
SURVEILLANCE, PRIVACY, AND HUMAN RIGHTS IN THE DIGITAL ERA: NAVIGATING CHALLENGES AND SAFEGUARDING RIGHTS IN THE INDIAN CONTEXT

E.A. Vidhyabharathi, Assistant Prof. of Law, KMC College of Law, Tirupur,
Research Scholar, The Tamilnadu Dr. Ambedkar Law University, Chennai.

ABSTRACT

The rapid expansion of India's digital public infrastructure and data-driven governance has intensified the conflict between state surveillance, national security, and individual fundamental rights. This paper examines the evolving landscape of digital surveillance in India, evaluating the legal, technological, and human rights challenges introduced by pervasive data collection and state monitoring systems. Analyzing India's regulatory framework, this study anchors its legal assessment on the Supreme Court's landmark Puttaswamy judgment—which recognized privacy as a fundamental right under Article 21 of the Constitution—and evaluates the statutory mechanisms established by the Digital Personal Data Protection (DPDP) Act, 2023. It contrasts these domestic realities with international benchmarks like the European Union's General Data Protection Regulation (GDPR) to identify regulatory gaps. The analysis reveals critical structural vulnerabilities; while the DPDP Act introduces essential principles of user consent, data minimization, and principal rights, broad state exemptions for national security and public order frequently bypass independent judicial oversight. Furthermore, rapid technological deployments—including facial recognition, predictive policing, and sophisticated spyware—outpace current legislative protections and challenge the constitutional tests of necessity and proportionality. The paper suggests that to reconcile state security imperatives with international human rights standards, India must reform its surveillance architecture by embedding independent judicial review into interception protocols, guaranteeing the absolute autonomy of the Data Protection Board of India (DPBI), mandating "privacy by design" across tech platforms, and cultivating systemic cybersecurity resilience alongside public digital literacy.

Keywords: DPDP Act 2023; Puttaswamy Judgment; Digital Surveillance; Right to Privacy; Data Protection Board of India (DPBI); Proportionality and Necessity.

1. Introduction

1.1 Background

The digital revolution has fundamentally altered how governments and corporations collect, store, and process information. In India, this transformation has brought significant benefits, including improved service delivery and enhanced national security. However, it also raises critical questions about privacy and human rights. This paper explores the intersection of surveillance, privacy, and human rights in India, providing a detailed analysis of current practices, legal frameworks, and challenges.

1.2 Objectives

The primary objectives of this paper are:

- To examine the current state of digital surveillance in India.
- To analyze the legal frameworks governing privacy and surveillance.
- To discuss landmark cases that have shaped privacy jurisprudence in India.
- To explore the balance between national security and privacy.
- To provide recommendations for strengthening privacy protections in the digital age.

2. Digital Surveillance: An Overview

2.1 Government Surveillance

Government surveillance in India has expanded significantly, driven by national security concerns and the need for efficient governance. Key government surveillance initiatives include:

2.1.1 Aadhaar

Aadhaar is the world's largest biometric identification system, collecting personal data from over a billion Indian citizens. Launched in 2009 by the Unique Identification Authority of India (UIDAI), Aadhaar aims to streamline service delivery and reduce corruption by

providing a unique identification number to residents. The system captures demographic information (name, age, address) and biometric data (fingerprints, iris scans) to ensure accuracy and prevent fraud.¹

Benefits of Aadhaar:

- **Service Delivery:** Aadhaar has facilitated the direct transfer of subsidies, pensions, and other benefits to the bank accounts of beneficiaries, reducing leakages and corruption.
- **Financial Inclusion:** The system has enabled millions of previously unbanked individuals to open bank accounts and access financial services.
- **Authentication:** Aadhaar's biometric authentication is used to verify identity in various contexts, including voting, obtaining SIM cards, and accessing government services.

