International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Right to Privacy V/S National Security Examining Media Surveillance Laws in India

Sarvajith Kumar J N[1], Manohar N[2]

[1]Assistant Professor, Department of Management, Cresta First Grade College, Mysuru, Karnataka – 570028.
[2]Assistant Professor, Department of Journalism, Government First Grade College for Women, M G Road, Hassan, Karnataka – 573202.

Abstract
This research examines the intricate legal and ethical issues of right to privacy versus national security in the context of media surveillance acts in India. Since surveillance activities with the use of the digital platform have been becoming increasingly prevalent, concerns about the constitutional validity, transparency, and proportionality of state-regulated media monitoring procedures have been arising. The article examines the laws that form the basis of Indian surveillance in the form of the Information Technology Act (2000), the Telegraph Act (1885), the Aadhaar Act, and the forthcoming Personal Data Protection Bill. The laws are examined against Article 21 of the Indian Constitution and the Supreme Court judgment in Justice K.S. Puttaswamy v. Union of India (2017), which established privacy as a constitutional right. The study employs qualitative, doctrinal research method founded on content analysis of legislative documents, case law, policy guidelines, and secondary scholarly literature. Comparative insights are made from foreign surveillance models to contrast India's model against a comparative model. The evidence shows serious legal and ethical issues, specifically the absence of judicial review, transparency gaps, and chilling effects on freedom of the press. The evidence points towards a rebalanced regime of surveillance based on accountability, democratic protection, and constitutional fidelity.

Keywords: Right to Privacy**,** National Security, Media Surveillance, Media Laws, Digital Rights.

1. INTRODUCTION

Background and Context

The regulation and law of surveillance in India have significantly evolved with accelerated digitization, heightened security threats, and more state intervention in monitoring digital communication. The balance between privacy rights and national security has been heightened as the state justifies surveillance programs as a counter to cyber attacks, terrorism, and disinformation (Bhatia, 2020). Nonetheless, concerns regarding judicial review, accountability, and their status in democratic rights have created a space for discussion of proportionality and necessity of state-initiated surveillance (Singh, 2021).

Multiple legal structures constitute India's surveillance machinery. The Information Technology (IT) Act, 2000 grants the executive the power to intercept, decrypt, and monitor electronic communication in the interest of security (Chandrasekhar, 2019). Indian Telegraph Act, 1885, one of the earliest

surveillance acts in India, authorizes the government to intercept and monitor telephone calls in the interest of wide national security interests (Ganguly, 2018). The Personal Data Protection Bill (PDPB), 2019, for regulating data privacy has been opposed on the ground that it permits the state to have blanket exemptions from data protection law, thus potentially facilitating mass surveillance (Basu, 2020). The Aadhaar biometric identity scheme has also generated legal issues over its applications in state surveillance and profiling of citizens (Bhatia, 2020).

The Justice K.S. Puttaswamy v. Union of India (2017) ruling marked a milestone in Indian privacy law as it established that privacy is a constitutional right under Article 21 of the Constitution (Bhatia, 2017). The ruling also held that reasonable restrictions on privacy are permissible in the interest of national security, allowing scope for liberal government interpretation of surveillance statutes. Projects like the Central Monitoring System (CMS) and NATGRID (National Intelligence Grid) have increased the surveillance potential of the state to monitor activities on the internet, which raises issues of transparency, judicial recourse, and misuse of surveillance systems (Ganguly, 2020).

The effect on online rights and freedom of the press has been a rising issue. The Pegasus spyware scandal, which involved journalists and activists allegedly being targeted by government-linked spyware, brought to light how vulnerable digital surveillance is to suppressing dissent and restricting freedom of the press (Mehta, 2021). Further, the more recent IT Rules amendments of 2021 have more strongly empowered the government to regulate digital media, social media, and online news media, raising concerns of censorship and government overreach (Saxena, 2021). All of these developments call for a careful analysis of whether India's present legal regime achieves an optimum balance between national security interests and constitutional privacy safeguards.

