CALL FOR PAPERS & ARTICLES 2025–26

Organised by LaWGiCo (Nivisam Lawgico Innovation Pvt. Ltd.)

Title:

Social Media Surveillance by Police: Between National Security and Privacy Rights

By:

Asmita Mallick

Institution:

Heritage Law College under the University of Calcutta

Abstract

The Internet has essentially changed international communications, commercial enterprise, infrastructure manipulate, and records garage with the aid of connecting a global community of computers, routers, and cables. This digital society, even as providing substantial opportunities in information and social relations, is likewise introducing new troubles, notably the boom in cyber-crime. Criminals are adapting popular activities together with fraud, robbery and blackmail to new mediums, leading to commonplace cyber-crimes consisting of online banking fraud, hacking and virus attacks, making the criminal factors of the virtual global or 'cyber law' increasingly important.

The emergence of social media as a major platform for conversation and public discussion has brought a brand-new task: police surveillance for countrywide safety and crime prevention. This practice creates tension among the government's security mandate and residents' non-public privateness rights and freedom of expression. This paper examines the structure of the Indian prison gadget to modify cybersecurity and social media surveillance, reading applicable laws and judicial reviews to advocate a balanced approach that addresses these competing pastimes and the felony and ethical dimensions concerned.

Keywords: Cyber Security, Digital Surveillance, Information Technology Act, Judicial Pronouncement, National Security and Schemes.

"If you spend more on coffee than on IP security, you will be hacked. What's more, you deserve to be hacked."

– Rechard Clarke.

Introduction

The speedy boom of social media (e.g., Facebook, WhatsApp) has essentially changed communique, information sharing, and political motion in India, making those systems integral to every day existence. Simultaneously, these systems have turn out to be resources of incorrect information, vulgar language, and threats to public safety, main police companies worldwide to adopt social media monitoring for crime prevention, intelligence collecting, and public order maintenance. This practice, but, sparks an essential debate, as indiscriminate surveillance dangers violating the fundamental proper to privateness (recognized under Article 21 of the Indian Constitution), chilling unfastened speech, and eroding democratic values, developing a serious venture to balance national security and civil liberties.

Definition of Cybercrime

Cybercrime is described as any crook activity concerning computer systems or networks, protecting profit-based crimes like ransomware and identity theft, direct attacks like hacking, and unlawful information garage. The upward thrust of the net and social media has extended its scope, allowing criminals to perform across borders effortlessly. The idea that every system is prone to hacking is supported with the aid of **Gödel's Incompleteness Theorem**[1], suggesting there may be no flawlessly steady barrier or fortress.

Issues associated with cybercrime are more often than not addressed via the Information Technology (IT) Act, 2000, which serves because the most important legislative degree on this field. Laws handling those troubles are regularly commonly called 'Cyber Laws' or 'IT Laws'. In addition to the IT Act, different statutory provisions, substantially the Copyright Act, 1957, and the Patents Act[2], 1970, have been amended to cope with problems regarding Intellectual

[1] Gödel, K. (2011) *Gödel's incompleteness theorems*, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/G%C3%B6del%27s_incompleteness_theorems (Accessed: 15 November 2025).

[2] The patent act, mainly ruled by the 1970 Patent Act in India, is for the inventions of security measures which are novels, non-tests, and industrial applications. This allows inventors to secure exclusive rights for using, manufacturing, sales and licensing their innovations for 20 years from the date of filing. It encourages technological development by rewarding inventors and giving them a temporary monopoly on their invention.

Property Rights (IPRs)[3], a broader class that includes protection for creations of the mind. Courts globally, but, have furnished inconsistent solutions when managing those complex and often interconnected problems.

Nature & Scope

The nature of cybercrime develops diverse and continuously, which includes activities such as data violations, financial frauds, cyber terrorisms and the spread of misinformation. The scope of cyber-crime is global, which affects individuals, corporations and governments equally. Social media platforms, with their vast user bases and rich data, have become the major goals and tools for cyber criminals. Actor ranks from Lone Hackers and Cyber Criminal gangs to state-interested institutions. The interaction of social media facilitates rapid dissemination of malicious material and coordination of illegal activities, which is an important focus area for law enforcement.

