

The dangers of facial-recognition technology in Indian policing

Thursday 1 June 2023, by [DHARMARAJ Nikhil](#) (Date first published: 26 May 2023).

CCTV cameras and facial recognition systems are surveillance tools that carry on the legacy of analogue technologies in stereotyping and targeting specific communities.

“When we don’t trust the police, how can we trust their cameras? Even the British would have behaved better than the Delhi Police at some point of time.” Sitting on the first floor of an apartment in north-east Delhi, a young Muslim man said this while recounting to me how Hindu mobs perpetrated communal violence over three days in February 2020. “I had to throw children, one- or two-month-old babies, down from the second story, had to make women jump down two floors,” he said. “Somehow, we escaped.”

Along with Hindu mobs, Delhi Police personnel were also accused of being involved in attacking Muslims. The media reported how the police did not register first-information reports based on complaints made by Muslims which incriminated members of the Bharatiya Janata Party for leading the violence. Forty of the 53 dead were Muslim. The police charged Muslim men even in cases where the victims were from the same community.

On 12 March 2020, the union home minister, Amit Shah, told the Rajya Sabha that the Delhi Police had used facial-recognition technology to identify nearly two thousand individuals as instigators of violence. Over the next year, FRT systems led to 137 arrests. Even as there was no legal framework to regulate the use of the tool in the country, the infrastructure was already in place. A quarter million state-sponsored CCTV cameras had been installed in Delhi by 2019, while another three hundred thousand were slated to be added. Governments had begun automating the recognition and identification of individuals from CCTV footage via FRT. When the Internet Freedom Foundation, a digital-rights advocacy group, inquired, in a right-to-information application, about the legality of the Delhi Police’s use of the technology, the force cited a 2018 high-court judgment that directed it to use the tool for tracking missing children. The IFF called this a worrying “function creep.”

According to a working paper by the think tank Vidhi Centre for Legal Policy, as of August 2021, “given the fact that Muslims are represented more than the city average in the over-policed areas, and recognising historical systemic biases in policing Muslim communities in India in general and in Delhi in particular, we can reasonably state that any technological intervention that intensifies policing in Delhi will also aggravate this bias.” The use of FRT by the Delhi Police, it adds, “will almost inevitably disproportionately affect Muslims.” These findings are a cause for immense concern, especially in view of the fact that 126 FRT systems are in use across the country.

FRT systems aim to “use the face like a fingerprint,” the technology scholar Kelly Gates writes in her 2011 book, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. “Simply by nature of being computerized, facial recognition systems are deemed more accurate and objective and less subject to the prejudices and apparent inadequacies of human perception.” However, she goes on to state that most modern FRT systems “are designed to make use of an

archive of facial images that define the parameters for the class of individuals that the system will identify,” which ultimately ends up facilitating “the diffusion of particular institutionalized ways of seeing.”

In essence, just because CCTV cameras and FRT are modern surveillance tools does not mean they do not have the same pitfalls as previous technologies. Instead, they carry on the legacy of analogue technologies in stereotyping and targeting specific communities. This is primarily because, in terms of surveillance and data collection, the aspirations of the Indian government appear to have remained the same as they were under the British Raj.

To begin, the police is predisposed to target marginalised communities due to the enduring cultural notion of hereditary criminality. The Manusmriti, for instance, delineates a linkage between caste and crime, explicitly stating that a judge investigating a case must “examine a Brahmana (beginning with) ‘Speak,’ a Kshatriya (beginning with) ‘Speak the truth,’ a Vaisya (admonishing him) by (mentioning) his kine, grain, and gold, a Sudra (threatening him) with (the guilt of) every crime that causes loss of caste.”

Such prejudice persisted during, and after, the colonial era. After some vernacular newspapers campaigned for the criminalisation of certain communities, which they deemed morally promiscuous and prone to bad behaviour by birth, the British passed the Criminal Tribes Act of 1871. The legislation stated that if local administrators had “reason to believe” that a certain community was “addicted to the systematic commission of non-bailable offences,” they could, with the governor general’s approval, declare the community as a criminal tribe. The Code of Criminal Procedure, 1898 also explicitly referred to “habitual offenders.”