Research Problem and Significance

The key issue behind India's surveillance law is whether state security initiatives exempt the infringement of privacy rights. National security, terrorism, and cyberattacks have a valid reason for internet monitoring, but unchecked state surveillance can encroach on natural rights, especially freedom of expression and the right to privacy (Basu, 2020). Absence of an independent agency to monitor surveillance operations creates concerns about abuse of authority, transparency, and accountability to the law (Singh, 2021).

Judicial checks are necessary to guarantee that surveillance is proportionate, necessary, and legally justified. Judicial checks, nevertheless, continue to be weak in India since surveillance orders frequently come through executive commands rather than judicious judicial supervision (Chandrasekhar, 2019). Legal vagueness enables mass surveillance schemes to be run on broad, hazy mandates, and it makes politically motivated surveillance, silencing dissent, and censorship of the press more likely (Mehta, 2021).

The moral consequences of mass surveillance, real-time interception of data, and selective monitoring of journalists, activists, and opposition politicians underscore the importance of having better legal frameworks and more privacy protections (Ganguly, 2020). The study aims to present an in-depth legal and theoretical examination of media surveillance law in India, examining whether present frameworks balance privacy and national security or allow unrestricted state control of cyberspace.

Objectives of the Study

1. To critically discuss theoretical explanations of privacy, national security, and online monitoring, examining how legal structures explain surveillance policies.

2. To determine the most pressing issues and ethical challenges with India's media spy policies, including mass surveillance proposals, press freedom, and judicial accountability.
3. Contrast the laws of India regarding surveillance by the media with international models of regulation, with a view towards best practices in balancing privacy and national security.

Research Questions

1. What are India's constitutional and legal basis for media surveillance? (Chandrasekhar, 2019).
2. How do the laws of India balance privacy with national security concerns? (Bhatia, 2020).
3. What are the ethical and legal implications of state-sponsored regulation of media surveillance? (Mehta, 2021).
4. In what ways are India's media surveillance legislations contrasted with international privacy and security legislation? (Saxena, 2021).

The paper offers a systematic, qualitative examination of India's media surveillance regime, along with remarks on constitutional, legal, and moral privacy and national security discourses. Comparative international surveillance law is also discussed in order to compare diverse legal models of regulating state surveillance while promoting privacy protection and press freedom.

2. Literature Review

Theoretical Perspectives on Privacy and National Security The debate over national security and privacy rights has been a century-old legal and philosophical problem, with many theories providing insight into the legitimacy and bounds of state surveillance. In the context of India, where security needs need to be balanced against constitutional rights, a number of theoretical approaches provide a foundation for perspective on media surveillance law.

The Social Contract Theory, which Hobbes, Locke, and Rousseau formulated, holds that citizens surrender some of their rights to the state for protection and order (Rousseau, 1762/2018). In contemporary jurisprudence, the theory maintains that government surveillance is acceptable as a way to achieve public safety. To critics, however, mass surveillance encroaches on limited government and democratic accountability principles (Rawls, 1971). In India, national security is used by the government to justify mass surveillance, although there are concerns about the absence of independent checks and judicial protection (Basu, 2020).

John Stuart Mill's Principle of Harm provides the alternative, where the state becomes involved only when the acts of one person cause harm to others (Mill, 1859/2015). When applied to surveillance of the media, it simply calls for only plain and proximal harms to require invasion into privacy. The Indian surveillance legislations, however, aim to legitimate anticipatory monitoring on the basis of ambiguous phrases such as "public safety" and "national security", which leave the way open to indiscriminate state interference and oppression of opposition (Singh, 2021).

Foucault's Panopticism and Theory of Surveillance posits that mass surveillance produces a self-regulated society in which individuals adjust their behavior as they are always being watched (Foucault, 1977). This theory is very much applicable in India, where Aadhaar-based identification, surveillance of data online, and cyber security legislation facilitate state surveillance (Mehta, 2021). Critics have cautioned that ongoing state surveillance violates civil liberties, press freedom, and democratic dissent to the point that people feel obligated to censor themselves and media engagement (Ganguly, 2020).