Common type of cybercrime

1. **Hacking and unauthorized access:** Hackers are obtaining illegal access to computer systems or networks to destroy data theft, change or data.
2. **Fishing and online fraud[4]:** Criminals are misleading practices to get sensitive information or money, often through fake websites or emails.
3. **Identity theft**: Stealing personal information to replicate individuals for financial or other benefits.
4. **Ransomware attacks[5]:** By this method the criminals are infected systems with malicious software that locks the data until the ransom pays.
5. **Cyberstalking and harassment:** The hackers are using digital platforms to threaten, harass or intimidate individuals.
6. **Distribution of illegal materials:** Sharing or selling prohibited materials such as child pornography or pirated software through digital means.

---

[3] Intellectual Property Rights (IPR) is a broad term that incorporates various legal protection for the compositions of the mind. In addition to copyright and patent, it includes trademarks, industrial designs, geographical signals and business secrets. The objective of IPR laws is to encourage innovation and creativity by ensuring creators, inventors and businesses, while promoting fair competition in the market and can get financial benefits from their work.

[4] Agrim Tandon, 'Is Social Media Driving the Rise of Cyber Crime? Exploring the Intersection between Social Media Use and Cybercrime Victimization' (2022) 2(3) *Journal of Cyber Law and Policy*

[5] Deloitte, 'Phishing and Ransomware: How to Prevent Threats' (Deloitte Luxembourg) https://www.deloitte.com/lu/en/services/risk-advisory/research/phishing-ransomware-how-to-prevent-threats.html accessed 14 November 2025.

7. **Digital arrest**[6]: Digital arrest is a scam strategy where fraudsters motivate law enforcement or government officials to intimidate the victims to hand over money or sensitive information. This is psychological manipulation, not real arrests.
8. **Toxic panda**[7]**:** Toxic panda is a new Android banking trojan- a type of malware that infects the phone to steal money from bank accounts.

Historical Background of Social Media and Cybercrime

The ancient progression of cyber threats, paralleling technological advances since the time of Alan Turing, demonstrates increasing complexity and get admission to. Cybercrime advanced from the misuse of telegraph and phone structures within the 19th and 20th centuries, into electronic mail-based scams, viruses, and malware inside the 1980s and 90s (the Internet technology). The social media growth within the 2000s made those structures attractive goals for facts robbery and scams, whilst the relationship of everyday devices thru the Internet of Things (IOT)[8] has similarly multiplied vulnerabilities and possibilities for cybercriminals.

Legal Framework Governing Social Media Surveillance in India

1. **Constitutional Provisions**
    - **Right to Privacy:** The Right to Privacy is a fundamental constitutional guarantee, installed thru the vital implications of Article 21 of the Constitution of India, which ensures the proper to existence and private liberty. This is proper to complete, extending safety to individuals towards issues like informative privacy and unwarranted country tracking.

      The constitutional basis for privateness become initially explored within the *Gobind v. State of Madhya Pradesh (1975)*[9] case, in which the Court examined the validity of police surveillance policies in opposition to ordinary offenders. While the Court did no longer invalidate the policies, it first diagnosed the

[6] Mallick, A. and Ganguli, P. (2024b) 'Understanding toxic panda: The new Cyber threat targeting data security', *Social Science Research Network* [Preprint]. doi:10.2139/ssrn.5018562.

[7] Mallick, A. and Ganguli, P. (2024) 'Understanding toxic panda: The new Cyber threat targeting data security', *Social Science Research Network* [Preprint]. doi:10.2139/ssrn.5018562.

[8] Faddom (2025) Cybercrime: History, Global Impact & Protective measures [2025], BlueVoyant. Available at: https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022 (Accessed: 15 November 2025).

