The Automated Facial Recognition System (AFRS) recently proposed by the Ministry of Home Affairs is geared towards modernising the police force, identifying criminals, and enhancing information sharing between police units across the country. The AFRS will use images from sources like CCTV cameras, newspapers, and raids to identify criminals against existing records in the Crime and Criminal Tracking Networks and System (CCTNS) database.

The Home Ministry has clarified that this will not violate privacy, as it will only track criminals and be accessed only by law enforcement. However, a closer look at facial recognition systems and India’s legal framework reveals that a system like the AFRS will not only create a biometric map of our faces, but also track, classify, and possibly anticipate our every move.

Technically speaking, it is impossible for the AFRS to be truly used only to identify, track and verify criminals, despite the best of intentions. Recording, classifying and querying every individual is a prerequisite for the system to work.

**Assumed guilty**

The system will treat each person captured in images from CCTV cameras and other sources as a potential criminal, creating a map of her face, with measurements and biometrics, and match the features against the CCTNS database. This means that we are all treated as potential criminals when we walk past a CCTV camera – turning the assumption of “innocent until proven guilty” on its head.

It is assumed that facial recognition will introduce efficiency and speed in enforcing law and order. However, the evidence suggests otherwise. In August 2018, a facial recognition system used by the Delhi police was reported to have an accuracy rate of only 2%. This is a trend worldwide, with similar levels of accuracy reported in the U.K. and the U.S.

Accuracy rates of facial recognition algorithms are particularly low in the case of minorities, women and children, as demonstrated in multiple studies across the world. Use of such technology in a criminal justice system where vulnerable groups are over-represented makes them susceptible to being subjected to false positives (being wrongly identified as a criminal). Image recognition is an extremely difficult task, and makes significant errors even in laboratory settings. Deploying these systems in consequential sectors like law enforcement is ineffective at best, and disastrous at worst.

**Fears of mass surveillance**

Facial recognition makes data protection close to impossible as it is predicated on collecting publicly available information and analysing it to the point of intimacy. It can also potentially trigger a seamless system of mass surveillance, depending on how images are combined with other data points. The AFRS is being contemplated at a time when India does not have a data protection law. In the absence of safeguards, law enforcement agencies will have a high degree of discretion. This can lead to a mission creep. The Personal Data Protection Bill 2018 is yet to come into force, and even if it does, the exceptions contemplated for state agencies are extremely wide.

The notion that sophisticated technology means greater efficiency needs to be critically analysed. A deliberative approach will benefit Indian law enforcement, as police departments around the world are currently learning that the technology is not as useful in practice as it seems in theory. Police departments in London are under pressure to put a complete end to use of facial recognition systems following evidence of discrimination and inefficiency. San Francisco recently implemented a complete ban on police use of facial recognition. India would do well to learn from their mistakes.

Vidushi Marda is a lawyer and researcher at Article 19, a human rights organisation.