INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE INTERSECTION OF LAW, TECHNOLOGY, AND POLICING: LEGAL CHALLENGES IN USING SOCIAL MEDIA FOR CRIMINAL JUSTICE

AUTHORED BY - MANINDERJIT SINGH & DR. CHEENA ABROL
School of Law
CT University, Ludhiana

ABSTRACT

The research analyzes how Indian police operations use social media platforms as their main operational base while documenting the technological methods that create different legal problems which affect police work and their ability to gather evidence and protect citizens' rights. The study examines how the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) establishes a new procedural framework through its legal acceptance of "electronic communication" and "audio-video electronic means" which requires police to document their search procedures through video evidence for all investigations under Section 105. The study evaluates Bharatiya Sakshya Adhiniyam, 2023 (BSA) evidence requirements by examining how the law defines electronic records admissions and how Section 63(4) establishes proof standards for social media content access based on certificate requirements. The research examines law enforcement access to digital platforms through the IT Act of 2000 which includes Sections 69 and 69A and the Intermediary Rules of 2021 and the Digital Personal Data Protection Act of 2023 which includes Section 17 while analyzing how Articles 14 and 19 and 21 restrict constitutional rights. The research proposes rights-respecting safeguards and accountability measures for lawful, proportionate social media policing.

Keywords: Social media policing; BNSS 2023; BSA 2023; Electronic evidence; DPDP Act 2023; Intermediary regulation

1 INTRODUCTION

Social media platforms now function as continuous spaces of communication, identity, commerce, and political participation, but they also operate as high-volume data repositories which contain trace evidence that law enforcement uses to prevent and detect crimes and

ISSN: 2582-6433

prosecute offenders. The Indian legal system creates a unique combination of law and technology and police enforcement because social media content can exist as both protected speech and processable data whose recordable and shareable components function as potential electronic records which serve as evidence. The legal system needs to establish methods for collecting and storing and examining posts and messages and metadata and live streams and platform-generated logs which should maintain constitutional freedoms instead of allowing them to become mere tools for investigation. [1]

The new criminal law framework strengthens technology-facing procedure and proof. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) formally recognizes "audio-video electronic means" and "electronic communication" (Section 2(1)(a) and Section 2(1)(i)) and normalises digital service and workflow within criminal procedure, including service of summons through electronic communication (Sections 64 and 71), recording of search and seizure through audio-video electronic means (Section 105), and the centrality of the first information report recorded under BNSS procedure (Section 173), with disclosure duties in police-report cases (Section 230). Social media-derived leads become operationally easier to convert into procedural steps through these provisions, which create new legal and proportionality and digital policing auditability challenges.[2]

The Bharatiya Sakshya Adhiniyam 2023 BSA establishes direct regulations for electronic records through its Section 63 which describes how electronic records must meet specific conditions to become admissible in court and its Section 634 requirement which mandates electronic record certification during evidence presentation. The Digital Personal Data Protection Act 2023 establishes personal data processing rules that include law enforcement and public order exemptions which exist in Section 17. The established legal framework enables social media content monitoring by law enforcement authorities however actual enforcement requires complete adherence to established procedures and validation of evidence and controlled information access which makes it difficult to proceed with investigations because it leads to evidence loss and violation of rights and unauthorized monitoring.[3]

[1] Yong Shan, *Digital platforms and the transformation of crime governance*, 13 The Journal of Chinese Sociology 1- (2026)

[2] Sharnam Agarwal & Yashika Chouksey, *From Lalita Kumari To Section 173(3) BNSS: Navigating The New Frontier Of FIR Registration*, Live Law, Mar. 9, 2026, *available at*: https://www.livelaw.in/lawschool/articles/lalita-kumari-section1733-bnss-fir-registration-525575 (last visited May 2, 2026)

[3] Abhiraj Jayant, *How To Fulfill Requirements Of Admissibility Of Electronic Evidence Under Bhartiya Sakshay Adhiniyam,...*, Live Law, June 26, 2024, *available at*: https://www.livelaw.in/articles/electronic-evidence-admissibility-section-63-bhartiya-saksha-adhiniyam-2023-261511 (last visited May 2, 2026)

ISSN: 2582-6433

1.1 Meaning and Scope of Social Media in the Contemporary Digital Environment

The legal technical definition of social media describes it as a system which uses intermediaries to enable users to produce content which gets stored and organized and distributed through automated systems while the system maintains permanent articles that include both content and its associated metadata. The BSA 2023 becomes essential for court proceedings because it establishes the rules which determine which electronic records can be presented as evidence through its Section 63 provisions that include the certification process described in Section 63(4) and its assumptions about electronic contracts and protected digital records and signatures that apply to Sections 85 to 87 which define how parties may present and assess screenshots and downloads and chat exports and platform logs.[4]

1.2 Growth of Technology-Driven Policing in India

Police departments have started using technology more since digital workflows became standard for conducting criminal investigations. The definition of "audio-video electronic means" (Section 2(1)(a)) and "electronic communication" (Section 2(1)(i)) which BNSS 2023 provides shows that investigators and courts can use digital communication and video-conferencing and electronic transmission as normal procedures during their work. The social media policing process begins with leads which start from online posts and direct messages and live videos and user complaints which people submit through digital channels.[5]

The BNSS establishes digital accountability systems which monitor social media activities for operational purposes because it requires footage of search and seizure activities to be documented through audio and video recording technology (Section 105) and it allows summons delivery through electronic methods (Sections 64 and 71). The provisions improve operational efficiency but they create legal problems because they question the legal authority for police actions which begin from social media platforms and the authenticity of digital evidence and the verification process of electronic delivery. [6]

[4] Abhiraj Jayant, *How To Fulfill Requirements Of Admissibility Of Electronic Evidence Under Bhartiya Sakshay Adhiniyam,...*, Live Law, June 26, 2024, *available at*: https://www.livelaw.in/articles/electronic-evidence-admissibility-section-63-bhartiya-saksha-adhiniyam-2023-261511 (last visited May 2, 2026)

[5] Bharatiya Nagarik Suraksha Sanhita : Paradigm Shift from Procedural Code to Nagarik Suraksha, *available at*: https://www.lexisnexis.com/blogs/in-legal/b/law/posts/bharatiya-nagarik-suraksha-sanhita-paradigm-shift-from-procedural-code-to-nagarik-suraksha (last visited May 2, 2026)

[6] Justice Narayana Pisharadi, *Recording Of Search And Seizure Through Audio-Video Electronic Means Under Section 105 Of The BNSS*, Live Law, Jan. 19, 2025, *available at*: https://www.livelaw.in/articles/recording-of-search-and-seizure-electronic-mode-section-105-bnss-281366 (last visited May 2, 2026)

