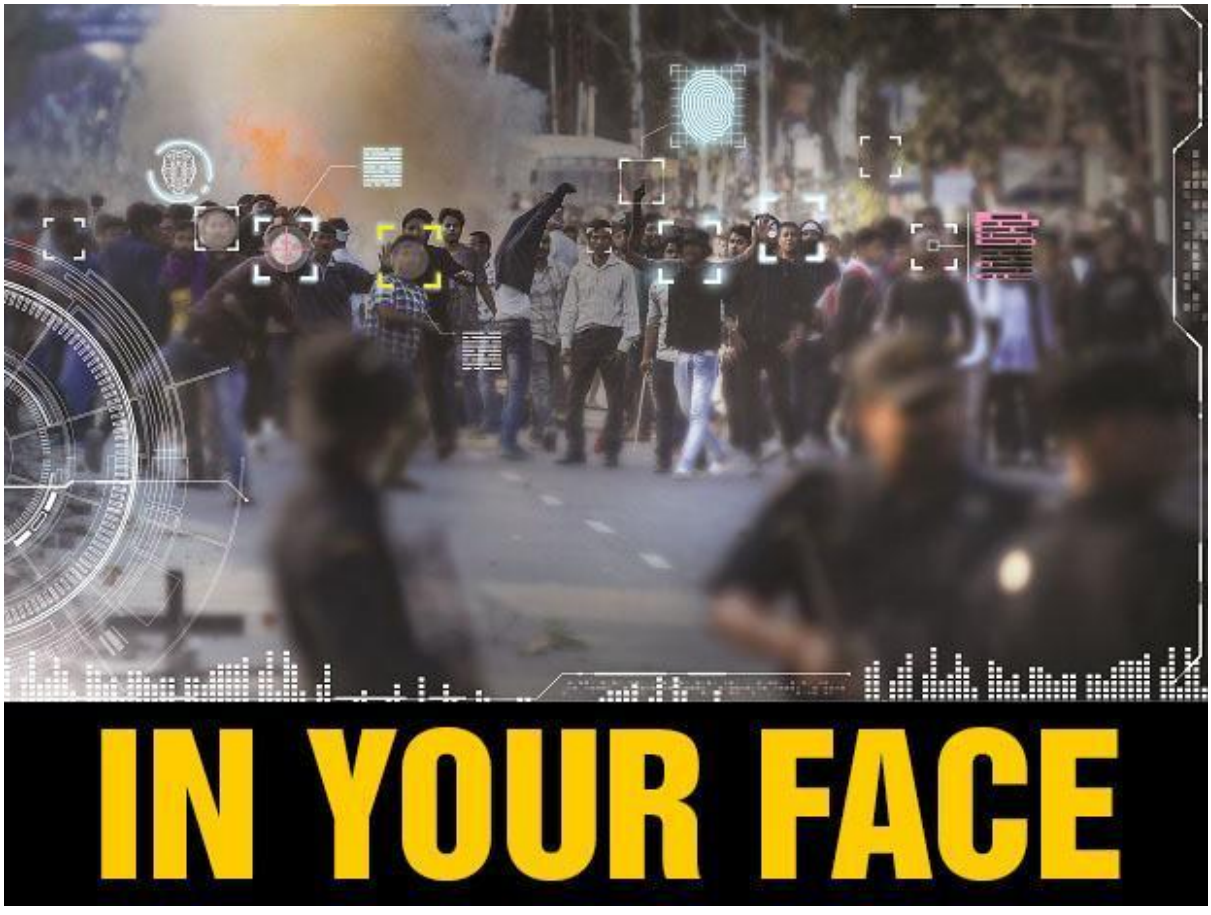
Privacy concerns over facial recognition systems aimed at ordinary citizens

Facial recognition technology can be used to identify missing children or protesting citizens, it also raises serious privacy concerns

---

Source: Business Standard- https://www.business-standard.com/article/technology/privacy-concerns-over-facial-recognition-systems-aimed-at-ordinary-citizens-120010301338_1.html

Date: Jan 3, 2020



Find someone who looks at you the way Delhi Police cameras look at protesters. It came to light recently that the capital's law enforcement agency has been using a facial recognition system to observe people who gathered to protest changes in the citizenship Act. The system, like an

overattentive lover, learns every inch of one's face, only to convert it into a cold numerical code, which can be added to a database and compared with other digital images, whenever needed.

Photos of regular protesters are being listed in a new category in the police records, *The Indian Express* reported, as suspected "rabble-rousers and miscreants". The police, reports in various newspapers said, used this information to filter potential dissenters from the crowd in Delhi's Ramlila Maidan where Prime Minister Narendra Modi was to give a speech last month and to scan footage where there was violence.

