, UK, tested a facial-recognition technology used by London's Metropolitan Police, and found it made just 8 correct matches out of a series of 42, an error rate they suspect would not be found lawful in court. Subsequently, a parliamentary committee called for trials of facial-recognition technology to be halted until a legal framework could be established.

But we should not imagine that the most we can hope for is technical parity for the surveillance armoury. Much more than technical improvements are needed. These tools are dangerous when they fail and harmful when they work. We need legal guard rails for all biometric surveillance systems, particularly as they improve in accuracy and invasiveness. Accordingly, the AI Now Institute that I co-founded at New York University has crafted four principles for a protective framework.

First, given the costly errors, discrimination and privacy invasions associated with facial-recognition systems, policymakers should not fund or deploy them until they have been vetted and strong protections have been put in place. That includes prohibiting links between private and government databases.

THESE TOOLS ARE DANGEROUS WHEN THEY FAIL AND HARMFUL WHEN THEY WORK.

Second, legislation should require that public agencies rigorously review biometric technologies for bias, privacy and civil-rights concerns, as well as solicit public input before they are used. Agencies that want to deploy these technologies should be required to carry out a formal algorithmic impact assessment (AIA). Modelled after impact-assessment frameworks for human rights, environmental protection and data protection, AIAs help governments to evaluate artificial-intelligence systems and guarantee public input.

Third, governments should require corporations to waive any legal restrictions on researching or overseeing these systems. As we outlined in the AI Now Report 2018, tech companies are currently able to use trade-secrecy laws to shield themselves from public scrutiny. This creates a legal 'black box' that is just as opaque as any algorithmic 'black box', and serves to shut down investigations into the social implications of these systems.

Finally, we need greater whistle-blower protections for technology-company employees to ensure that the three other principles are working. Tech workers themselves have emerged as a powerful force of accountability: for example, whistle-blowers revealed Google's work on a censored search engine in China. Without greater protections, they are in danger of retaliation.

Scholars have been pointing to the technical and social risks of facial recognition for years. Greater accuracy is not the point. We need strong legal safeguards that guarantee civil rights, fairness and accountability. Otherwise, this technology will make all of us less free. ■

Kate Crawford *is a distinguished research professor and co-director of the AI Now Institute at New York University, and a principal researcher at Microsoft Research in New York City.*
Twitter: @katecrawford