According to the historian Mira Rai Waits, colonial authorities believed “that if one observed the exterior traits of an individual one could then obtain empirical information about that individual’s interior character and propensity for certain kinds of behaviour. In other words, British colonialists were searching for a way of detecting what they saw as native treachery through visual analysis of physical features.” Following the Revolt of 1857, British administrators began installing full-fledged systems of biometric surveillance and the collection of ethnographic data, including fingerprints and photographs.

Although not widely deployed, the profiloscope was a crucial biometric technology that emerged in this context. Developed in the 1930s by the Brahmin statistician Prasanta Chandra Mahalanobis, it was a measuring instrument supposedly used to determine a person’s race. The profiloscope deployed a metric of statistical similarity, initially formulated in the context of distinguishing caste groups, that the historian Projit Mukharji describes as a “Risleyan race-technology”—referring to the phrenological writings of the ethnographer and colonial administrator Herbert Risley. Risley influenced the anthropometric practices of the time through ludicrous pronouncements, such as “the social position of a caste varies inversely as its nasal index.” A 2021 paper by the historians Simon Michael Taylor, Kalervo N Gulson and Duncan McDuie-Ra calls the profiloscope an “early version of facial recognition technology,” noting that the same Mahalanobis distance measure remains a central concept in contemporary machine learning and FRT algorithms.

In a 2021 paper, the sociologist Shivangi Narayan argues that the colonial practice of “preventive policing” still continues to enable selective criminalisation. The official repeal of the Criminal Tribes Act, in 1952, was just a “paper promise,” Disha Wadekar, a lawyer from one of the tribes targeted by the legislation, told Scroll. The present Code of Criminal Procedure, enacted in 1973, operationalises much the same language, and states still have legal provisions to conduct surveillance on “history-sheeters.” In practice, according to a 2021 report by the Transnational Institute, a research and advocacy organisation, this yields a similar result as in the colonial era.

Most recently, in April 2022, parliament passed the Criminal Procedure (Identification) Act, a mere reincarnation of the Identification of Prisoners Act, 1920, which permitted the police to take photographs and “measurements”—fingerprints and footprints—of “convicts and others.” The new law merely expanded the scope of the term “measurements,” which now includes, among other data, “fingerimpressions, palm-print and foot-print impressions, photographs, iris and retina scan, physical, biological samples and their analysis.”

These legal resonances make explicitly clear what is already culturally obvious: India’s modern FRT debacle is merely a rearticulation of long-established cultural and political infrastructures of repression. Narayan argues that “there is little radically new about data-driven predictive policing systems—apart from scale and speed, and interoperability of databases and the granularity of the data which only promises to accelerate social sorting, bias, and inequalities.” As the Dalit feminist writer Thenmozhi Soundararajan notes in her book *The Trauma of Caste*, “Policing does not end with the police. Under Brahminism, all aspects of our lives are dominated by a control and surveillance ethos.”

Corporate interest in facilitating surveillance tools for policing is perhaps a key difference between the old and the new. An essay published by the AI Now Institute highlights that “Big Tech is reinforcing and accelerating a system of caste-based discrimination in India and reinforcing the power and impunity of its police.” Among other instances, it speaks about the partnership between the US conglomerate Honeywell International and the Bhopal Police as well as the Surat Police’s reported use of NeoFace, an application developed by the Japanese company NEC Corporation.

To add yet another layer of concern, these systems have low bars for accurate measurement and identification. In 2018, the FRT used by the Delhi Police had a staggering accuracy rate of two percent.

More recently, in response to another RTI application by the IFF, the Delhi Police revealed that only eighty-percent accuracy is necessary for it to be considered a “positive” match. The *Economic Times* quoted an expert who said that “an 80% confidence threshold is not the right setting for public safety use cases as it is far too low to ensure the accurate identification of individuals.” This suggests that misidentification and spotty reasoning can be paired with the scientific veneer of instruments such as CCTV or FRT to indict anyone.