These theoretical lenses furnish a blueprint for the analysis of India's surveillance media legislation,

including from a perspective of legitimacy, proportionality, and morality.

Legal Framework Governing Surveillance in India

India's surveillance law is governed by an array of legislation and government orders, creating a diffuse but pervasive framework of regulation.

The Indian Telegraph Act of 1885 permits tapping the phone and wiretapping in the event that it is needed for public safety and national security (Chandrasekhar, 2019). Although the act predates modern means of communications, it remains to be one of the main legal instruments for state surveillance. The Information Technology Act, 2000 grants additional powers of internet surveillance, under which government authorities can intercept, decrypt, and censor internet content in the name of national security (Bhatia, 2020). The laws do not have explicit judicial protection, and wide discretionary powers are conferred on the executive (Ganguly, 2020).

The Personal Data Protection Bill (PDPB), 2019, being a privacy protection bill, has been faulted for excluding the government from data protection (Basu, 2020). The criticisms fear that state agencies can spy, store, and process citizen information without legal monitoring, opening avenues for mass surveillance and abuse of personal data (Mehta, 2021).

Aadhaar surveillance is a real-time concern, with the biometric database being utilised for identity authentication, welfare dispensation, and security surveillance (Singh, 2021). Although the Justice K.S. Puttaswamy v. Union of India (2017) judgment reinforced privacy as a constitutional right, the verdict also permitted state surveillance in equilibrium situations, with space for government discretion over policy interpretation for surveillance (Bhatia, 2020).

The Pegasus spyware scandal showed how government spyware can be utilized against opposition leaders, activists, and journalists, raising concerns about press freedom and political abuse of surveillance technology (Mehta, 2021). The IT Rules (2021) also increased the powers of the government to monitor online content and social media, raising fears about censorship and possible limitations on media autonomy (Saxena, 2021).

Challenges in Balancing Privacy and Security

India faces several challenges in balancing privacy protections with national security needs, including mass surveillance concerns, threats to press freedom, and the absence of judicial oversight.

The government also has mass surveillance initiatives like the Central Monitoring System (CMS) and the National Intelligence Grid (NATGRID), which enable agencies to intercept, monitor, and record history of electronic communications (Ganguly, 2020). The programs are criticized as being opaque, running without independent oversight, and without any apparent judicial review mechanisms in place (Basu, 2020). Lack of a data protection authority to oversee storage and use of information gathered under surveillance magnifies privacy issues (Singh, 2021).

Press freedom has been impacted to a significant extent by state surveillance and online monitoring. Government surveillance, telephone tapping, and hacking attempts have been reported and documented by investigative reporters, resulting in self-censorship and the stifling of critical perspectives (Mehta, 2021). Online attacks on journalists conducted through Pegasus spyware have also raised questions regarding the responsibility of governments with regard to internet surveillance policies (Saxena, 2021).

Judicial supervision is also weak in India's surveillance apparatus. In contrast to the United States and Europe, where judicial approval is needed for the majority of digital surveillance, executive agencies in India can grant surveillance clearances without judicial supervision (Bhatia, 2020). This has the potential for abuse of surveillance authority for political and ideological domination (Chandrasekhar, 2019).

Comparative Analysis of Global Surveillance Laws

India's surveillance laws are compared with global privacy and security frameworks, highlighting key differences and best practices in regulating digital monitoring and protecting individual rights.

- United States (Patriot Act & FISA) – The USA Patriot Act expanded state surveillance post-9/11, allowing broad national security-based monitoring (Greenwald, 2014). However, legal challenges have led to reforms, including stricter judicial oversight and privacy protections (Basu, 2020).
- European Union (GDPR) – The General Data Protection Regulation (GDPR) establishes strict privacy rights, requiring government surveillance programs to undergo legal scrutiny (Ganguly, 2020). Unlike India, the EU mandates independent oversight bodies to regulate surveillance activities.
- China's Digital Surveillance System – China operates a state-controlled surveillance network with AI-based monitoring, censorship, and facial recognition tracking (Mehta, 2021). India's increasing reliance on digital surveillance has drawn comparisons to China's centralized monitoring system, raising concerns over authoritarian tendencies in media regulation (Saxena, 2021).