ISSN: 2582-6433

1.3 Relevance of Social Media in Criminal Justice Administration

Social media has become relevant across the criminal justice chain—complaints, intelligence, investigation, witness location, intimidation detection, and evidentiary reconstruction—because it captures contemporaneous communications and behavioural footprints. The BNSS, 2023 framework establishes early criminal proceedings through its first information report system (Section 173) and police-report case disclosal requirements (Section 230) which require social media content to be officially recorded through BNSS-compliant processes instead of being treated as informal online leads. This process guarantees that all information collected from platforms leads to established official procedures.[7]

The IT Act 2000 and the IT Rules 2021 define platform response procedures for legitimate legal requests and takedown/blocking orders and due-diligence requirements at the regulatory and access layer. The DPDP Act 2023 establishes rules for personal-data processing which include investigation and public order exemptions defined in Section 17 of the law. The social media "criminal justice value" depends on two factors because it requires both public information and permitted government access to restricted information which includes logs and identifiers and retention and disclosures to be examined in court according to BSA Section 63 standards. [8]

1.4 Objectives of the Study

1. To analyse how BNSS 2023 enables digital-era policing practices which include social media monitoring and assessment of related legal risks.
2. To assess BSA 2023 social media content admissibility standards as electronic evidence while focusing on Section 63 certification and its related presumptions.
3. To examine police practices for accessing and monitoring and removing content on social media platforms according to the IT Act 2000 and IT Rules 2021.
4. To examine how social media policing under the DPDP Act 2023 affects data protection rights through investigative processing under Section 17.

[7] Sharnam Agarwal & Yashika Chouksey, *From Lalita Kumari To Section 173(3) BNSS: Navigating The New Frontier Of FIR Registration*, Live Law, Mar. 9, 2026, *available at*: https://www.livelaw.in/lawschool/articles/lalita-kumari-section1733-bnss-fir-registration-525575 (last visited May 2, 2026)

[8] What about the Intermediary? Demystifying the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 SCC Times, *available at*: https://www.scconline.com/blog/post/2021/07/12/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-3/ (last visited May 2, 2026)

ISSN: 2582-6433

5. To recommend legal and procedural protections which respect rights for social media usage throughout investigation and prosecution and trial processes.

1.5 Research Questions

1. Which specific procedural powers and duties established by BNSS 2023 most effectively govern police activities that start through or rely on social media content?
2. What primary evidentiary challenges must be overcome to establish the authenticity, integrity, and admissibility of social media content according to BSA 2023 Section 63 requirements?
3. How do intermediary obligations under the IT Act, 2000 and IT Rules, 2021 (updated) affect law-enforcement access and accountability?
4. How does DPDP Act, 2023 (including Section 17) reshape the legality of collection, use, and retention of personal data in social-media policing?
5. What reforms are required, to prevent overreach while retaining legitimate criminal justice objectives in the face of social media?

1.6 Research Methodology

The study performs its research through doctrinal methodology which requires researchers to read statutory texts and rules and official legal documents that govern criminal procedure and evidence and platform regulation and personal data. The primary materials are BNSS, 2023 (which contains Sections 2(1)(a), 2(1)(i), 64, 71, 105, 173, and 230), BSA, 2023 (which contains Section 63 and Sections 85–87), the IT Act, 2000 (which includes Sections 69, 69A, and 79), the IT Rules, 2021 (which received its latest update), and the DPDP Act, 2023 (which contains Section 17). The analysis follows chapter themes which include policing powers and evidentiary reliability and rights and accountability and reforms as its main structure.

1.7 Review of literature

Subhajit Basu (2010)[9] article examines Indian privacy policy through social, cultural, and regulatory perspectives and argues that privacy protection in India cannot simply replicate European-style umbrella legislation. The document serves analytical purposes which enable researchers to study Indian digital governance as well as informational privacy and technology-sensitive policymaking.

[9] Subhajit Basu, "Policy-Making, Technology and Privacy in India", 6 *Indian Journal of Law and Technology* 65 (2010). *Available at*: https://repository.nls.ac.in/ijlt/vol6/iss1/3/

ISSN: 2582-6433

Apar Gupta (2010)[10] article investigates how online privacy changed after the Information Technology (Amendment) Act, 2008 while studying surveillance systems and identification methods which operate through internet communications. The research demonstrates that legal protections exist in criminal law through their documented wording yet they present actual operational limitations.

Latha R. Nair (2008)[11] article examines India's initial data protection initiatives and demonstrates how disconnected legal solutions have created a vulnerability to privacy violations and personal data theft. The research enables researchers to trace pre-DPDP legal gaps and examine the structural shortcomings which affect India's developing data protection framework.

Jaideep Reddy (2014)[12] article examines the Central Monitoring System through its privacy implications while it assesses the Illegal surveillance systems of India which lack transparency and accountability. The study enables researchers to assess state surveillance abilities while they investigate legal protections and constitutional restrictions on digital surveillance activities.

Bedavyasa Mohanty (2016)[13] article assesses whether India's surveillance system operates within constitutional boundaries while examining its legal framework and monitoring methods and ways to protect classified information. The study establishes a link between social media monitoring activities and surveillance systems which protect privacy rights and individual freedoms and uphold constitutional responsibility.

Giancarlo F. Frosio (2017)[14] article presents worldwide intermediary liability systems while showing how regulatory and theoretical developments affect platform responsibilities. The study shows how social media intermediaries manage state requests and track user activities and handle their legal responsibilities during digital law enforcement situations.

Ananth Padmanabhan and Vasudha Singh (2019)[15] article shows how Aadhaar judgment surveillance practices affect constitutional rights to establish personal identity and handle data

[10] Apar Gupta, "Balancing Online Privacy in India", 6 *Indian Journal of Law and Technology* 43 (2010). *Available at*: https://repository.nls.ac.in/ijlt/vol6/iss1/2/
[11] Latha R. Nair, "Data Protection Efforts in India: Blind Leading the Blind?", 4 *Indian Journal of Law and Technology* Art. 2 (2008). *Available at*: https://repository.nls.ac.in/ijlt/vol4/iss1/2/
[12] Jaideep Reddy, "The Central Monitoring System and Privacy: Analysing What We Know So Far", 10 *Indian Journal of Law and Technology* 13 (2014). *Available at*: https://repository.nls.ac.in/ijlt/vol10/iss1/2/
[13] Bedavyasa Mohanty, "Inside the Machine: Constitutionality of India's Surveillance Apparatus", 12 *Indian Journal of Law and Technology* 206 (2016). *Available at*: https://repository.nls.ac.in/ijlt/vol12/iss2/4/
[14] Giancarlo F. Frosio, "Internet Intermediary Liability: WILMap, Theory and Trends", 13 *Indian Journal of Law and Technology* Art. 2 (2017). *Available at*: https://repository.nls.ac.in/ijlt/vol13/iss1/2/
[15] Ananth Padmanabhan and Vasudha Singh, "The Aadhaar Verdict and the Surveillance Challenge", 15 *Indian Journal of Law and Technology* 1 (2019). *Available at*: https://repository.nls.ac.in/ijlt/vol15/iss1/1/

ISSN: 2582-6433

and enforce state surveillance. The study examines how proportionality measures and privacy protection methods and extensive digital governance systems create threats to personal safety.

