Caste counts

A vision for a just India, and not partisan political gains, should inspire a fresh census.

Socio-Economic Caste Census:

1. The clamour for a fresh caste census is getting louder in the country. No political party in the country has publicly opposed the demand as yet, and most have supported the call. Predictably, there will be more political mobilisation on the issue.
2. The Bharatiya Janata Party has the advantage of being in the saddle and could time an announcement best suited for itself. The last time India's population was enumerated on the basis of caste was in 1931 when it was under colonial rule.
3. There is a strong argument that the colonial census was about creating and reinforcing caste and religious categories in India rather than recording them in a benign manner.
4. Effective governance requires robust data on the governed. The creation of categories is itself a political act. Indian politics and the governance structure are all premised on categories that were firmed up during colonialism. But the salience of caste as the fundamental marker of identity for an Indian has only grown since Independence.

Knowing the status of the downtrodden:

1. As the democratisation of society deepens, questions are being raised regarding the status of Dalits, tribal communities and a large section of the population that is characterised in the Constitution as Socially and Educationally Backward Classes.
2. Political representation of these communities has increased and their participation in government jobs has risen. It is assumed that particular groups within each category have benefited disproportionately from political and job reservations, and there are demands for sub-quotas.
3. Many communities are demanding inclusion in one category or the other. Some communities are feeling short-changed by the affirmative action steps

of the state. With the role of the Government as a big employer diminishing, there is a demand for affirmative action in the private sector.

4. All these questions are being debated without adequate and reliable data, leading to conflicting and often misleading claims. Supporters of a caste census cite these reasons, while sceptics fear it will only widen social rifts.
5. They also point to the multitude of practical problems such an exercise will encounter. What is not debatable, however, is the fact that inequitable distribution of power and wealth endangers the stability of any society.
6. Partisan political gains should not be the motivation for a fresh census. A renewed vision for a just and united India, where all divides are reduced must guide the discussion on a caste census.

The ugly face of a crime-fighting move

The implementation of the National Automated Facial Recognition System in India lacks adequate safeguards.

Pegasus:

1. In the monsoon session of Parliament, no meaningful debate could take place due to the controversy over Pegasus, the spyware. Some Indian journalists, civil society activists and political leaders, and a top election strategist were possibly under surveillance.
2. There has been no categorical denial by the Government and that the Israeli software was not purchased. But above this, there is a much bigger issue of the privacy of the entire citizenry which has not received much public attention.
3. On June 23, 2021, the Joint Committee examining the Personal Data Protection Bill (2019) was granted a fifth extension by Parliament.
4. While informational privacy is not the Government's priority, it has been simultaneously exploring the potential of facial recognition technology.

A prying technology

1. To empower the Indian police with information technology, India approved the implementation of the National Automated Facial Recognition System

(NAFRS) to "facilitate investigation of crime and detection of criminals" in a quick and timely manner.

2. On its implementation, it will function as a national-level search platform that will use facial recognition technology: to facilitate the investigation of crime or for identifying a person of interest (e.g., a criminal) regardless of face mask, makeup, plastic surgery, beard or hair extension.
3. The technology is absolutely intrusive: computer algorithms map unique facial landmarks (biometric data) such as the shape of the cheekbones, contours of the lips, distance from forehead to chin, and convert these into a numerical code — termed a faceprint.
4. Thus, for the purposes of 'verification' or 'identification', the system compares the faceprint generated with a large existing database of faceprints (typically available to law enforcement agencies) through a database on driver's licence or police mugshots).
5. But the real problem is that facial recognition does not return a definitive result — it 'identifies' or 'verifies' only in probabilities (e.g., a 70% likelihood that the person shown on an image is the same person on a watch list). Though the accuracy of facial recognition has improved over the years due to modern machine-learning algorithms, the risk of error and bias still exists.
6. For instance, there is a possibility of producing 'false positives' — a situation where the algorithm finds an incorrect match, even when there is none — resulting in wrongful arrest.
7. Moreover, much research suggests facial recognition software is based on pre-trained models. Therefore, if certain types of faces (such as female, children, ethnic minorities) are under-represented in training datasets, then this bias will negatively impact its performance.

The National Automated Facial Recognition System (NAFRS)

1. As NAFRS will collect, process, and store sensitive private information: facial biometrics for long periods; if not permanently — it will impact the right to privacy.
2. Accordingly, it is crucial to examine whether its implementation is arbitrary and thus unconstitutional, i.e., is it 'legitimate', 'proportionate to its need' and

'least restrictive'? What is its potential for abuse and misuse with the pending status of the Personal Data Protection Bill (PDPB), and the absence of clear guidelines for its deployment? How does it impact other fundamental rights such as the right to dissent? Should NAFRS be banned or simply regulated?