These comparisons suggest that India could benefit from stronger judicial safeguards, transparency in surveillance programs, and independent oversight mechanisms to ensure privacy protections.

3. Methodology

Research Design

This study applies qualitative analysis to the examination of surveillance laws in the Indian media, with emphasis on constitutional law, precedent judicial, and regimes of policy. The research is guided by theoretical models and legal case study to influence an integrated privacy and national security act. As an empirical work that does not include consumer interviews, surveys, or statistical analysis, the study utilizes doctrinal research methods, thematic analysis, and comparative legal study (Bhatia, 2020).

The study examines to what degree Indian surveillance laws conform or deviate from international legal standards. The comparison of international privacy and security legislation, i.e., the U.S. Patriot Act, the General Data Protection Regulation of the European Union (GDPR), and China's surveillance legislation is done to put India's law in perspective (Ganguly, 2020). It also looks into matters relating to legal and ethical concerns regarding press freedom, mass surveillance programs, and judicial oversight in India.

Selection of Case Studies to Analyze

This research compares key legal cases, government actions, and media accounts to analyze the Indian national security interests and privacy protections' balance. The case studies listed below were chosen:

- Justice K.S. Puttaswamy v. Union of India (2017) – In this case, privacy has been held as a constitutional right by Article 21 of the Indian Constitution. The ruling placed restrictions on state surveillance but had exceptions in cases where national security is at stake (Bhatia, 2020). This case is held to consider the way Indian courts perceive privacy related to state surveillance.
- The Pegasus Spyware Scandal (2021) – The revelation of the investigations unveiled the use of Pegasus spyware to target journalists, activists, and opposition leaders in India sparked illegal government spying and freedom of the press abuse issues (Mehta, 2021). This case study examines the government agencies' legal responsibility for the mass surveillance activities.
- The IT Rules, 2021 – They strengthened the monitoring of the government over social media websites, online news portals, and moderation of content online (Saxena, 2021). This study examines

the effect of such rules on freedom of expression, media autonomy, and regulatory supervision.

- The Aadhaar Biometric Identification System – The Aadhaar system has been criticized for its participation in biometric surveillance, data gathering, and privacy violations (Singh, 2021). The study investigates whether Aadhaar-linked surveillance systems are in line with constitutional privacy protection.

Data Collection and Analysis

The research relies on secondary data for the qualitative analysis of the media surveillance laws in India and other countries mentioned prior.

- Judicial Decisions and Constitutional Provisions – Examining court judgments, legal precedents, and constitutional arguments regarding surveillance and privacy (Basu, 2020).
- Legal Commentaries and Policy Reports – Examining scholarly debates on India's surveillance acts for the media, digital privacy, and national security exceptions (Chandrasekhar, 2019).
- Comparative Legal Analysis – Examining international surveillance regimes, e.g., the U.S. Foreign Intelligence Surveillance Act (FISA), the European GDPR, and China's cybersecurity law (Ganguly, 2020).
- Ethical and Theoretical Approaches – Using theoretical models like the Social Contract Theory, the Harm Principle, and Foucault's Surveillance Model to examine the philosophical and legal aspects of media surveillance (Mehta, 2021).

Analytical Framework

Thematic analysis is used in this study to spot major trends, legal rationales, and ethical issues in media surveillance law. Four major themes are examined by the study:

- Rationale for State Spying – The means by which Indian legal orders legitimate mass surveillance and internet monitoring.
- Press Freedom and Privacy Issues – The effect of surveillance law on journalism, freedom of expression, and democratic accountability.
- Judicial Scrutiny and Regulatory Holes – The contribution of judicial review, legal protection, and independent regulation to surveillance policy.
- Comparative Legal Analysis – The degree to which India's media surveillance law is comparable to or divergent from international privacy and security regimes.