Lalit Panda (2019)[16] article studies informational privacy through regulatory frameworks which identify how secrecy practices and inadequate disclosure and noncompliance create obstacles. The study assesses data governance practices and state responsibility and the privacy effects of digital regulatory systems which lack transparency.

Varun Majithia (2019)[17] article studies how intermediary liability laws evolved through time while showing that digital platforms now face stricter obligations. The study provides insights into platform responsibility and notice-and-takedown systems and their subsequent legal implications.

Mark J. Taylor and Jeannie Marie Paterson (2020)[18] article examines how India protects personal data through consent requirements and fair data processing rules. The study serves two main purposes because it establishes the normative foundation for personal data regulations and evaluates the effectiveness of legal consent frameworks in safeguarding digital users rights.

1.8 Research Gap

Researchers have studied various aspects of privacy surveillance and data protection in India through their work on intermediary liability but no complete research exists that examines how social media impacts policing authority and criminal procedures and evidential requirements based on Indias present criminal legal system. The existing research predating the Bharatiya Nagarik Suraksha Sanhita 2023 and the Bharatiya Sakshya Adhiniyam 2023 fails to address audio-video electronic procedures and electronic communication methods and electronic records treatment in criminal justice systems. The research lacks sufficient theoretical examination which would connect constitutional rights to platform regulation and digital law enforcement methods and personal data management within a unified criminal justice framework.

[16] Lalit Panda, "The Weight of Secrets: Assessing the Regulatory Burden for Informational Privacy in India", 15 *Indian Journal of Law and Technology* Art. 3 (2019). *Available at*: **https://repository.nls.ac.in/ijlt/vol15/iss1/3/**

[17] Varun Majithia, "The Changing Landscape of Intermediary Liability for E-Commerce Platforms: Emergence of a New Regime", 15 *Indian Journal of Law and Technology* Art. 8 (2019). *Available at*: https://repository.nls.ac.in/ijlt/vol15/iss2/8/

[18] Mark J. Taylor and Jeannie Marie Paterson, "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection", 16 *Indian Journal of Law and Technology* Art. 4 (2020). *Available at*: https://repository.nls.ac.in/ijlt/vol16/iss1/4/

ISSN: 2582-6433

2. EVOLUTION OF POLICING POWERS IN THE DIGITAL AGE

Law enforcement agencies in India now use digital technology for police operations which allows them to gather data through social media platforms to create leads which stop crimes and maintain control of public spaces. The legal framework permits this transition because the criminal procedure system acknowledges electronic communication and audio-video electronic methods as valid procedures for conducting official duties and creating official records according to the definitions of audio-video electronic means and electronic communication established in the Bharatiya Nagarik Suraksha Sanhita 2023 BNSS. The current state of policing allows law enforcement officers to conduct their duties at locations which include platform feeds and group chats and live streams because the legal assessment process needs to follow the newest procedural standards instead of digital practices which do not have formal guidelines.[19]

2.1 Digital Platforms Bring Transformation to Traditional Policing Methods

Police departments now use digital platforms to launch their operations because these platforms enable officers to receive complaints through electronic channels and track social media activity and validate information through quick verification systems which process information. The BNSS 2023 framework establishes common electronic procedures for main legal procedures which include using electronic communication to deliver summons documents in Sections 64 and 71 because this system enables quick access to online data and official judicial proceedings. Law enforcement agencies now begin their investigations through platform data which leads to BNSS documentation because compliance with procedural regulations establishes the legal framework to maintain digital records. [20]

2.2 Social Media Functions as a Resource for Monitoring and Identifying and Gathering Intelligence Information

Authorities use social media platforms for open-source intelligence gathering together with heightened surveillance operations although their ability to conduct advanced surveillance activities depends on existing legal frameworks and protective measures. The Information

[19] Dr. Pupul Dutta Prasad, *AI In Policing: Framing Issue Of Regulation*, Live Law, Oct. 4, 2025, *available at*: https://www.livelaw.in/articles/ai-policing-framing-issue-regulation-305808 (last visited May 2, 2026)
[20] Nupur Thapliyal, *Delhi High Court Seeks SOP From Social Media Platforms To Prevent Delay In Sharing Of Information About...*, Live Law, Oct. 1, 2024, *available at*: https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-seeks-sop-from-social-media-platforms-to-prevent-delay-in-sharing-of-information-about-missing-persons-with-police-271244 (last visited May 2, 2026)

ISSN: 2582-6433

Technology Act, 2000 enables authorities to intercept and monitor communications and decrypt data under Section 69 and to restrict public access through blocking directions under Section 69A whereas Section 69B allows authorities to monitor and collect traffic data during cyber security operations which creates pathways for digital policing activities. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 establish intermediary due diligence requirements through Rule 3 which applies to all intermediaries and Rule 4 which requires additional due diligence from significant social media intermediaries thus determining how platforms will handle lawful orders and law enforcement requests which include 24×7 operational roles and structured compliance reporting.[21]

2.3 Expansion of Investigative Powers in Online Spaces

Law enforcement agencies nowadays need to quickly obtain all devices and accounts together with digital evidence because social media platforms require immediate access to all digital evidence for authorized evidence collection that will be documented during active casework. BNSS 2023 establishes a strong procedural requirement which mandates that all search and seizure operations must use audio-video electronic recording systems for documentation purposes according to Section 105 and all recorded materials must be submitted to the designated Magistrate without any delay which creates a reliable evidence chain that connects online activities to physical evidence and device confiscation. The expansion of investigative abilities creates operational problems for police which arise from their need to maintain selective recording and partial device capture and proper device handling and device evidence forwarding process. [22]