These events have parallels in the ongoing pro-democracy protests in Hong Kong, where a fear of facial recognition technology led demonstrators to wear masks. At marches and sit-ins in Delhi, too, face covers ranging from the laboratory kind to the Guy Fawkes mask have been spotted. Some activists have suggested painting faces.

New Delhi-based advocacy group The Internet Freedom Foundation (IFF) sent a notice to Delhi Police asking what exceptional circumstances had led it to use unlicensed drones without legal authority. Besides, targeted monitoring, especially in peaceful protests, is undemocratic, they deem. "This directly impairs the rights of ordinary Indians to assembly, speech and political participation," says Apar Gupta, lawyer and executive director, IFF.

The rate at which the technology is being applied and the relatively slow evolution of privacy laws has stoked a number of concerns among cyber security and privacy experts. In October 2019 the National Crime Records Bureau released a tender inviting bids to make an Automated Facial Recognition System (AFRS) which would lead to a centralised "national level searchable platform of facial images", probably among the largest in the world. The outline includes no mention of matters like consent and privacy. The tender, which calls for adding photographs from newspapers, raids and those sent by people, set off fears that China-style surveillance is imminent in India. According to New York-headquartered TechSci Research, cited by Bloomberg, the facial recognition market in India is poised to grow six times by 2024 to $4.3 billion, almost the same as China.

Facial recognition is the latest in a series of data being gathered for diverse reasons but which can ultimately aid in surveillance too. Aadhaar, which includes sensitive biometric details like iris scans and fingerprints together with demographic details of birth and residence, was made mandatory for filing tax returns. The idea of a DNA bank that stored citizens' profiles for criminal investigations was okayed in 2018, although questions about cross contamination persist. The Central Monitoring System (CMS) for lawful interception of telecommunications exists too. With 179,000 cameras for 18,600,000 people (9.62 cameras per 1,000 people), New Delhi is among the 20 most surveilled cities in the world, according to data by comparative analysis firm Comparitech. Chennai, with 4.67 cameras per 1,000 people, and Lucknow, with 2.59 cameras per 1,000 people, are among the 50 most surveilled cities. Comparitech also said it found the level of public CCTV coverage rarely affected rates of crime and safety.

The face is a critical aspect of personal data and efforts to document it have met with mixed reactions globally. China, covered by 170 million CCTVs currently, is set to triple that figure. Its police even use sunglasses equipped with facial recognition capabilities. In Israel, facial recognition company

AnyVision is under investigation by its investor Microsoft for surveilling Palestinians in the occupied West Bank. Last year, San Francisco became the first city in the United States to ban facial recognition by police and other agencies. A month ago, fundamental rights groups in the European Union warned member states that collecting facial images during demonstrations creates a “chilling effect” that might prevent people from exercising their freedom of assembly and expression.

The police have enthusiastically incorporated facial recognition in the last two years. Many acknowledge the police in India is understaffed and overworked, and that technology can help to deter pickpocketing or fine helmet-less drivers.

Chennai-based Vijay Gnanadesikan began tinkering with facial recognition systems after seeing a child begging at a signal. The co-founder of the FaceTagr app offers it free to NGOs and railway police for tracing trafficked or lost children, and also sells it to the police for investigating general crimes. His company built a database from newspapers and notices posted on Facebook and other social media, while his clients, which include the Chennai Police, rely on their own databases. “It is not that Big Brother is watching you, but Big Brother is watching *for you*,” he believes.

Facial recognition systems, however, are still evolving with no manifest figures for their success on the ground just yet. Thiruvallur Superintendent of Police P Aravindhan says the force’s initial attempts to use facial recognition in moving images failed because that needed high-quality, well-lit feed, so they now use the technology only for photo-based identification. The FaceTagr app, which is under 4MB and compatible with most phones, contributes to identifying repeat chain-snatchers, says Aravindhan.

While Gnanadesikan has secured the app by offering access only to government-verified users and letting ethical hackers have a go at it, there is at least one cautionary tale in the wider AI face recognition industry. The database for *CopsEye*, an app used by the Madurai Police, was found floating online by security researcher Oliver Hough and it contained all submitted photographs, regardless of whether they were a match, and even had OTP codes listed.

Private players, big and small, are working on facial recognition, claiming their software can find matches within seconds — even if the subject has switched hairstyles or grown a beard. The celebration of this technology has been short-lived. The women and child development ministry submitted a report last year stating that the facial recognition software used by the Delhi Police to identify missing children had a match rate of a mere one per cent. The software also mistook boys for girls.