4. Analysis and Discussion

This part discusses the constitutional, ethical, and legal controversies of media surveillance in India in terms of landmark case studies, thematic legal debate, and comparative analysis. The argument raises questions of balance between national security rationale and privacy rights, intrusion by the judiciary, and effects of media surveillance on democratic freedoms.

Descriptions of Selected Case Studies

1. Justice K.S. Puttaswamy v. Union of India (2017) – Establishing the Right to Privacy

- Legal Significance: The Supreme Court of India established privacy as a constitutional right under
- Article 21 of the Constitution, establishing a legal precedent regarding data protection, surveillance

- limits, and citizens' rights (Bhatia, 2020).
- Impact on Surveillance Law: The judgment established the doctrine of proportionality, which states that any restriction on privacy must be necessary, legitimate, and proportionate to the national security need (Singh, 2021).
- Limitations: Although the judgment acknowledged privacy as a constitutional right, it did not explicitly ban mass surveillance schemes such as Aadhaar-based surveillance and monitoring of CMS data (Ganguly, 2020).

2. The Pegasus Spyware Scandal (2021) – Surveillance of Journalists and Activists

- Incident: Investigative journalism reported that Pegasus spyware, which is reportedly employed by government agencies, had been employed against activists, opposition figures, and journalists (Mehta, 2021).
- Legal Issues: The absence of judicial supervision and accountability has raised issues about illegal monitoring, Press Freedom abuses, and abuse of national security legislation (Basu, 2020).
- Judicial Response: The Supreme Court ordered an independent technical committee to probe the allegations of surveillance, but no accountability mechanism was put in place (Saxena, 2021).

3. Aadhaar Biometric Surveillance and Data Privacy Issues

- Legal Basis: Aadhaar scheme, initiated for welfare disbursement and identity authentication, has been criticized for biometric surveillance, tracking of data, and security issues (Chandrasekhar, 2019).
- Privacy Risk: The government has associated Aadhaar with digital authentication, SIM cards, and financial transactions because they are all linked in one central database, raising the possibility of mass surveillance (Ganguly, 2020).
- Judicial Safeguard: The Supreme Court of India validated Aadhaar but limited its application to private sector authentication, recognizing the need for more robust data protection law (Singh, 2021).

4. The IT Rules, 2021 – Government Control and Censorship of Media

- Key Provisions: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 tightened state control over the internet by mandating content moderation and adherence to state instructions (Bhatia, 2020).
- Implications for Free Speech: Social media platforms and digital news portals must delete content that is considered dangerous to national security by the government, sparking censorship and press restriction issues (Mehta, 2021).
- Legal Issues: There have been a number of petitions submitted in the Supreme Court contending that the IT Rules are a violation of fundamental rights under Articles 19 and 21 of the Constitution (Saxena, 2021).

Major Legal and Ethical Issues surrounding Media Surveillance in India

The legal and ethical issues surrounding state surveillance in India center on three major issues: the justification of surveillance for national security, the scope of judicial oversight, and the threat to press freedom and democratic government.

Justifications for State Surveillance under National Security Laws

The Indian state has always justified mass surveillance programs on grounds of national security, anti-terrorism, and protection from cyber attacks. The Indian Telegraph Act of 1885 and the Information

Technology (IT) Act of 2000 provide the legal bases for interception, monitoring, and decryption of electronic communications in moments of need for state security (Basu, 2020). But these laws provide broad and expansive powers to the executive, which have generated fears of untrammelled surveillance regime and absence of legal safeguards (Chandrasekhar, 2019).

Initiatives like the Central Monitoring System (CMS) and NATGRID enable real-time monitoring of online and telephonic communications, establishing a regime of surveillance with minimal judicial scrutiny (Ganguly, 2020). While these initiatives are meant to counter cybercrimes, prevent terror plots, and facilitate intelligence coordination, they also run the risk of state overreach, political surveillance, and stifling dissent (Mehta, 2021).

