

Surveillance is not the only privacy issue

Who is responsible, when a protester is identified by a camera, doxxed by anonymous accounts, and then threatened at home? What happens to privacy when an electoral-roll decision determines whether someone can vote? Which safeguard applies when data gathered by the police is held by a private company?

Updated - September 30, 2026 02:08 pm IST

PANKHURI AGARWAL



Police officers move past Ikshana, a mobile surveillance van at Jantar Mantar during the Cockroach Janta Party (CJP) protests. File | Photo Credit: Reuters

In August 2026, the **Supreme Court disposed of a public interest litigation on doxxing and deepfakes**, asking the Union Ministries to take remedial measures. Earlier in July, A.A. Rahim, a Rajya Sabha member, petitioned the top court against the **Delhi Police's use of facial recognition and biometric surveillance** during **the Cockroach Janta Party (CJP) protests**. And in May, the SC upheld the Election

Commission's (EC) Special Intensive Revision (SIR) of electoral rolls, though critics had warned that it could exclude a large number of eligible voters.

While these may look like three unrelated stories, read together, they form a pattern connecting the state, private firms, online networks and the citizens caught among them.

Three kinds of watching

Facial recognition is the most visible; the State watches people in public and tries to establish who they are. Mr. Rahim's petition alleges that the police used facial recognition, AI-enabled smart glasses, drones and a mobile command vehicle at Jantar Mantar, and that the data was hosted by two private firms.

The CJP protests revealed a second layer. Women who took part were later targeted online: their personal details were published with reported rape and death threats. Public identification as punishment is not new; in March 2020, the Uttar Pradesh administration put up hoardings in Lucknow with the photographs and addresses of people protesting against the Citizenship Amendment Act. The Allahabad High Court ordered them removed, calling the display an "unwarranted interference in privacy". Today, a hoarding is not needed; a photo can be uploaded, identified, amplified and linked to an address within hours.

The SIR is a third kind of watching, wherein identity checks decide who stays on the electoral roll. The top court has held that the EC may examine citizenship for this limited purpose, though it cannot decide upon citizenship itself. But the scale is considerable: Bihar's SIR began with about 7.89 crore electors and ended with a final roll of 7.42 crore.

None of this falls evenly. For minorities, migrants, Dalits, Adivasis, women and the poor, surveillance decides whether they are counted, believed or safe.

India's privacy jurisprudence has a powerful foundation. In *K.S. Puttaswamy vs. Union of India* (2017), a nine-judge Bench held privacy to be a constitutionally protected right. However, *Puttaswamy* was decided in a case against the state, and its test is framed around state action. The Digital Personal Data Protection Act, 2023 lets the Union government exempt any state instrumentality from the Act by notification, on grounds which include the security of the state and public order. Consider Pegasus then, the

spyware made by an Israeli firm and allegedly used against journalists, activists and others. A court-appointed independent expert committee reported malware in some phones which it examined in 2022, but could not say for sure if it was Pegasus; it also noted that the Union government had not cooperated. Later in 2025, the SC indicated that parts of the report would not be made public.

The result is, therefore, a legal landscape in which the strongest constitutional protection may apply at one point in the chain, while the same person's information passes through other hands beyond it. Who is responsible, then, when a protester is identified by a camera, doxxed by anonymous accounts, and then threatened at home? What happens to privacy when an electoral-roll decision determines whether someone can vote? Which safeguard applies when data gathered by the police is held by a private company? India does not have clear answers to these questions.

None of this is new. The state's interest in identifying individuals predates Aadhaar by more than 150 years. In 1858, William Herschel, a British magistrate, began taking handprints on contracts. The technique was later developed into a fingerprint classification system in Bengal. The technology has changed, but the impulse to make a population identifiable has not. It shows up in Aadhaar, in Delhi's cameras, and in the SIR.

What is different today is the scale and speed. The state's cameras, the private companies that operate them, social media accounts that spread deepfakes and the bureaucratic exercises that decide who counts on the rolls are not separate stories that happen to unfold in the same summer. They are connected.

Therefore, the current moment calls for a different starting point: one that treats surveillance not as a discrete act by an identifiable actor against an identifiable person, but as a diffuse act spread across states, companies, and foreign vendors at once. Until India's privacy debate catches up to that reality, every right it wins will only ever be half a win, built to match the threats of the moment it is written in and already out of date by the time it is actually enforced.

Pankhuri Agarwal is Lecturer and Leverhulme Early Career Fellow at King's Business School, King's College London. Author of 'Fictions of Freedom: Migration, Modern Slavery and Bureaucracy in India' (2026)

Published – September 30, 2026 12:50 am IST