Delhi Police is a client of New Delhi-based artificial intelligence company Innefu Labs, whose products promise to make policing “predictive” by training deep learning algorithms on “this side of hemisphere faces and texts”. This might involve teaching it to distinguish between types of local faces and languages. And to provide something called “narrative management”, as their website puts it — tracking public conversations to find “elements gone rogue” and “balancing the propaganda not in tune with the law of the land”.

Part of the fear related to facial recognition is linked with prejudices that programmers and users bring to it. Certain communities have traditionally been targeted by police forces. Their data is a part of such

systems and the algorithm is trained in such a way that they are far more likely to be identified than people from other communities. This ensures that the failures of the past will not just be the failures of the future, they will in fact be "made worse," feels IFF's Gupta.

For instance, in Hyderabad over the last few years, the police have been cordoning off areas in low-income neighbourhoods in what they maintain is an attempt to nab criminals. This military technique used to hunt insurgents gained traction when Ivanka Trump was to visit the city in November 2017 and has been almost normalised now. What started with documentation of fingerprints and biometrics has now seen the addition of facial recognition systems since 2018. As an increasing number of media reports suggest, people have been randomly asked by the Hyderabad Police to stand for a picture. K Prudhvi Raj, a corporate employee, was stopped on his way home after a nightshift at 2.30 am last November and told he was being photographed "simply like that".

Atul Rai, founder of Gurugram-based Staqu, which works with police in Uttar Pradesh, Rajasthan and Punjab, among others, observes that the technology is neither positive nor negative. "It is the person using it that makes it positive or negative. We don't want to have any government partners using our technology to harm people's privacy," he says. Police official Aravindhan says Chennai Police takes up a daily review of facial recognition operations to eliminate any misuse.

The future of facial recognition in law enforcement appears certain. The Smart City projects, which include CCTV installations for city surveillance, could drive it further. Mumbai Police has 13 licences for facial recognition software from an international vendor at present. These are deployed at its discretion over the existing network of some 5,200 CCTVs.

Pranaya Ashok, deputy commissioner of police (operations) for Mumbai Police, says they are expanding the database of digital photos of "history-sheeters" to increase the chances of spotting wanted criminals in surveillance. In the "technology cell" next to his office, now and then each month, unmissable alarms go off when a CCTV detects a blacklisted match. As yet reluctant to tie any arrests directly to facial recognition, Ashok holds that the feature is useful for locating frequent chain snatchers and for crowd control. Mumbai plans to add another 5,600 CCTVs, and with that the number of licences could hit 100.

Companies, including those from Japan and Israel, bid for the Mumbai Police tender. The bulk of the identification is done using the local police databases, while the rest is based on the centralised Crime and Criminal Tracking Network System. When the national AFRS database comes into being, these will be integrated with the Interoperable Criminal Justice System, and Immigration, Visa and Foreigners Registration & Tracking.

Law enforcers in Karnataka seem very keen to improve their ability to track faces, too. They hosted the India Police Hackathon 2019 last November in Bengaluru where facial recognition was among the topics in focus. Of the top 10 teams, three, including the winners from the city's Indian Institute of Science, presented solutions specifically for this technology. They coded for 36 hours, and the winning team showed how people can be identified from a live feed (not just static images) — and even after faces have aged 20 years. They say the police are in continuous touch to see if they can modify the existing algorithm with modules from the new prototypes.

It is often said that in the digital age, privacy is dead. People are increasingly immune to intrusions in privacy, offering up faces to phone and internet companies. Governments, Mumbai-based cyber lawyer N S Nappinai cautions, should be guarding citizens from excessive data mining by private players, rather than partaking in it. The right to be left alone, as upheld by the Puttaswamy judgement of 2017, is being diluted in the name of security, Nappinai adds. “Unless the government can prove the proportionality of the use of these technologies, they are not acceptable. It must say why its need for such action is greater than my right to privacy.”

Neither the government nor law enforcement authorities have put out a white paper to justify the use of facial surveillance on common citizens. “The rise of machine learning and deep learning algorithms is making it possible to easily implement these systems. It’s going to spread everywhere because that’s how it is designed to be. It becomes a standard way of doing things,” says Hyderabad-based independent security researcher Srinivas Kodali. These infrastructures need several years to improve and are best not pushed through fast in the absence of a clear legal framework, he says.

So far, in the case of protests, facial monitoring does not appear to have deterred dissenters. But one placard in the Mumbai protests did have the following request: “We would like to be seen, not watched.”