The Justice K.S. Puttaswamy v. Union of India (2017) judgment which constitutionalized privacy brought judicial checks on unregulated surveillance activities. The judgment also stressed that any infringement of privacy has to meet the criteria of legality, necessity, and proportionality (Bhatia, 2020). Yet, government surveillance initiatives remain within the realm of executive discretion with no independent agency to regulate their enforcement (Singh, 2021).

Judicial Control and Absence of Regulatory Protections

Compared to Western democracies, in which the judiciary has to approve surveillance prior to implementing state surveillance, the Indian legal system enables executive departments to issue surveillance orders without review by the judiciary (Ganguly, 2020). This absence of oversight makes it challenging to identify whether state surveillance is implemented legally or politically (Chandrasekhar, 2019).

For example, the Aadhaar biometric identification program, intended initially for welfare distribution, is utilized for security monitoring with fears of bulk collection of data, citizen tracking, and privacy invasion (Mehta, 2021). Aadhaar's constitutionality was upheld by the Supreme Court but only placed conditions on its mandatory usage for private sector activities, proving the interference of the judiciary in surveillance law administration while still permitting state surveillance in some situations (Bhatia, 2020).

The absence of an independent data protection commission worsens the situation since government agencies have sweeping powers to gather and store citizens' data under the draft Personal Data Protection Bill (PDPB), 2019 (Singh, 2021). Critics contend that surveillance operations should be subjected to open legal processes, independent supervisory mechanisms, and regular judicial oversight to avoid overreach and misuse of state power (Basu, 2020).

Impacts of Surveillance Media on Democratic Rights and Press Freedom

Media surveillance conducted by the Indian state has massive implications for editorial autonomy, press freedom, and free speech safeguards. The 2021 Pegasus spyware scandal brought to light selective monitoring of journalists, dissidents, and opposition figures with the connotations of abuse of online surveillance technologies for political repression (Mehta, 2021). While the government cited national security as a justification, the lack of transparency regarding the legal basis for such actions has raised charges of state censorship and suppression of dissent (Saxena, 2021).

The IT Rules, 2021, mandating social media platforms and online news websites to adhere to government content regulation guidelines, have also evoked fears of censorship of the media and state dominance over online media (Chandrasekhar, 2019). The rules compel digital platforms to remove posts that are "against the interest of sovereignty and security of the state", a provision that can be interpreted subjectively and also to silence critical journalism (Ganguly, 2020).

Thematic Representation of Privacy vs. Security in Indian Surveillance Laws

Issue	Government Justification	Privacy and Legal Concerns
Mass Surveillance Programs (CMS, NATGRID, Pegasus, Aadhaar)	National security, cybercrime prevention	Lack of transparency, risk of political misuse
Judicial Oversight in Surveillance Approvals	Executive discretion in monitoring digital activity	No independent review process, weak accountability
Press Freedom and Digital Rights	Regulation of digital content for public safety	Potential for government censorship and self-censorship in media
Data Protection and Privacy Laws	Protection against cyber threats, national database for citizen tracking	No strong data protection authority, broad state exemptions

Comparative Analysis of Global Surveillance Laws

A comparative examination of worldwide surveillance law gives perspective to other frameworks of law to achieve equilibrium between national security and privacy in democratic regimes.

United States: The Patriot Act and Judicial Oversight of Surveillance

After the 9/11 terrorist attacks, the USA Patriot Act broadened the surveillance powers of the state by enabling law enforcement to engage in mass data collection, wiretapping, and internet monitoring (Greenwald, 2014). But after court action and grousing about civil liberties, the U.S. government instituted reforms like the USA FREEDOM Act (2015), limiting bulk data collection and increasing judicial control over surveillance orders (Basu, 2020). In contrast to India's weak judicial control over surveillance, the U.S. system involves judicial approval for the vast majority of intelligence activities (Mehta, 2021).