Given the low burden of proof required, anyone that matches a preconceived notion of criminality can now be subjected to an FRT identification and arrest. In the case of political protests or riots, this stipulation can essentially permit mass surveillance, the construction of a biometric database of dissidents, and the potential linking of facial scans with Aadhaar data. With Aadhaar’s collection of headshots for almost all welfare services across the nation, this conjoining has the potential to create FRT algorithms that quickly and easily detect any Indian citizen. For instance, the young Muslim man told me that the Delhi Police “arrested people passing by the protest site, whose faces have been captured on footage.” While the camera can claim to objectively determine a person’s presence at the site of crime, it cannot provide any comprehensive answer to questions of innocence and guilt.

As video surveillance and algorithmic detection become further automated, there is great scope for misidentification as well as discrimination, given the selective deployment of FRT algorithms. The Transnational Institute argues that the use of artificial intelligence will “provide a veneer of neutrality to India’s casteist policing, and entrench the criminalities inscribed on Vimukta and other marginalized caste communities.” In other words, CCTV cameras and FRTs are slated to do what the pseudoscientific tools of anthropometry and physiognomy did under previous casteist and colonial rule: validate stereotypes about marginalised communities as ground truths.

In May 2021, during the COVID-19 lockdown, the activist SQ Masood was traveling in Shahran Market, located in a Muslim-dominated area, towards his home in Old Hyderabad. A group of policemen randomly stopped him on the street. Masood said they photographed him without cause or consent, and then released him. Masood was not the only one who was pulled over—that day, he saw the police doing the same to several people in that area. Amnesty International has recently named Hyderabad as “one of the most surveilled cities in the world,” with these checks becoming commonplace. A command-and-control centre is reportedly being built in Banjara Hills, which would streamline and process footage from six hundred thousand city-wide CCTV cameras.

Masood suggested a clear power imbalance and selective bias in this surveillance. “Police don’t take these photographs in Banjara Hills,” he told me, “because there are educated people, there are people who belong to elite classes and business classes.” As a result, he said, it is more likely for the exercise to be repeated in slums and in Old Hyderabad. “You’re targeting a class of people,” he added. As part of its recent “Ban the Scan” campaign, Amnesty International noted that a whopping 53.7 percent of the area of Kala Pathar, the locality where Masood resides, is engulfed by CCTV cameras, as is 62.7 percent of Kishan Bagh. Both areas have a high Muslim and working-class population. Masood recounted that an additional commissioner of the Hyderabad Police once stated on Twitter that there is lots to learn from the New York Police Department—an unnerving goal, given the egregiously racist practices of the NYPD. “You can’t copy and paste a New York police model in India,” Masood said.

A recent death in Telangana appears to illustrate the dangers of surveillance technologies. In January this year, the Hyderabad Police arrested Khadeer Khan, a 36-year-old daily-wage labourer who was allegedly caught chain-snatching via CCTV footage—it is unclear if FRT was used to facilitate the arrest. However, it was then discovered that Khan had been wrongly identified. The News Minute reported that, in a video statement taken before his death, Khan “graphically described the torture inflicted on him.” He died shortly thereafter.

Ultimately, the projects of state surveillance and data collection, as well as the ethos that drive them, need to be urgently examined and dismantled. In any such conversations, it needs to be kept in mind that, across centuries, what has remained ultimately unchanged are the legal codes that support surveillance, the Brahminical need to watch and the political impulse to cement criminality based on pseudoscientific notions of caste, ethnicity and religion. Given my own positionality as a Brahmin with family ties to Silicon Valley, it is only in recent years that I have become aware of these truths as well as the need to interrogate our collective complicity in digital violence. The Indian police’s enthusiasm for FRT represents a dangerous first step into a digital dystopia that Hindu India is rapidly spiralling towards.

Nikhil Dharmaraj is a recent graduate of Harvard University, who is interested in situating contemporary AI systems within transnational structures of violence and disparity. For his senior thesis project on digital surveillance in India that aimed to trace AI Ethical complicities, Dharmaraj connected and conducted research with NGOs Karwan-e-Mohabbat, ASEEM India and the Internet Freedom Foundation.

[Click here](#) to subscribe to ESSF newsletters in English and/or French.

P.S.

The Caravan

<https://caravanmagazine.in/technology/dangers-of-facial-recognition-technology-in-indian-policing>