

4. Social Media Monitoring – Polity

States across India have witnessed a steady rise in the use of Social Media Monitoring Cells (SMMCs) by state police forces to counter misinformation, maintain law and order, and pre-empt digital threats

Key Findings and Trends

Rapid Expansion of Social Media Monitoring Cells (SMMCs) – The number of dedicated Social Media Monitoring Cells (SMMCs) increased from 262 (January 1, 2020) to 365 (January 1, 2024), reflecting a nearly 40% rise within four years. This expansion indicates a structural shift in policing, where online spaces are increasingly treated as extensions of the physical law-and-order domain. The growth aligns with the rise in digital crimes, misinformation, and online mobilisation, particularly during elections, protests, and communal flashpoints.

States Leading in Social Media Surveillance – As of 2024, the highest number of operational SMMCs are concentrated in

1. Bihar (52)
2. Maharashtra (50)
3. Punjab (48)
4. West Bengal (38)
5. Assam (37)

These states combine large populations, high social media penetration, and recurrent law-and-order sensitivities, necessitating continuous digital monitoring.

Expansion in Conflict-Prone and Sensitive Regions

Manipur – Increase from 3 SMMCs in 2020 to 16 in 2024. This expansion occurred despite nearly 140 days of internet suspension in 2023, indicating

1. A state perception that digital platforms remain critical drivers of conflict mobilisation, even under restricted connectivity.
2. Reliance on monitoring for early-warning intelligence during ethnic and communal tensions.

Assam – Expansion from 1 cell in 2022 to 37 in 2024. Reflects concerns related to cross-border misinformation, insurgency narratives, and identity-based mobilisation.

West Bengal – Growth from 2 cells in 2022 to 38 in 2024. Driven by political polarisation, electoral competition, and protest mobilisation, where social media plays a decisive role.

Punjab – Increase from 24 cells in 2022 to 48 in 2024. Linked to concerns over radical propaganda, organised crime networks, and diaspora-linked online narratives.

Institutionalisation of Digital Monitoring

From Informal Practice to Formal Structures – Prior to 2021, social media monitoring was

1. Conducted informally within cybercrime police stations, or
2. Embedded within Special Branch or Intelligence units without distinct identity.

Since 2021, DoPO (Data on Police Organisations) reports have recognised SMMCs as independent operational units, marking Bureaucratic legitimisation of digital surveillance. Integration of online monitoring into routine policing architecture.

Parallel Growth in Cybercrime Infrastructure

Cybercrime Police Stations – Increased from 376 (2020) to 624 (2024). Demonstrates

1. Escalation in financial frauds, phishing, identity theft, and online scams.
2. Growing need for specialised cyber expertise, separate from conventional policing.

Interpretation – The simultaneous expansion of SMMCs and cybercrime stations highlights the convergence of law-and-order policing and cyber policing, reflecting the hybrid nature of modern crimes.

Modernisation of Policing Tools

Use of Drones – Police-owned drones increased from 1,010 (2023) to 1,147 (2024). Drones are increasingly deployed for

1. Crowd surveillance and riot management.
2. Monitoring large religious or political gatherings.
3. Reconnaissance in insurgency-affected or difficult terrain areas.

Role of Bureau of Police Research and Development – BPR&D attributes the expansion of

1. SMMCs,
2. Cybercrime units, and
3. Surveillance technologies to enhanced funding under the Modernisation of State Police Forces (MPF) Scheme.

Modernisation of State Police Forces (MPF) Scheme

Overview

Launched by– Ministry of Home Affairs in 1969–70.

Recent focus– 2017–2025 period, with emphasis on technology-led policing.

Funding Pattern

1. **Union Territories**– 100% Central funding.
2. **North-Eastern and Himalayan States**– Centre (90%), State (10%).
3. **Other States**– Centre (60%), State (40%).

Key Components

1. **Modern Weapons and Equipment** – Firearms, protective gear, drones, CCTV, and surveillance software.
2. **Mobility Support** – Vehicles for law-and-order duties, emergency response, and border areas.
3. **Communication Systems** – Integration with CCTNS for real-time crime data sharing.
4. **Forensic and Cyber Capacity** – Strengthening forensic science laboratories and cyber forensic units.
5. **Infrastructure Development** – Police stations, offices, training centres, and housing.
6. **Special Focus Regions** – Left Wing Extremism (LWE) areas, North-East states, and Jammu & Kashmir.

Operational Framework of SMMCs

Organisational Placement – Typically function at

1. District level, or
2. Range / Commissionerate level,
under Cyber Cells or Special Branch supervision.

Core Functions

Monitoring online content that may

1. Disturb public order or communal harmony.
2. Trigger protests, riots, or panic situations.

Detecting

1. Cyberbullying, hate speech, and online fraud.
2. Coordinated misinformation or disinformation campaigns.

Producing – Trend reports, heat maps, and sentiment analyses for senior officers.

Liaising with – Social media intermediaries for content takedown, blocking, or user identification.

Positive Outcomes of SMMCs

1. Misinformation Control – Effective during crises such as COVID-19, floods, and cyclones.
2. Counter-Radicalisation – Tracking extremist propaganda, terror recruitment narratives, and encrypted outreach.
3. Prevention of Mob Violence – Early detection of fake videos or rumours that could spark lynching or riots.
4. Investigative Support – Assisting probes into cyber fraud, human trafficking, organised scams, and financial crimes.
5. Advanced State Models – States such as Maharashtra, Uttar Pradesh, Tamil Nadu, and Karnataka use AI-assisted analytics, enabling real-time anomaly detection and network mapping.

Concerns and Related Issues

Privacy and Oversight Deficit – SMMCs often operate

1. Without explicit statutory backing.
2. With limited judicial or legislative oversight.

Raises risks of

1. Mass surveillance.
2. Chilling effects on free speech.

Risk of Censorship and Misuse – Instances reported were

1. Individuals were summoned or booked for critical or dissenting posts.
2. Vague provisions of the IT Act or IPC were invoked.

This blurs the line between legitimate policing and political censorship.

Persistent Manpower Shortage – Despite technological upgrades India's police-to-population ratio remains below global norms. Shortage of trained personnel affects Effective use of advanced surveillance tools. Data analysis, follow-up, and accountability mechanisms.

Way Forward- Balancing Technology with Accountability

Clear Legal Framework – Enact comprehensive legislation governing digital policing and online surveillance.

Independent Oversight – Establish external oversight committees at state or national levels for SMMCs.

Transparency Mechanisms – Mandatory publication of transparency reports on

1. Content flagged.
2. Data accessed.
3. Takedown requests issued.

Rights-Based Policing – Align digital monitoring with principles of necessity, proportionality, and legality, as articulated in the privacy jurisprudence of the Supreme Court.

Capacity Building – Invest equally in human resources, legal literacy, and ethical training, alongside technological tools.

Source- <https://www.thehindu.com/news/national/police-social-media-monitoring-cells-rise-from-262-to-365-in-four-years/article70474620.ece>