2.4 Limits of Police Authority in Monitoring Digital Communication

Police powers to monitor digital communications reach their constitutional boundaries through their constitutional rights and statutory requirements because these need technical methods for information access. The IT Rules 2021 which establish intermediary obligations through Rule 3 and Rule 4 require platforms to deliver their cooperation through legitimate judicial procedures instead of handling requests through informal channels. The Digital Personal Data

[21] Why Do We Need Surveillance Reform in India? – Recent Developments SCC Times, *available at*: https://www.scconline.com/blog/post/2021/11/08/why-do-we-need-surveillance-reform-in-india-recent-developments/ (last visited May 2, 2026)

[22] Vagisha Mandloi, *AI In Digital Forensics: Are Indian Evidence Laws Equipped To Handle Machine-Generated Proof?*, Live Law, Apr. 27, 2026, *available at*: https://www.livelaw.in/articles/digital-forensics-indian-evidence-laws-ai-generated-proof-531826 (last visited May 2, 2026)

ISSN: 2582-6433

Protection Act 2023 recognizes substantial exemptions for personal data that investigators use during investigation and preventive measures and prosecutorial activities (Section 17(1)(c)). The legal system requires organizations to demonstrate all three elements of necessity and legality and internal accountability through their protection systems because constitutional rights under Articles 14 and 19 and Article 21 remain in effect against government actions. [23]

3. CONSTITUTIONAL PROTECTIONS AND CIVIL LIBERTIES IN INDIA

The constitutional framework establishes its rules for social-media policing as State action which needs to satisfy all three equality requirements through Article 14 and speech protection requirements which include reasonable restrictions through Articles 19(1)(a) and 19(2) and life and personal liberty protection through Article 21. The legal protections function through three operational stages which include the following steps of determining which activities hinder legal expression through their monitoring or takedown functions and evaluating whether law enforcement measures operate through arbitrary methods or target specific groups and that data collection needs to match legitimate operational goals. The use of digital tools for policing enables social media platforms to combine public and private spaces which increases the level of constitutional examination.[24]

3.1 Right to Privacy and Informational Autonomy in Digital Spaces

Social media privacy extends beyond content secrecy because it enables users to control their personal data and their online conduct and their connections with other people. The State's data collection practices which involve user data from platforms which it stores and connects across different databases violate Article 21 which safeguards life and personal freedom. The DPDP Act 2023 permits certain processing activities to proceed without restrictions because these activities serve law enforcement needs which include crime prevention and criminal investigation and prosecution (Section 17(1)(c)). The legal framework requires organizations to demonstrate their monitoring needs through established objectives which guide their monitoring activities while maintaining oversight to prevent unauthorized data collection. The

[23] Raghav Ahooja, *Challenging The Validity Of The IT Rules, 2021 - Can Rules Relating To Digital Media Be Made Under The IT ...*, Live Law, Mar. 4, 2021, *available at*: https://www.livelaw.in/columns/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-ministry-of-electronics-and-information-technology-meity-170715 (last visited May 2, 2026)

[24] naman vig, *Can Regulation Curb The Spread? Evaluating Social Media Controls Against Misinformation*, Live Law, Jan. 28, 2026, *available at*: https://www.livelaw.in/lawschool/articles/social-media-controls-misinformation-regulation-520770 (last visited May 2, 2026)

ISSN: 2582-6433

constitution mandates that governments need to provide legitimate reasons for conducting their surveillance activities because they cannot assume authority over their citizens.

3.2 Freedom of Speech and Expression on Social Media Platforms

Article 19(1)(a) protects speech and expression, and Article 19(2) allows only "reasonable restrictions" which must follow the specified grounds that include sovereignty and integrity and security of the State and public order and decency and morality and defamation and contempt of court and incitement to an offence. When law enforcement agencies depend on social media the primary legal issue becomes determining which types of speech should face restrictions and which ones should receive protection as lawful criticism and political dissent and satire. Government authorities need to base their content restrictions on statutory procedures which require constitutional standards of reasonableness instead of using their institutional preferences or reputation considerations.[25]

3.3 Equality, Non-Arbitrariness, and Protection against Discriminatory Policing

The implementation of Article 14 delivers legal protection against discrimination through two fundamental rights which establish equal treatment under the law and equal rights to legal protection. The enforcement of social media laws creates a risk of discrimination because police activities concentrate on specific social groups and geographical areas and particular political beliefs, especially when officers use risk assessment methods that rely on social connections and user behavior instead of direct evidence against specific individuals. The DPDP Act 2023 exemptions which enable investigative processing through Section 17, need Article 14 to govern State choices through standard operating procedures which utilize scientific methods and established protection measures. The system of digital policing creates an environment where bias can propagate throughout operations because it operates without proper oversight mechanisms and limited access to solutions. [26]

3.4 Balancing State Security Interests with Individual Constitutional Rights

Legal frameworks depend on constitutional boundaries and statutory protections to establish

[25] Constitutional Law of India - Chapter 8 Right to freedom, http://student.manupatra.com/Academic/Abk/Constitutional-Law-of-India/CHAPTER-8.htm (last visited May 2, 2026)

[26] Uddhav Gupta & R Sathvik, *The Regulatory Blind Spot In India's Digital Personal Data Protection Framework*, Live Law, Mar. 11, 2026, *available at*: https://www.livelaw.in/articles/regulatory-blind-spot-digital-personal-data-protection-framework-525875 (last visited May 2, 2026)

ISSN: 2582-6433

their balance between security needs and individual rights. Article 19(2) establishes valid reasons for speech limitations while Article 21 restricts government actions that infringe upon personal freedom and privacy rights, and Article 14 prevents authorities from choosing their enforcement targets through arbitrary methods. The IT Act Section 69 establishes formal methods for interception and monitoring while Section 69A enables blocking and the IT Rules 2021 intermediary compliance system establishes traceable processes through Rule 3 and Rule 4. Criminal procedure initiation through online content requires compliance with BNSS 2023 for recording and all following procedures. The State must demonstrate its security justification through actions that the law permits to be examined instead of imposing perpetual unexamined digital authority. [27]

4. EVIDENTIARY AND PROCEDURAL ISSUES IN SOCIAL MEDIA-BASED CRIMINAL JUSTICE

The criminal justice system which uses social media for investigations fails to function because authorities must establish evidence through legal methods that prove its authenticity and integrity and proper collection methods. The Bharatiya Sakshya Adhiniyam 2023 BSA establishes electronic record evidence rules which Indian evidentiary law now uses to authenticate digital records. BNSS 2023 Section 105 which requires digital audit trails for all procedures establishes a standard by which investigators and prosecutors must handle social media evidence.