European Union: The GDPR and Privacy-First Digital Regulation

The European Union General Data Protection Regulation (GDPR) has stringent privacy safeguards and legal responsibility. The surveillance activities of the EU must pass the test of necessity and proportionality to ensure an assurance that the government should not be putting people under surveillance randomly without strong legal grounds (Singh, 2021). It is juxtaposed with India because the Indian surveillance law is weak, and the government officials have broad latitude in carrying out digital eavesdropping (Bhatia, 2020).

China: State-Controlled Media Spying and AI Surveillance

China has one of the most sophisticated state surveillance systems using artificial intelligence, digital censorship, and facial recognition to track the daily life of its citizens (Mehta, 2021). The Chinese state's domination of encrypted messages, online expression, and media websites is a model of mass state surveillance with minimal privacy protection (Saxena, 2021). While India's surveillance legislation is not yet on the same digital authoritarianism footing as in China, concerns are still raised that additional state surveillance would result in similar constraints on freedom of speech and freedom of the press (Basu, 2020).

Lessons from Global Surveillance Regimes for India

Comparative Analysis of Global Surveillance Frameworks

Country/Region	Key Surveillance Laws	Judicial Oversight	Privacy Protections
India	IT Act (2000), Telegraph Act (1885), PDPB (2019)	Executive discretion, weak oversight	Limited, no independent privacy regulator
United States	Patriot Act (2001), FISA	Court approval required for most surveillance requests	Some privacy protections under USA Freedom Act
European Union	GDPR, European Data Protection Directive	Strict oversight by independent privacy authorities	High, requires proportionality in data collection
China	Cybersecurity Law, Social Credit System	State-controlled, no judicial independence	Minimal, heavy government monitoring

Comparative analysis recommends that India consider taking:

- Sufficient judicial review processes to oversee surveillance authorizations.
- Independent data protection agencies to oversee government-controlled surveillance schemes.
- Transparency and accountability mandates based on the GDPR.
- Legal safeguards against selective monitoring of media outlets and journalists.

5. Summary of Findings

The research explored the media surveillance legislation in India and its effects on privacy, national security, and press freedom. The findings indicate that India's surveillance regime is run on sweeping legal mandates, where extensive state surveillance is conducted with no oversight from the judiciary. Notwithstanding the fact that the government explains surveillance as a mechanism for fighting terror, cybersecurity, and national security, concerns remain regarding the absence of legislation for averting abuse, transparency of regulations, and abuse of surveillance equipment.

The Justice K.S. Puttaswamy v. Union of India (2017) judgment had declared privacy as a fundamental right, but the government policies afterward, such as the Aadhaar-based surveillance program and the Pegasus spyware scandal, show that privacy is still being breached because of the lack of strong enforcement mechanisms. The IT Rules, 2021 also further fortified the hold of the government over digital platforms, which has raised eyebrows regarding censorship, press censorship, and media autonomy. The lack of an independent data protection authority only adds to risks of state misuse and misuses of mass surveillance.

Comparison with global benchmarks of the surveillance law in India is framing outstanding regulatory

deficits. In contrast to the United States and Europe, where constitutional protection against surveillance is established by judicial review mechanisms, India has no explicit legal provision for pre-judicial clearance of online surveillance. The European Union's GDPR model seeks to emphasize privacy-first policies and independent regulatory investigation, while the Chinese AI-based surveillance system constitutes state-controlled media surveillance with poor personal protections. India's current legal route sits between these two models, as it has wider state surveillance rights but lacks strict privacy protections.

Implications for Legal and Policy Reforms

From the findings, there are several legal and policy reforms that are needed such that the surveillance laws of India conform to constitutional protection and global standards of privacy.

