The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2024
Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

EXPLORING PRIVACY RIGHTS IN THE AGE OF SOCIAL MEDIA: A LEGAL LOOK AT INDIA

INTRODUCTION

Exploring Privacy Rights in the Age of Social Media: A Legal Look at India Social media has revolutionized our lives, but it has also thrown up complex legal questions, particularly concerning privacy rights. In India, where social media usage is exploding, navigating this legal landscape is crucial for both individuals and platforms. Here's a dive into the key legal aspects surrounding privacy rights in the age of social media in India.

LEGAL FRAMEWORK IN INDIA:

1. The Constitution and Right to Privacy: Puttaswamy vs. Union of India (2017): This landmark judgment recognized the right to privacy as a fundamental right inherent in Article 21, which guarantees the right to life and personal liberty. This established a strong foundation for privacy protection in the digital realm. Scope of Privacy Right: The Court acknowledged that privacy encompasses various aspects, including informational privacy (protection of personal data), decisional autonomy (control over choices), and bodily privacy. Balancing Act: The right to privacy is not absolute and can be restricted under certain circumstances, such as national security, public order, and prevention of crime. However, any restriction must be reasonable and proportionate.

2. Information Technology Act, 2000 (IT Act): Limited Scope: While enacted before the rise of social media, the IT Act provides some legal framework for online privacy. Key Provisions: Section 43A: Mandates reasonable security practices to protect sensitive personal data like passwords and financial information. Section 66A: (now repealed) Controversial provision that criminalized "offensive" online content, raising concerns about freedom of expression and

potential misuse. Section 72A: Empowers government agencies to intercept, monitor, and decrypt information under specific conditions, raising concerns about surveillance.

3. Draft Personal Data Protection Bill, 2019 (PDPB): Comprehensive Framework: This proposed legislation aims to establish a robust data protection regime addressing concerns not adequately covered by the IT Act. Key Features: Consent and Purpose Limitation: Users must provide informed consent for data collection and processing, and data can only be used for explicitly stated purposes. Data Minimization: Entities can only collect and process data necessary for the stated purpose. Right to Access, Rectification, and Erasure: Individuals have rights to access, correct, and request deletion of their personal data. Data Breach Notification: Entities must notify authorities and affected individuals in case of data breaches. Data Localization: Certain sensitive personal data may need to be stored within India. Current Status: The PDPB is under review and yet to be enacted. Its final form and impact on social media platforms remain uncertain.

KEY PRIVACY CONCERNS IN INDIA'S SOCIAL MEDIA LANDSCAPE:

1. Data Collection and Use: Extent of Data Collection: Social media platforms gather a vast array of personal data, including demographics, location, browsing history, interactions, and even private messages. This raises concerns about: Unauthorized Collection: Users might not be fully aware of the extent of data collected or give sufficient consent, leading to privacy violations. Use for Targeted Advertising: Platforms personalize ads based on collected data, which can feel intrusive and potentially discriminatory. Sharing with Third Parties: Sharing data with advertisers, data brokers, or other entities without transparent disclosure undermines user trust and control.

2. Right to be Forgotten: Current Ambiguity: While the Puttaswamy judgment hinted at the potential for a "right to be forgotten," the legal framework lacks concrete provisions specifically for social media platforms. Challenges in Implementation: Even if established, implementing this right could be complex due to concerns about balancing individual privacy with freedom of expression and public interest.

3. Profiling and Targeting: Algorithmic Bias: Platforms use algorithms to profile users based on data, leading to potential biases in targeted advertising or content recommendations. This can: Reinforce discrimination: Algorithmic bias can perpetuate existing societal biases, leading to unfair targeting based on race, gender, or other factors. Manipulation and "filter bubbles":

Personalized content can create echo chambers, filtering out diverse viewpoints and limiting exposure to new ideas.

4. Surveillance and Censorship: Government Surveillance: Concerns exist regarding government agencies accessing user data for surveillance purposes, potentially chilling free speech and dissent. Content Censorship: Government pressure or platform policies might lead to censorship of certain content, raising concerns about freedom of expression and access to information.

RECENT DEVELOPMENTS AND CHALLENGES IN PROTECTING PRIVACY RIGHTS ON SOCIAL MEDIA IN INDIA:

1. Supreme Court Rulings:

- Puttaswamy (2017): Established the right to privacy as fundamental, paving the way for stronger legal protections.
- K.S. Puttaswamy (Privacy) vs. Union of India (2019): Recognized specific aspects of privacy like informational privacy and the right to restrict data sharing.
- Shreya Singhal vs. Union of India (2015): Struck down Section 66A of the IT Act, protecting freedom of expression online.
- Justice KS Puttaswamy vs. Union of India (Aadhaar) (2018): Upheld the Aadhaar program with limitations, highlighting the need for balancing privacy with legitimate state interests.

Challenges:

- Interpreting the rulings' application to specific online activities and platforms.
- Ensuring effective enforcement of court-mandated safeguards.

2. Data Protection Regulations:

- Draft Personal Data Protection Bill (PDPB) 2019: Awaits finalization and implementation, offering potential for a comprehensive framework.
- Key features: Consent regulations, data minimization, individual rights like access and erasure, data breach notification, potential data localization.
- Challenges: Delays in enactment, concerns about government access to data, unclear provisions on right to be forgotten, limitations on cross-border data transfers.

3. Social Media Platform Accountability:

- Data breaches: Recent incidents exposed vulnerabilities and raised questions about data security practices of platforms.
- Targeted advertising and algorithmic bias: Concerns remain about discriminatory targeting and lack of transparency in algorithms.
- Content moderation and censorship: Balancing platforms' responsibility with freedom of expression remains a complex issue.
- Challenges: Implementing effective enforcement mechanisms, holding platforms accountable for opaque algorithms and content moderation decisions.

THE WAY FORWARD FOR PRIVACY RIGHTS IN INDIA'S SOCIAL MEDIA LANDSCAPE:

1. Stronger Legal Framework: Prioritize the Personal Data Protection Bill (PDPB): Timely enactment and effective implementation of the PDPB with clear provisions for: Strong consent mechanisms: Informed, freely given, and specific consent for data collection and use. Data minimization: Collecting and processing only the data necessary for stated purposes. Individual rights: Right to access, rectify, erase, and port personal data. Right to be forgotten: Clear guidelines for platforms to remove data upon request, considering legitimate interests. Data breach notification: Mandatory notification of data breaches to individuals and authorities. Data protection authority: An independent authority to enforce the law and address user complaints.

2. Platform Accountability: Transparency and user control: Platforms should provide clear and accessible information about data collection, use, and sharing practices. User-friendly dashboards: Individuals should have easy-to-use tools to manage their data privacy settings and preferences. Effective enforcement mechanisms: Regulatory bodies with power to investigate and impose sanctions on platforms violating privacy rights. Algorithmic accountability: Auditing algorithms for bias and ensuring transparency in content moderation decisions.

3. Privacy Education: National awareness campaigns: Educate the public about their privacy rights, online data risks, and tools for managing their data. Curriculum integration: Include

digital literacy and privacy education in school and university curricula. Empowering civil society: Support civil society organizations working on digital rights and user advocacy. Collaborative initiatives: Partner with platforms, educational institutions, and civil society to develop privacy-conscious online environments.