4.1 Admissibility of Social Media Content in Criminal Proceedings

Social media content becomes admissible when it meets the requirements of an electronic record and fulfils the legal requirements for establishing such records. The BSA 2023 law establishes rules for admitting electronic records as evidence which requires a specific certificate to prove its validity (Section 63) that contains particular details about the evidence (Section 63(4)) and describes how the record material was obtained and which devices were used and who is authorized to confirm its authenticity. The legal requirement demands that posts and chats and videos must undergo extraction and certification processes which need to follow proper standards because any failure to meet this requirement will result in court

[27] Restrictions on Public Official's Freedom of Speech: Judgement Summary Supreme Court Observer, *available at*: https://www.scobserver.in/reports/restrictions-on-public-officials-freedom-of-speech-judgement-summary/ (last visited May 2, 2026)

ISSN: 2582-6433

treatment of crucial evidence as unverified evidence.[28]

4.2 Authenticity, Reliability, and Integrity of Digital Evidence

Social media platforms raise greater authenticity issues because users can edit content and re-upload it and create deepfake materials and strip away its original context and generate content through automated systems while the metadata information which includes timestamps and device identifiers and origin data holds more valuable evidence than the visible text. The BSA 2023 law establishes stable evidence through two pathways which allow electronic records and secure electronic records together with their signature components to receive presumption status from the Act (Sections 85-87). The proof system requires proper evidence collection and preservation and certification through Section 63 which means that the random screenshot lacks automatic validation through these presumptions. [29]

4.3 Procedural Safeguards in Collection, Preservation, and Production of Online Material

The enforcement of procedural safeguards maintains social media evidence which depends on established legal procedures as well as complete investigative documentation. BNSS 2023 requires that all search and seizure activities need to be documented through audio-video electronic means at Section 105 which requires authorities to send these recordings to the Magistrate. The evidence from social media platforms needs device evidence collection through BNSS recording requirements and BSA 2023 certification procedures at Section 63(4) which establish two protection systems that include one standard for evidence collection methods and one standard for evidence presentation methods.

4.4 Anonymity and Encryption Protection Problems

Along With Jurisdictional Problems Which Create Investigation Difficulties The process of identifying people who use encryption technology and their protected activities becomes complicated because both anonymity and encryption methods hide their identities. The IT Rules 2021 establish compliance requirements for major social media platforms through their Rule 4 regulations which include procedures for executing legal mandates while the IT Act

[28] Abhiraj Jayant, *How To Fulfill Requirements Of Admissibility Of Electronic Evidence Under Bhartiya Sakshay Adhiniyam,...*, Live Law, June 26, 2024, *available at*: https://www.livelaw.in/articles/electronic-evidence-admissibility-section-63-bhartiya-saksha-adhiniyam-2023-261511 (last visited May 2, 2026)
[29] Aayushman Gaikwad & Smruti Mishra, *Three Hours To Comply: India's New Rules For AI-Generated Content And Deepfakes*, Live Law, Feb. 21, 2026, *available at*: https://www.livelaw.in/articles/ai-generated-content-deepfakes-524064 (last visited May 2, 2026)

ISSN: 2582-6433

2000 grants authorities the power to monitor and intercept communications according to Section 69 and Section 69A regulations. The process of investigating a case requires lawful entry to systems while obtaining valid evidence through BSA 2023 Section 63 standards needs proper authority and legal procedures instead of using informal connections with platforms.[30]

5. DATA PROTECTION, ACCOUNTABILITY, AND REGULATORY GAPS

Social media policing necessitates the collection of personal information which includes user identifiers, their behavioural patterns, their contact information, their geographical data, and the attributes which people deduce about them. The DPDP Act 2023 establishes rules for personal data processing in India while allowing exemptions for specific functions which include police investigations and judicial proceedings according to Section 17(1)(c). Police surveillance systems do not receive automatic protection because the law lacks such operational security measures. The implementation process requires multiple agencies to handle regulatory gaps because it needs officials to decide who can collect information and how long data can be kept and what auditing procedures will take place and how instances of misuse will be identified.[31]

5.1 Collection and Use of Personal Data by Law Enforcement Agencies

Law enforcement agencies obtain personal information from public posts platform reports device extractions and intermediary responses. The collection of personal data becomes legal when authorities establish a specific purpose and use approved methods. The DPDP Act 2023 allows processing for prevention detection investigation or prosecution as an exemption under Section 17(1)(c) yet it should serve as a limited exception which requires permission because constitutional boundaries under Articles 14 and 21 restrict all government data processing. The IT Act 2000 provisions which include Section 69 monitoring and decryption directions and the intermediary due diligence requirements established in IT Rules 2021 Rule 3 and Rule 4 serve as the official rules for obtaining and handling platform data when access goes through

[30] Child safety and encryption: Analysing the IT Rules of 2021 SCC Times, *available at*: https://www.scconline.com/blog/post/2021/06/08/child-safety-and-encryption/ (last visited May 2, 2026)
[31] Shally Bhasin & Varun Pathak, *Consent: The Foundation Of Digital Data Protection*, Live Law, Mar. 18, 2026, *available at*: https://www.livelaw.in/articles/consent-digital-data-protection-future-526937 (last visited May 2, 2026)

ISSN: 2582-6433

intermediaries. [32]

5.2 Consent, Purpose Limitation, and Risks of Excessive Data Retention

Social media policing bypasses meaningful consent because investigators process data through their legal authority instead of obtaining consent from individuals, which requires organizations to follow specific rules for handling data and maintaining data security. The DPDP Act 2023 establishes exemptions for particular investigative needs which exist in Section 17 but the law still requires essential legal boundaries to be established when organizations keep data for "just in case" purposes which leads to their ability to track people and use their information for purposes that differ from what was studied during the initial investigation. The IT Act 2000 establishes requirements for intermediaries to maintain and store their information through its Section 67C rules which demonstrate that retention functions as a legal tool but retention practices become unrestricted when organizations lack sufficient regulatory control which leads to the unlawful collection of public data for noncriminal purposes.