[9] AIR 1975 SCC 468

lifestyles of a proper to privacy underneath Article 21, albeit as a constrained right. The ruling introduced the principle of **"hypnotic state interest"**, emphasizing that any violation of privacy must be legally mandated and strictly proportional to the state's goal.

- **Reasonable Restrictions:** Article 19(2) balances essential rights and kingdom wish by allowing affordable regulations on loose speech to protect pastimes like countrywide safety or public order. For surveillance, this clause is the prison mechanism for weighing person privateness towards national security needs.

  The precept of balancing privateness and press freedom changed into similarly refined inside the *State of Tamil Nadu (1994)*[10]*, or the Auto Shankar case*. When a mag posted a death-row convict's autobiography, the Court showed that the freedom of expression below Article 19 consists of the proper to submit lifestyles histories, mainly whilst based on public information. Most considerably, this selection clarified that public officials cannot declare the proper to privateness concerning their responsibilities finished in an official capacity, thereby strengthening press freedom against pre-censorship and authentic claims of privateness.

2. Statutory Provisions

- **Information Technology Act, 2000 (IT Act)**[11]**:** Section 69 gives the government the right to prevent, monitor or decry to prevent electronic information in the interest of national security, sovereignty, or public order. The rules of the year 2021 increase the concerns of privacy to help social media middlemen explore the origin of messages.
- **Digital Personal Data Protection Act, 2023:** This Act empowers officials to prevent, monitor and decrypt digital information for national security and law enforcement purposes.
- **Indian Telegraph Act, 1885:** Section 5 (2) and related rules of this act allow telecommunications to be intercepted under specific circumstances.
- **Unlawful activities (prevention) Act, 1967 (UAPA):** This act allows monitoring and custody to prevent threats to terrorism and sovereignty.

---

[10] (1994)6 SC 632

[11] The Information Technology Act is explained the meaning of information. It is a very vast expression of Information including this Act like data related any technology, message through any electronic mode, massage including text, any types of images; sound which is liable to expression, electronic voice, machine codes, various computer programmes included all operative system, etc.

3. Absence of Dedicated Data Protection Law

India currently lacks a comprehensive data protection law, although the purpose of individual Data Protection Bill (pending) is to regulate data privacy and government access. Globally, many countries have enacted laws to regulate digital monitoring, such as the USA Patriot Act in the US and General Data Protection Regulation in the European Union (GDPR). The purpose of these laws is to balance safety needs with personal privacy rights, but often faces criticism for transparency or lack of transparency. In recent cases of developments, the legal outlines continue to develop, to address and address objectionable materials with new rules for digital middlemen and guidelines for social media platforms.

Jurisdiction and cyberspace

Traditionally where the cause of action arises is where the jurisdiction Lines. There are multiple parties involved in various parts of the world in cyberspace. In any transaction three parties takes place-

i) User;
ii) Service provider;
iii) Person or business

Therefore, ideally the most efficient Law must address whether a particular event in cyber space in controlled by the Laws of the state on country or where the user is located on application of all the other countries on state Laws.

Jurisdictional issues in India

Cyberspace jurisdiction is exceedingly complicated due to the fact the absence of virtual borders reasons overlapping claims and makes it difficult to find cyber incidents. Resolving these conflicts is based on international cooperation thru treaties for statistics sharing and the principle of comity respecting other international locations' legal guidelines, even though attaining global consensus remains a continuous task requiring diplomacy.

Judicial Pronouncements on Surveillance and Privacy

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[12]

[12] AIR 2017 SC 4161

The Supreme Court of India unanimously declared the right to privateness an essential proper beneath Article 21 of the Constitution, overturning in advance rulings. This right covers non-public autonomy and manipulates over information. Any infringement has to meet strict standards of legality, necessity, and proportionality, forming a key foundation for India's digital rights and data protection laws.

