NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief
No. 759 – 13 March 2020

AI and Facial Recognition in India

Karthik Nachiappan

Summary

Indian Home Minister Amit Shah's admission of his government's use of facial recognition technologies to detect perpetrators of the Delhi riots has renewed questions concerning the governance of these technologies.

Speaking in the Lok Sabha on 12 March 2020, India's Home Minister Amit Shah revealed, rather unexpectedly, that the Narendra Modi government has used facial recognition software to root out instigators of the recent violent riots in New Delhi. The stunning admission, seemingly off the cuff, has reopened discussions on using facial recognition without proper constraints and how to best regulate a technology that could have serious repercussions on national security, privacy and citizens' rights. How Delhi handles this question could influence the approach taken by various Indian states that are already deploying such methods for law and order purposes. It appears as though the Modi government has decided to veer towards the former (national security) at the expense of the latter.

Some Delhi residents have sent captured video footage of the riots as it unfolded last month to police authorities who have since compared the footage with existing individual data, including voter identity and driver license, held by the government. Shah disclosed that this data was fed into a facial recognition software that was used to identify 1,100 people who participated in the violence. Shah also suggested that the data revealed around 300 people involved were from Uttar Pradesh, a development, he claims, is indicative of a 'deep conspiracy' behind the conflagration. Questions from Shah's legislative disclosures have not centred around whether nefarious elements from neighbouring states were involved in the riots and reasons thereof but around the technology used to arrive at this judgment and of the implications from the continued use of such technologies by law enforcement agencies.

Facial recognition refers to technologies, largely based on artificial intelligence (AI), that uses biometric data collected from citizens to identify an individual based on facial patterns. Specifically, there are two types of facial recognition. The first is one-on-one recognition or when an existing database possesses an individual's facial image which is then corroborated by the individual who provides an image to confirm. The second is one-to-many recognition or when an individual's image is captured and used to confirm identity through an existing database. The Indian government has relied on facial recognition methods to bolster its law enforcement capabilities, particularly in criminal identification. Soon, plans are afoot to establish a nation-wide Automated Facial Recognition System (AFRS) to streamline and quicken the process of criminal identification. Once operational, this system could extract an image from a video and match it to an image that exists in a related government database. However, the government's intent to have this system up and running could run up against thorny concerns related to privacy, transparency and security. How the government squares these considerations will end up determining its regulatory approach vis-a-vis AI that drives facial recognition techniques.

In terms of benefits, law enforcement officials trust facial recognition technologies will enhance the state's ability to detect criminal behaviour and patterns by matching facial images to a vast data repository. Officials insist this tool should assist in crime prevention and detection, finding missing children, ensuring public safety, curbing human trafficking and maintaining law and order. In terms of data, the AFRS is expected to harvest images from multiple sources, including newspapers, police intelligence and closed-circuit television feeds, plus use existing data from the Crime and Criminal Tracking Networks and Systems portal. To assuage critics fearful of such facial recognition methods, government officials from the National Crime Records Bureau stipulate that images collected and stored in the database will not be used unless 'the video footage is part of a crime' or they will not be used arbitrarily. Yet, reassurances have not dealt with the raft of concerns raised by civil society groups on the efficacy and use of facial recognition technologies, particularly the one-to-many facial recognition approach.

Resistance to facial recognition stems from notions that the data fed into systems to detect individuals will not be robust and accurate, making them open to errors in judgment. It is also unclear, opponents assert, whether existing data will be able to clarify images, given differences in gender, race and ethnicity, all biases that ostensibly constrain the utility of facial recognition. Without adequate protections around data, civil society groups also question the ways through which private data is collected without sufficiently notifying citizens whose privacy is potentially compromised. Government officials will have to consider whether public safety and crime prevention should rest on the shoulders of mass surveillance. The use of facial recognition could also be in contravention of the Indian Supreme Court's 2017 Puttaswamy judgment which reaffirmed the right to privacy that also extends to public spaces which effectively bars the unlawful collection of personal data. The lack of a final data protection bill in India gives the Modi government discretion to design and operationalise facial recognition systems under the pretext of national security and law and order. Indeed, the most recent draft of India's data protection legislation grants exemptions to the government on national security grounds.

The Modi government appears keen to use facial recognition technologies to advance state, principally security, interests at the expense of constitutional, legal and ethical considerations. Should the new data protection law bifurcating the obligations of the state and other actors pass, robustly regulating AI and its different application like facial recognition will become more difficult.

. . . . .

Dr Karthik Nachiappan is Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg. The author bears full responsibility for the facts cited and opinions expressed in this paper.