5.3 Transparency and Accountability in Social Media Surveillance Practices

Law enforcement agencies can achieve better accountability through their ability to capture all police activities in written format which allows their activities to undergo evaluation while citizens can challenge their decisions through established protocols. The BNSS 2023 law mandates audio video documentation of search and seizure activities according to its Section 105 requirement which functions as a procedural accountability tool because it helps prevent evidence tampering while enabling judicial examination at future times. The IT Rules 2021 establish extra monitoring requirements for major social media platforms through their Rule 4 implementation which mandates platforms to report their compliance status while maintaining 24×7 contact procedures which produce evidence of legal orders and platform activities. Institutions fail to provide transparent practices because their "soft surveillance" operations conduct informal monitoring operations which collect data without legal permission, creating constitutional violations of Articles 14, 19, and 21 rights. [33]

[32] Digital Personal Data Protection Rules, 2025 Explained SCC Times, *available at*: https://www.scconline.com/blog/post/2025/11/14/meity-notified-digital-personal-data-protection-rules-2025/ (last visited May 2, 2026)

[33] Justice Capacity: Challenges and Opportunities - NALSAR Conference Report SCC Times, *available at*: https://www.scconline.com/blog/post/2025/10/16/justice-capacity-challenges-opportunities-nalsar-conference-report/ (last visited May 2, 2026)

ISSN: 2582-6433

5.4 Regulatory Deficiencies in Governing Police Access to Digital Platforms

Police access to social media data (public and non-public) lacks regulation because no comprehensive legal framework exists which would create standardized procedures for their access. The BNSS 2023 document defines procedural rules for electronic summons which appear in Sections 64 and 71 and recorded searches which appear in Section 105 while the IT Act of 2000 grants special monitoring powers through Section 69 and blocking rights through Section 69A and the DPDP Act 2023 creates exemptions through Section 17. Social media policing practices need clearer standards which explain how to measure proportionality and minimisation and retention and independent audit of social media policing operations because existing legal instruments do not provide those standards.

6 MISUSE, OVERREACH, AND HUMAN RIGHTS CONCERNS IN DIGITAL POLICING

Digital policing expands governmental authority through its ability to maintain continuous surveillance while it conducts immediate operational changes and creates complete networks which enable authorities to monitor citizens' speech activities and their ability to establish social connections and their freedom rights. The constitutional risks are not abstract: Article 19(1)(a) speech protection is vulnerable to chilling effects; Article 14 equality is vulnerable to selective enforcement; and Article 21 liberty and privacy are vulnerable to intrusive monitoring and profiling. The situation becomes more dangerous when authorities use unofficial online surveillance to replace proper legal procedures which require them to gather evidence and when officials fail to record their investigation activities according to BNSS 2023 standards.

6.1 Risks of Profiling, Targeting, and Predictive Monitoring through Social Media

The police develop profiling risks because they base their operational decisions on patterns of public engagement and identification through social media connections and group membership and their ability to assess individual traits. The DPDP Act 2023 allows investigative processing exemptions through Section 17(1)(c) yet profiling must meet constitutional standards which require non-arbitrary implementation according to Article 14 and protection of individual freedom and privacy rights according to Article 21. The BNSS 2023 recording requirement of Section 105 functions as the basic protection against hidden enforcement methods because it demands real-time documentation of how enforcement officials executed their forceful

ISSN: 2582-6433

measures.[34]

6.2 Chilling Effect on Dissent, Association, and Democratic Participation

A chilling effect occurs when people self-censor because they anticipate surveillance, harassment, or punitive action for lawful speech. Article 19(1)(a) protects expression, and Article 19(2) restricts the State to specified grounds for imposing reasonable restrictions; therefore, blanket monitoring or punitive responses to lawful dissent raise constitutional concerns even before criminal process begins. The State must follow IT Act 2000 Section 69A and IT Rules 2021 Rule 3 and Rule 4 for content removal and blocking activities because they require lawful orders and traceable compliance; this requirement helps maintain legal boundaries between proper public-order management and suppression of legitimate expression.

6.3 Arbitrary Interference, Selective Enforcement, and Abuse of Discretion

The online environment makes it simpler to apply selective law enforcement because police actions begin with viral content rather than assessment of serious crimes and political pressure bypasses legal requirements while police officers use their own discretion to decide which violations to pursue instead of following established procedures. Article 14 prohibits arbitrary State action, while Article 21 operationalizes judicial restrictions that control official powers which impact citizens' essential rights to freedom and control their personal information, and these legal protections extend to law enforcement procedures which depend on digital technology. The BNSS 2023 document establishes methods to decrease arbitrariness through its electronic service regulations and search and seizure documentation which create authentic records that enable analysis of judicial processes based on established fairness and rights and legal standards.[35]

6.4 Human Rights Standards Applicable to Technology-Assisted Policing

The implementation of technology-assisted policing systems with human rights compliance needs to follow five main requirements which include: valid legal basis, clear intent, proven necessity, proportionality requirements and functional monitoring systems. The Indian legal system implements these standards through constitutional rights and legal protections which

[34] Uddhav Gupta & R Sathvik, *The Regulatory Blind Spot In India's Digital Personal Data Protection Framework*, Live Law, Mar. 11, 2026, *available at*: https://www.livelaw.in/articles/regulatory-blind-spot-digital-personal-data-protection-framework-525875 (last visited May 2, 2026)

[35] Jennifer Earl et al., *The digital repression of social movements, protest, and activism: A synthetic review*, 8 Science advances eabl8198 (2022)

ISSN: 2582-6433

exist in current laws. The integrated approach emerges as the critical solution because severe violations of rights emerge from multiple minor unauthorized processes which become possible through technological systems.[36]

6.5 Case Laws

Justice ***K.S. Puttaswamy (Retd.) v. Union of India***[37] Supreme Court recognized privacy as a fundamental right which exists under Articles 14 19 and 21 and this established constitutional boundaries for technology-based law enforcement and extensive data collection methods. The investigation of social media surveillance together with the DPDP Act 2023 Section 17 and BNSS 2023 operational procedures establishes a framework for examination.

People's Union for Civil Liberties PUCL v. Union of India[38] Court established that State surveillance operations must conform to constitutional standards which require monitoring of communications to be conducted according to legal authority and protective measures that apply to IT Act 2000 Section 69 and Article 21 restrictions on digital surveillance.

Shreya Singhal v. Union of India[39] Court established that online speech receives protection through Article 19 1 a and the ruling established constitutional boundaries which restrict criminal charges against people who use ambiguous online language. This establishes the minimum requirements which police officers must meet when they monitor social media speech and conduct platform removals according to IT Act 2000 Section 69A and IT Rules 2021.

Anuradha Bhasin v. Union of India[40] Court ruled that internet access restrictions required evaluation and should be tested through proportionality assessment. This rule applies in cases where authorities use network disruptions together with content controls and platform-based public-order methods to enforce order, which infringes on Article 19 rights.

Faheema Shirin R.K. v. State of Kerala[41] High Court established that internet access functions as fundamental right because it enables people to exercise autonomy and receive education while safeguarding their privacy rights. The Court recognized that police practices which restrict online access to legitimate activities infringe upon Articles 19 and 21 rights.