2. Dr Chakradhar Paswan v State of Bihar [13]

The matter dealt with the validity of reservation in public employment. The Supreme Court said that 100% reservation for Scheduled Castes in the same post violates Article 16 (1) of the Constitution. This emphasized that reservation should be appropriate and cannot remove the principle of equal opportunity.

3. Anvar P.V. v P.K. Basheer[14]

A historical decision on electronic evidence. The Supreme Court ruled that Section 65B of the Indian Evidence Act should be strictly complied with for the acceptance of electronic records. It rejected the earlier situation in the *state of Bihar vs Navjot Sandhu* and clarified that the secondary electronic evidence without proper certification is unfair.

4. Manohar Lal Sharma v. Union of India (2021)[15]

In the Pegasus adware case, the Supreme Court dominated that countrywide safety can't be a blanket excuse to keep away from judicial review when fundamental rights (Article 21) are at chance. Due to the government's loss of a detailed affidavit, the Court appointed an impartial professional committee (headed by Justice R.V. Raveendran) to analyze the claims, maintaining that country surveillance must be valid, essential, and proportional.

5. *People's Union for Civil Liberties (PUCL) v. Union of India (1996)*[16]

In this landmark case, the Supreme Court examined the legality of telephone tapping under Section 5(2) of the Telegraph Act, 1885, amid concerns over unauthorized surveillance of political figures. The Court upheld that the right to privacy is part of Article 21, and phone tapping is a serious intrusion. While not invalidating Section 5(2), it mandated strict

[13] (1988) 2 SCC 214 (SC)
[14] (2014) 10 SCC 473 (SC)
[15] Writ Petition (Crl.) No. 314 Of 2021
[16] AIR 1997 SC 568

safeguards: approval only by the Home Secretary, time limits, regular review, and mandatory record destruction.

6. Gujarat Steel Tubes Ltd v Gujarat Steel Tubes Mazdoor Sabha[17]

This case addressed industrial relations and unfair labour practices. The Court held that termination of workers without proper inquiry violates principles of natural justice and the Industrial Disputes Act.

7. Union of India v East Coast Boat Builders & Engineers Ltd[18]

This case revolves around contractual obligations and government liability. The court investigated whether the Union of India was bound by the terms of a contract and clarified the scope of sovereign immunity in commercial behaviour.

8. Kharak Singh v. State of Uttar Pradesh (1962)[19]

In the *Kharak Singh vs. State* case, the Supreme Court investigated police surveillance on unconvicted persons. The majority struck down night-time domiciliary visits as violating Article 21 (personal liberty) due to a lack of legal support, but upheld other monitoring forms since privacy was not yet a recognized fundamental right. The dissenting opinion, however, strongly argued that privacy is an essential part of personal liberty.

9. Hussainara Khatoon v State of Bihar[20]

The pilot exposed the plight of undertrial prisoners in Bihar. The Supreme Court said that the right to a quick testing is a fundamental right under Article 21. It also emphasized the need for free legal aid for the indigestion accused.

10. Navtej Singh Johar v Union of India[21]

A historical decision that reduced the consent gay work by reading Section 377 IPC. The court retained the right to constitutional morality, dignity and privacy under Article 21, marking a major victory for LGBTQ+ rights in India.

---

[17] (1980) 2 SCC 593 (SC)
[18] (1998) 1 SCC 278 (SC)
[19] AIR 1963 SC 1295
[20] (1979) 3 SCR 532 (SC)
[21] (2018) 10 SCC 1 (SC)

11. Transformative Constitutionalism

Not a case per se, but a **jurisprudential doctrine**. It refers to the idea that the Constitution is a **dynamic instrument** aimed at achieving **social justice and equality**. It was notably invoked in *Navtej Singh Johar*, *Joseph Shine*, and *KS Puttaswamy* to interpret rights progressively.

These cases underscore the ongoing judicial efforts to delineate the boundaries of lawful surveillance and protect individual rights in the digital age.