1. Enhancing Judicial Scrutiny in Approvals of Surveillance: India must have a judicial review process for all the state-approved surveillance programs such that the government departments must approach the court of law for their permission to practice mass surveillance. This will check untrammelled executive power and maintain accountability.
2. Establishing an Independent Data Protection Authority**:** Lack of a separate agency for overseeing government spying leaves a lacuna in legal protection of privacy. There must be a robust Data Protection Authority (DPA) that can audit, inspect, and prosecute surveillance programs falling short of constitutional and legal standards.
3. Increasing Transparency in Government Spying Programs: Surveillance activities need to be placed under transparency reports and parliamentary monitoring. State organizations must be forced to report information regarding collection methods, justification of surveillance, and compliance with legislative demands to an independent monitoring body.
4. Saving Journalists and Press Freedom from State Surveillance**:** Legal protections need to be put in place to stop targeted monitoring of journalists, activists, and opposition figures. The Pegasus spyware scandal uncovered the absence of protections for media workers, and more robust legal provisions against politically motivated monitoring are needed.

Future Research Directions

Even though this study offers a legal and theoretical examination of media surveillance in India, future research must investigate long-term effects, new surveillance technologies, and other models of privacy protection systems.

1. Examining the Role of Artificial Intelligence under Indian Surveillance Laws: Since India is implementing AI-based surveillance technologies, facial recognition technology, and predictive policing mechanisms, future research must consider how these technologies influence privacy rights and civil liberties.
2. Evaluating the Long-Term Effect of Digital Surveillance on Democratic Government: Longitudinal research must evaluate whether India's growing use of digital surveillance contributes to more authoritarian media regulation and press control.
3. Comparing Other Legal Models for Privacy and National Security: Subsequent research must compare the manner in which other democratic countries balance surveillance statutes with privacy protection and determine best practices for India's legal model.

6. Conclusion

India's changing media surveillance system poses complicated legal, ethical, and constitutional issues. National security interests call for strong mechanisms of intelligence collection, but unchecked surveillance imperils individual freedoms, press autonomy, and democratic accountability. Security and privacy must be balanced through a legal system that respects constitutional norms while avoiding state excesses.

A reformed system of law with a focus on judicial oversight, transparency, and data protection will guarantee that national security is not achieved at the expense of constitutional rights. Fortifying privacy protections, instituting independent regulatory review, and making sure that media freedom is not restricted by online surveillance legislation are crucial steps toward a democratic and accountable surveillance system in India.

References

1. Basu, P. (2020). Privacy and the state: Understanding India’s data protection laws. Journal of Law & Policy, 14(2), 132–150.
2. Bhatia, G. (2017). The transformative Constitution: A radical biography in nine acts. HarperCollins India.
3. Bhatia, G. (2020). Digital surveillance and the Indian Constitution: Examining proportionality and necessity. Indian Journal of Constitutional Law, 18(1), 45–68.
4. Chandrasekhar, S. (2019). India’s information technology laws: A critical analysis. South Asian Law Review, 22(3), 112–135.
5. Foucault, M. (1977). Discipline and punish: The birth of the prison. Pantheon Books.
6. Ganguly, P. (2018). The Indian Telegraph Act: An outdated law in a digital world. Cyber Law Journal, 10(4), 76–89.
7. Ganguly, P. (2020). National security vs. individual freedoms: Evaluating India’s mass surveillance programs. Journal of Privacy & Security Studies, 5(1), 54–72.
8. Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Metropolitan Books.
9. Mehta, K. (2021). The Pegasus spyware controversy and its implications for press freedom in India. Indian Media Law Review, 9(2), 88–103.
10. Mill, J. S. (2015). On liberty. Yale University Press. (Original work published 1859)
11. Rawls, J. (1971). A theory of justice. Harvard University Press.
12. Rousseau, J. J. (2018). The social contract and discourses. Penguin Classics. (Original work published 1762)
13. Saxena, R. (2021). The IT Rules, 2021: A challenge to digital free speech? Law & Technology Journal, 15(3), 211–230.
14. Singh, A. (2021). National security laws and the erosion of privacy rights in India. Constitutional Review Journal, 12(2), 165–182.