---

[36] Asress Adimi Gikay, *REGULATING USE BY LAW ENFORCEMENT AUTHORITIES OF LIVE FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SPACES: AN INCREMENTAL APPROACH*, 82 The Cambridge Law Journal 414–449

[37] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; AIR 2017 SC 4161

[38] People's Union for Civil Liberties PUCL v. Union of India (1997) 1 SCC 301 AIR 1997 SC 568

[39] Shreya Singhal v. Union of India (2015) 5 SCC 1 AIR 2015 SC 1523

[40] Anuradha Bhasin v. Union of India (2020) 3 SCC 637 AIR 2020 SC 1308

[41] Faheema Shirin R.K. v. State of Kerala (2019) 4 KER LT 301

ISSN: 2582-6433

The court required proof of electronic evidence through ***Anvar P.V. v. P.K. Basheer***[42] which established new standards for BSA 2023 Section 63 and Section 63(4) to handle social media evidence.

The court established mandatory certification requirements for electronic records according to ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal***[43] because the BSA 2023 Section 63(4) framework currently demands social media extracts to comply with trial standards.

The court defined intermediary responsibility requirements together with monitoring and takedown obligations through ***Sabu Mathew George v. Union of India***[44] which established police-platform coordination must follow the statutory process defined by the IT Act of 2000 and the IT Rules of 2021.

The court demonstrated through ***Swami Ramdev v. Facebook Inc.***[45] that injunctions and platform removal procedures establish new legal connections between courts and intermediaries which control online content according to IT Act 2000 Section 79 and IT Rules 2021 takedown processes.

The Division Bench established through ***Myspace Inc. v. Super Cassettes Industries Ltd***[46] that requiring intermediaries to implement extensive worldwide monitoring systems inhibits free speech which violates Article 19 and establishes the necessity for intermediaries to comply with legally established order-based compliance frameworks.

7 CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

Policing now uses social media as its primary operational platform. Social media usage in criminal justice needs to follow precise law enforcement standards which have reached their most recent updates. The digital-era procedure of BNSS, 2023 enables electronic communication through its Section 2(1)(i) provision while its Sections 64 and 71 enable electronic summons service and Section 105 mandates audio-video recording of search and seizure. The BSA, 2023 establishes social media content proof as electronic evidence through its Section 63 requirements for admissibility and certification. The legal system uses Articles 14, 19, and 21 constitutional rights to evaluate both arbitrary actions and their impact on public safety and digital policing operations.

[42] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
[43] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCR 180
[44] Sabu Mathew George v. Union of India, (2018) 3 SCC 229; AIR 2018 SC 578
[45] Swami Ramdev v. Facebook Inc. (2019) 263 DLT 689; AIRONLINE 2019 DEL 1749
[46] Myspace Inc. v. Super Cassettes Industries Ltd. 236 (2017) DLT 478

ISSN: 2582-6433

7.2 Recommendations

1. All operational policing manuals together with their training programs must establish links to the digital accountability tools from BNSS 2023 which specifically require complete compliance with Section 105 for both recording and immediate submission to the Magistrate in order to decrease legal disputes about social media-based search and seizure operations.
2. Investigation units must implement standard evidence-handling protocols which directly match the BSA 2023 Section 63 and Section 63 4 certification standards to demonstrate social media content as electronic records instead of informal screenshots.
3. All platform requests must follow the authorized procedures established by IT Act 2000 which includes Sections 69 and 69A while their tracking should occur through intermediary due diligence procedures specified in IT Rules 2021 Rule 3 and Rule 4 to stop unauthorized monitoring and provide trackable records.
4. Oversight mechanisms must receive stronger support because they need to control DPDP Act 2023 investigative exemptions which exist in Section 17 to ensure their application stays limited and matches Articles 14 19 and 21 through documented explanations, minimization procedures, retention boundaries, and regular assessment of digital policing methods.

BIBLIOGRAPHY

STATUTES

1. The Constitution of India, 1950
2. The Bharatiya Nagarik Suraksha Sanhita, 2023
3. The Bharatiya Sakshya Adhiniyam, 2023
4. The Digital Personal Data Protection Act, 2023
5. The Information Technology Act, 2000
6. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

BOOKS

1. Pavan Duggal, *Cyber Law* (Universal LexisNexis, New Delhi, 3rd edn., 2025). *Available at*: https://store.lexisnexis.com/en-in/products/cyber-law-an-exhaustive-section-wise-commentary-on-the-information-technology-act-along-with-rules-regulations-policies-notifications-etc-insku9788196241070.html

ISSN: 2582-6433

2. Justice Yatindra Singh, *Cyber Laws* (LexisNexis, 6th edn., 2016). *Available at*: https://store.lexisnexis.com/en-in/products/cyber-laws-insku9789351437338.html
3. S. V. Joga Rao, *Law of Cyber Crimes and Information Technology Law: Policy, Law & Practice* (LexisNexis Butterworths/Wadhwa, Nagpur, 2nd edn., 2009). *Available at*: https://library.bharatividyapeeth.edu/cgi-bin/koha/opac-detail.pl?biblionumber=668635
4. Pavan Duggal, *Cyberlaw: The Indian Perspective* (Saakshar Law Publications, New Delhi, 2002). *Available at*: https://cyberlawuniversity.com/product/cyberlaw-the-indian-perspective/
5. Justice Yatindra Singh, *Information Technology Law* (Law & Justice Publishing Co., New Delhi, 2024). *Available at*: https://lawjusticepublishing.com/bookcategory.asp?catid=136
6. M. P. Jain, *Indian Constitutional Law* (LexisNexis, 9th edn., 2025). *Available at*: https://store.lexisnexis.com/en-in/products/indian-constitutional-law-by-m-p-jain-insku9788119403134.html
7. H. M. Seervai, *Constitutional Law of India* (Eastern Book Company, 4th edn., reprint 2025). *Available at*: https://www.ebcwebstore.com/product/constitutional-law-of-india-in-3-volumes-h-m-seervai-4th-edition?products_id=16657
8. V. N. Shukla, *V. N. Shukla's Constitution of India* (revised by Mahendra P. Singh, Eastern Book Company, Lucknow, 13th edn., 2017). *Available at*: https://opac.kila.ac.in/cgi-bin/koha/opac-MARCdetail.pl?biblionumber=21491
9. Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, Oxford, 2014). *Available at*: https://global.oup.com/academic/product/asian-data-privacy-laws-9780199679669
10. B. N. Kirpal, Ashok H. Desai, Gopal Subramanium, Rajeev Dhavan and Raju Ramachandran (eds.), *Supreme but Not Infallible: Essays in Honour of the Supreme Court of India* (Oxford University Press, New Delhi, 2000). *Available at*: https://global.oup.com/academic/product/supreme-but-not-infallible-9780195672268

