

# **Critique of Kate Crawford's Regulate Facial-Recognition Technology**

Sarthak Behera

October 2021

Facial recognition has undoubtedly gained prominence over the past few years. Initially, it was used for security and surveillance but its winsome appeal and wide applicability bubbled over to other disparate domains like medical diagnosis, ID verification, facilitation of secure transactions, attendance systems, forensic investigations, biometric checks, unlocking phones, smart advertising, etc. They are predominantly used to identify people through faces which acts as their digital signature. In spite of face recognition achieving great eminence, the author raises concern about its unethical usage and propounds moratorium on its utilization until proper safeguards are put in place.

The author begins with reports of unethical and discriminatory operation of facial recognition in government departments like Immigration and Customs, Enforcement and Police where facial data is accumulated without consent from concerned individuals to track and target them. Then she proposes temporary shut-down of this technology till comprehensive legislation guarantees transparency and ethical utilization. It is indeed very concerning when agencies use sensitive facial data in such unscrupulous ways but cessation of its usage altogether seems harsh and callous. Face recognition is now ubiquitous with smartphones employing them for contact-less unlocks and corporations harnessing them for quick ID and biometric attendance checks. Clamping down on these systems might have widespread negative impact perpetuating across various sectors and industries. She also voices concern with reference to the accuracy of these models. She opines that these systems are inherently filled with biases analogous to human operators handling these systems thereby delivering specious 'technically-neutral' results. People of color are spuriously stereotyped. This is truly disquieting and lays bare the current limitations of these models. But one must note that these models are mere ancillary to law enforcement agencies and in no way can they be presented as evidence for crime. Ultimately, it is the human judgement that determines the criminal. These models only work when current input is from similar distribution to training dataset. Thus, instead of utterly discarding these systems, giving negative feedback in cases of false positives may mitigate inherent biases and seems a more sensible and rational approach.

The writer proposes steps to tackle with some of the insidious effects of face recognition technology. She demands policymakers to discard this technology until strong protections against its abuse are in place. These systems should be screened before utilization against potential prejudices. Furthermore, stringent regulations curtailing corporations from using these databases immorally can safeguard against adverse social implications. Finally, she also vouches for greater whistle-blower protections to enhance accountability within corporations. These steps might hinder the progress of face-recognition technology due to data privacy concerns which in turn might hamper advancement in technical accuracy of these models. This trade-off remains a moot point.

All-in-all, this article serves as reality-check for the heavily hyped face recognition technology. Concerns regarding inaccuracies, inherent prejudices, identity theft, etc. are all well founded. Governments in various countries are now more sensitive about privacy concerns and have embarked on regulations to safeguard people's freedom. Until robust measures are in place, face recognition systems should only act as buttress for critical government agencies and in no way act as substitute for fair human judgement. Corporations should refrain from violating people's privacy and lawmakers should bring in stringent data protection laws in this regard.