3. The Federal Bureau of Investigation in the United States uses facial recognition technology for potential investigative leads; police forces in England use facial recognition to tackle serious violence.
4. In other cases, countries such as China use facial recognition for racial profiling and mass surveillance — to track Uighur Muslims.
5. Policing and law and order being State subjects, some Indian States have started the use of new technologies without fully appreciating the dangers involved.

Test of 'proportionality'

1. Facial recognition being an intrusive technology has an impact on the right to privacy. The Constitution of India does not explicitly mention the right to privacy.
2. However, a nine-judge Bench of the Supreme Court, in Justice K.S. Puttaswamy vs Union of India (2017) recognised it as a precious fundamental right. Since no fundamental right can be absolute and thus even in respect of privacy, the state may impose reasonable restrictions on the grounds of national integrity, security of the state, public order, etc.
3. The Supreme Court, in the K.S. Puttaswamy judgment provided a three-fold requirement (which was reiterated in Anuradha Bhasin while examining denial of the 'right to the Internet' to the people of Kashmir) to safeguard against any arbitrary state action.
4. Accordingly, any encroachment on the right to privacy requires the existence of 'law' (to satisfy legality of action); there must exist a 'need', in terms of a 'legitimate state interest'; and, the measure adopted must be 'proportionate' (there should be a rational nexus between the means adopted and the objective pursued) and it should be 'least intrusive.'

Unfortunately, NAFRS fails each one of these tests

1. First, NAFRS lacks 'legitimacy'. It does not stem from any statutory enactment (such as the DNA Technology (Use and Application) Regulation Bill 2018 proposed to identify offenders or executive order of the Central Government. Rather, it was merely approved by the Cabinet Committee on Economic Affairs in 2009 during United Progressive Alliance rule.
2. Second, and more importantly, even if we assume that there exists a need for NAFRS to tackle modern-day crimes, this measure is grossly disproportionate. This is because to satisfy the test of 'proportionality, benefits for the deployment of this technology have to be sufficiently great, and must outweigh the harm.
3. For NAFRS to achieve the objective of 'crime prevention' or 'identification' will require the system to track people on a mass scale — avoiding a CCTV in a public place is fiendishly difficult — resulting in everyone becoming a subject of surveillance: a disproportionate measure.
4. In the absence of a strong data protection law or clear guidelines on where this technology can be used or who can be put on a watch list? And, how long the system will retain sensitive personal data of those the surveilled people, NAFRS will indeed do more harm than good.

Impact on rights

1. With the element of error and bias, facial recognition can result in profiling of some overrepresented groups (such as Dalits and minorities) in the criminal justice system.
2. Further, as anonymity is key to the functioning of liberal democracy, unregulated use of facial recognition technology will dis-incentivise independent journalism or the right to assemble peaceably without arms, or any other form of civic society activism.
3. Due to its adverse impact on civil liberties, some countries have been cautious with the use of facial recognition technology. The Court of Appeal in the United Kingdom ruled the use of facial recognition technology by South Wales as unlawful in the absence of clear guidelines.

4. In the United States, the Facial Recognition and Biometric Technology Moratorium Act of 2020 was introduced in the Senate to prohibit biometric surveillance without statutory authorisation.
5. Similarly, privacy watchdogs in the European Union have called for a ban on facial recognition.

Unchecked pathway

1. At present, the Information Technology Act 2000, and the Rules framed thereunder offer broad powers to the Central government to infringe privacy in the name of the sovereignty, integrity or the security of the state.
2. The Personal Data Protection Bill 2019 is not much different. It gives the central government unchecked power for the purposes of surveillance — it can exempt any agency of the Government from the application of the proposed law in the name of legitimate state interest.
3. Without adequate safeguards such as penalties that are dissuasive and sufficiently deterrent, police personnel may routinely use facial recognition technology.
4. In sum, even if facial recognition technology is needed to tackle modern-day criminality in India, without accountability and oversight, facial recognition technology has strong potential for misuse and abuse.
5. In the interest of civil liberties and to save democracy from turning authoritarian, it is important to impose a moratorium on the use of facial recognition technology till we enact a strong and meaningful data protection law, in addition to statutory authorisation of NAFRS and guidelines for deployment.
6. If the Government has the will, it can get any law passed with godspeed just like the recently passed 20 Bills including the OBC Bill or three Farm Bills.