JOURNALS

1. Subhajit Basu, "Policy-Making, Technology and Privacy in India", 6 *Indian Journal of Law and Technology* 65 (2010). *Available at*: https://repository.nls.ac.in/ijlt/vol6/iss1/3/

ISSN: 2582-6433

2. Apar Gupta, "Balancing Online Privacy in India", 6 *Indian Journal of Law and Technology* 43 (2010). *Available at*: https://repository.nls.ac.in/ijlt/vol6/iss1/2/
3. Latha R. Nair, "Data Protection Efforts in India: Blind Leading the Blind?", 4 *Indian Journal of Law and Technology* Art. 2 (2008). *Available at*: https://repository.nls.ac.in/ijlt/vol4/iss1/2/
4. Jaideep Reddy, "The Central Monitoring System and Privacy: Analysing What We Know So Far", 10 *Indian Journal of Law and Technology* 13 (2014). *Available at*: https://repository.nls.ac.in/ijlt/vol10/iss1/2/
5. Bedavyasa Mohanty, "Inside the Machine: Constitutionality of India's Surveillance Apparatus", 12 *Indian Journal of Law and Technology* 206 (2016). *Available at*: https://repository.nls.ac.in/ijlt/vol12/iss2/4/
6. Giancarlo F. Frosio, "Internet Intermediary Liability: WILMap, Theory and Trends", 13 *Indian Journal of Law and Technology* Art. 2 (2017). *Available at*: https://repository.nls.ac.in/ijlt/vol13/iss1/2/
7. Ananth Padmanabhan and Vasudha Singh, "The Aadhaar Verdict and the Surveillance Challenge", 15 *Indian Journal of Law and Technology* 1 (2019). *Available at*: https://repository.nls.ac.in/ijlt/vol15/iss1/1/
8. Lalit Panda, "The Weight of Secrets: Assessing the Regulatory Burden for Informational Privacy in India", 15 *Indian Journal of Law and Technology* Art. 3 (2019). *Available at*: https://repository.nls.ac.in/ijlt/vol15/iss1/3/
9. Varun Majithia, "The Changing Landscape of Intermediary Liability for E-Commerce Platforms: Emergence of a New Regime", 15 *Indian Journal of Law and Technology* Art. 8 (2019). *Available at*: https://repository.nls.ac.in/ijlt/vol15/iss2/8/
10. Mark J. Taylor and Jeannie Marie Paterson, "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection", 16 *Indian Journal of Law and Technology* Art. 4 (2020). *Available at*: https://repository.nls.ac.in/ijlt/vol16/iss1/4/
11. Greg Nojeim, Namrata Maheshwari and Eduardo Miglani, "Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth", 17 *Indian Journal of Law and Technology* Art. 2 (2021). *Available at*: https://repository.nls.ac.in/ijlt/vol17/iss1/2/
12. M. Vasudev Devadasan, "Conceptualising India's Safe Harbour in the Era of Platform Governance", 19 *Indian Journal of Law and Technology* Art. 1 (2023). *Available at*: https://repository.nls.ac.in/ijlt/vol19/iss1/1/

ISSN: 2582-6433

13. Samyukta Ramaswamy, "The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State", 20 *Indian Journal of Law and Technology* Art. 4 (2024). *Available at*: https://repository.nls.ac.in/ijlt/vol20/iss2/4/
14. Gavin Sutter, "Rethinking Online Intermediary Liability: In Search of the 'Baby Bear' Approach", 7 *Indian Journal of Law and Technology* Art. 3 (2011). *Available at*: https://repository.nls.ac.in/ijlt/vol7/iss1/3/
15. Ananth Padmanabhan, "Give Me My Space and Take Down His: Copyright, Safe Harbours and Injunctions in India", 9 *Indian Journal of Law and Technology* Art. 1 (2013). *Available at*: https://repository.nls.ac.in/ijlt/vol9/iss1/1/
16. Nikhil Kamath, "Should the Law Beat a Retweet? Rationalising Liability for Republication in India", 9 *Indian Journal of Law and Technology* Art. 4 (2013). *Available at*: https://repository.nls.ac.in/ijlt/vol9/iss1/4/
17. Daniel Trottier, "'Fear of Contact': Police Surveillance through Social Networks", 4(4) *European Journal of Cultural and Political Sociology* 457 (2017). *Available at*: https://direct.mit.edu/ecps/article/4/4/457/126067/Fear-of-contact-Police-surveillance-through-social
18. Lauren Mayes, "Social Media and Community-Oriented Policing: Examining the Organizational Image Construction of Municipal Police on Twitter and Facebook", 22(1) *Police Practice and Research* 903 (2021). *Available at*: https://researchportal.northumbria.ac.uk/en/publications/navigating-the-digital-beat-a-review-of-social-media-as-a-public-/
19. Elizabeth E. Joh, "Policing the Smart City", 15(2) *International Journal of Law in Context* 177 (2019). *Available at*: https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/policing-the-smart-city/D107A5808D6561101FE1C54550AF2D95
20. Pete Birnstill, Paul Bernal and Susan B. Jones, "Privacy-Preserving Surveillance: An Interdisciplinary Approach", 5(4) *International Data Privacy Law* 298 (2015). *Available at*: https://academic.oup.com/idpl/article/5/4/298/2404456
21. Stephen Owen, "Monitoring Social Media and Protest Movements: Ensuring Political Order through Surveillance and Surveillance Discourse", 23(6) *Social Identities* 688 (2017). *Available at*: https://www.tandfonline.com/toc/csid20/23/6
22. Liam Ralph, Ian C. Elliott, Joanne Murphy and Russ Glennon, "Navigating the Digital Beat: A Review of Social Media as a Public Engagement Tool in Policing", 13(3) *International Journal of Emergency Services* 201 (2024). *Available at*:

ISSN: 2582-6433

https://researchportal.northumbria.ac.uk/en/publications/navigating-the-digital-beat-a-review-of-social-media-as-a-public-/

23. James P. Walsh, Victoria Baker and Brittany Frade, "Policing and Social Media: The Framing of Technological Use by Canadian Newspapers (2005–2020)", 24(4) *Criminology & Criminal Justice* 819 (2024). *Available at*: https://vlex.co.uk/vid/policing-and-social-media-1069632494
24. Nigel G. Fielding, "Police Communications and Social Media", 23(2) *Criminology & Criminal Justice* 316 (2023). *Available at*: https://journals.sagepub.com/doi/abs/10.1177/1477370821998969