Social Media Surveillance Practices by Police

In the digital age, balanced national security and privacy has become a controversial and complex issue. Governments around the world, including India, have relied on monitoring as a tool to maintain national security and public system. However, this dependence has raised concerns about potential violations on civil freedom, especially the right to privacy.

Police agencies use social media surveillance to:

- **Monitoring Equipment:** Police use special software to monitor public sentiment through large versions of social media data, track individuals or groups, analyze trends and detect potential hazards.
  Police have made Babel Street, Cobwbs, Cogito, Dataminer, DigitalStakeout, Edge NPD (ABTSEL), Geophydia, Giant Oak (Gost), Kapo Software, Care, Care, Lukles Cyber Solutions, Media Sonar, Nis (NISTRECENCENS SALISISIGE)[22].

- **Undercover operations:** Officers create fake accounts to infiltrate groups, inspect interaction and gather intelligence on employed protests, criminal activity or potential threats.
  In 2010, a DEA agent created a fake Facebook profile using a woman's identity and personal photos without her consent. Similarly, DHS used fake college profiles to trap immigrants, leading to over 170 arrests, and Memphis Police created false accounts to surveil Black Lives Matter activists.

[22] *Social Media Monitoring* (no date) *Street Level Surveillance*. Available at: https://sls.eff.org/technologies/social-media-monitoring (Accessed: 15 November 2025).

- **Surveillance methods:** Surveillance methods include public posts, private messages, metadata, facial recognition, and geolocation. For instance, the U.S. Postal Inspection Service's ICOP program monitored social media using keywords like "protest" and "attacks", but was later found to lack legal authority as it was unrelated to postal services.

- **Data Collection:** Police social media tracking entails accumulating public posts, metadata, and authorized personal communications, frequently included with gear like facial popularity, to perceive suspects and accumulate proof. Globally, regulation enforcement actively uses this device to fight antisocial behaviour, as exemplified by means of the police in the UK using software to predict crime (e.g., at some point of the London Olympics) and the NYPD[23] mining social media for intelligence on capability ailment.

- **Stop terrorism and cybercrime:** Police saw Hate speech, any kind of wrong information, and to instigate violence in social media. By this, they are also capable of preventing cybercrime terrorism.

  The social media lab of Mumbai Police monitors trending subjects to prevent and prevent mass meetings or unrest. Globally, the police have used social media to track gang activity, prevent violence and gather evidence for prosecutors.

Recently, a blog post on the official FBI blog urged the local police to monitor social media for criminal activity. The author, who is a retired head with Assistant Chief Agent at Montgomery, Alabama Police Department and now Alabama Criminal Justice Information Centre, has asked local law enforcement officers to use the Internet, which is a forecast tool for everything from the fugitives, to singing the Associate suspects, to the strut gangs, and the strategic activities for the strut gangs, and the criminal activity.

Balancing National Security and Privacy Rights

The duty of the state to protect citizens from terrorism, cyber threats and crime justifies some monitoring measures. However, it should be balanced against personal rights.

[23] 'Embrace Social Media Monitoring for Better Law & Enforcement' (no date a) *https://www.veetechnologies.com/blog/media-tracking-and-analysis/embrace-social-media-monitoring-for-better-law-enforcement.htm*. Available at: https://www.veetechnologies.com/blog/media-tracking-and-analysis/embrace-social-media-monitoring-for-better-law-enforcement.htm (Accessed: 15 November 2025).

i) **Need and Promotiveness:** Monitoring must be limited to large -scale data collections, what is necessary to achieve valid safety objectives and should be limited to specific goals. It should be in proportion to danger.

ii) **Transparency and accountability:** Governments should disclose monitoring policies and provide treatment for violations. It should equip law enforcement with up-to-date training on digital morality, privacy and cybercrime trends.

iii) **Judicial Inspection:** Independent courts should review and authorize monitoring to prevent misuse. Independent inspection mechanisms and transparency reports can help ensure valid and moral monitoring.

iv) **Validity:** Monitoring must be authorized by clear and accessible laws. Comprehensive data protection laws should be applied with clear boundaries on government access.

v) **Data by design minimalization and privacy:** Monitoring technologies should include privacy security measures from installation. To detect and prevent cybercrime, it should develop technologies and equipment enhancing privacy.

vi) **Public Trust:** Foster dialogue between policy makers, law enforcement, civil society and technical industry to ensure balanced policies. To create public confidence, it is required to showcase that monitoring meets legitimate security objectives and respects personal rights.

vii) **International Cooperation:** Creating a harmony of legal standards and sharing the best practices can help in cope with cross-border challenges.

Privacy Concerns and Risks

- **Violation of privacy:** Monitoring often involves large scale data collection without personal doubts; there is a risk of violation of privacy rights.
- **Privacy & Rights:** Large-scale statistics series threatens privateness, expression, and affiliation.
- **Data Misuse:** Personal information can be exploited or shared without consent.
- **Lack of Oversight:** Secretive systems permit abuse and political focused on.
- **Security Risks:** Collected data is prone to leaks and hacking.
- **Legal & Technical Gaps:** Outdated laws, AI complexity, and pass-border facts flow restrict duty.
- **Effectiveness:** Mass surveillance regularly curtails freedoms without enhancing protection.

Measures to Prevent Cybercrime

- **Stronger laws and oversight:** enact clear legal guidelines protecting statistics and impartial monitoring bodies.
- **Public awareness:** Educate users about privacy settings, safe online behaviour and identifying cyber threats.
- **Technical solutions:** Use encryption, multi-factor authentication and regular security audit to protect data.
- **International Cooperation:** Share intelligence and quality practices amongst law enforcement agencies worldwide.
- **Responsible tracking:** Apply strict recommendations, inspections and duty for police use of social media surveillance device.
- **Government schemes on cyber security:** Some schemes regarding cyber security in Indian government are *Cyber Surakshit Bharat*, *CERT-In, National Critical Information Infrastructure Protection Centre, Crisis Management Plan, Website Audit, Training & Mock Drills, Malware Protection.* Some important tool use for preventing cyber-attack is Kali Linux, Ophcrack, EnCase, SafeBack, Data Dumber.

Conclusion

Police monitoring of social media operates on the important intersection of national safety and privateness rights, imparting tools for crime prevention whilst elevating serious criminal and moral questions. Given the Supreme Court's popularity of privateness as a fundamental proper, tracking practices ought to be strictly regulated, obvious, and subject to judicial evaluate. Achieving the correct stability requires a sturdy criminal shape, obvious approaches, technological safeguards, and non-stop public engagement to defend both collective safety and character freedom inside the virtual age.

Furthermore, security features on my own are insufficient, because the cyber international requires consistent development. The smooth functioning and protection of cyberspace depend not just on generation and technical specialists, however also basically on felony sanctions. Therefore, cyber law is vital to offer the vital tips and regulations that aid technological security and allow effective, yet privateness-respecting, law enforcement.

References

1. Ahuja, K. (2024) *Balancing National Security and privacy: Analysing the legal framework for surveillance in India*, *Bhatt & Joshi Associates*. Available at: https://bhattandjoshiassociates.com/balancing-national-security-and-privacy-analyzing-the-legal-framework-for-surveillance-in-india/ (Accessed: 15 July 2025).
2. Shivani Gupta, 'The Real Struggle for Privacy and National Security in Terms of Liberty and Surveillance: A Study' (2021) 2(3) *Indique Law Journal* 1.

3. Publisher (2024) *Right to privacy vs. national security: Navigating the legal and political boundaries " Lawful legal, Lawful Legal*. Available at: https://lawfullegal.in/right-to-privacy-vs-national-security-navigating-the-legal-and-political-boundaries/ (Accessed: 15 July 2025).
4. Cyber Laws written by Justice Yatindra Singh: Universal LexisNexis, 6th edition