Criticisms and Concerns:

- **Data Security:** The centralized database storing Aadhaar information has been criticized for being vulnerable to data breaches. There have been instances where sensitive data was leaked, raising concerns about the adequacy of security measures.
- **Privacy:** Critics argue that Aadhaar's extensive data collection infringes on privacy rights. The system's ability to track individuals' activities and link various databases poses significant risks of surveillance and misuse.²
- **Exclusion:** There have been reports of individuals being denied services due to authentication failures, leading to concerns about the exclusion of vulnerable populations.
- In 2018, the Supreme Court of India upheld the constitutional validity of Aadhaar but imposed restrictions on its use. The court ruled that Aadhaar could be mandated for welfare schemes but not for services like banking and telecommunications, emphasizing the need for data protection and privacy safeguards.³

¹ <https://uidai.gov.in/>

² <https://amlegals.com/data-privacy-in-the-context-of-aadhaar-and-indias-digital-identity-systems/>

³ Justice K.S. Puttaswamy (Retd.) v. Union of India, reported in (2019) 1 SCC 1, AIR 2018 SC 4571.

2.1.2 Central Monitoring System (CMS)

The Central Monitoring System (CMS) is an extensive surveillance program that enables government agencies to monitor and intercept digital communications in real-time. Launched in 2013 by the Department of Telecommunications (DoT), CMS aims to enhance national security and law enforcement capabilities.⁴

Features of CMS:

- **Real-time Monitoring:** CMS allows authorized government agencies to intercept and monitor phone calls, emails, and internet traffic without notifying service providers.
- **Centralized Data Collection:** The system aggregates data from various telecommunications networks, creating a centralized repository of communication records.
- **Law Enforcement:** CMS is designed to support law enforcement agencies in investigating criminal activities, terrorism, and other security threats.

Drawbacks and Disputes⁵:

- **Potential for Abuse:** The broad powers granted to government agencies under CMS have raised concerns about the potential for abuse. Without adequate oversight, there is a risk of unauthorized surveillance and violations of privacy rights.
- **Lack of Judicial Oversight:** Critics argue that CMS lacks sufficient judicial oversight, making it difficult to ensure that surveillance activities are conducted lawfully and proportionately.⁶ The absence of an independent review mechanism increases the risk of arbitrary surveillance.
- **Transparency:** The operations of CMS are shrouded in secrecy, leading to concerns about accountability. The lack of transparency makes it challenging to assess the

⁴ <https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/>

⁵ <https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about>

⁶ <https://oig.hhs.gov/reports/all/2017/cms-did-not-provide-effective-oversight-to-ensure-that-state-marketplaces-always-properly-determined-individuals-eligibility-for-qualified-health-plans-and-insurance-affordability-programs>

system's impact on privacy and civil liberties.

2.1.3 National Intelligence Grid (NATGRID)

NATGRID is a counter-terrorism initiative that integrates data from various government agencies to track individuals in real-time. Launched in 2009, NATGRID aims to prevent terrorist activities by providing comprehensive intelligence to law enforcement and intelligence agencies.⁷

Key Features of NATGRID:

- **Data Integration:** NATGRID links databases from different agencies, including banking, travel, immigration, and telecommunications, to create a unified intelligence platform.
- **Real-time Access:** Authorized agencies can access NATGRID's integrated data in real-time, enabling swift responses to potential security threats.
- **Enhanced Intelligence:** By aggregating data from diverse sources, NATGRID provides a holistic view of individuals' activities, facilitating the detection and prevention of terrorism and other serious crimes.

Limitations:

- **Privacy Infringement:** NATGRID's extensive data integration raises significant privacy concerns. The system's ability to track individuals' activities across various domains can lead to invasive surveillance and profiling.
- **Civil Liberties:** Critics argue that NATGRID's expansive surveillance capabilities pose a threat to civil liberties. The lack of clear guidelines and oversight mechanisms increases the risk of misuse and arbitrary actions by government agencies.⁸
- **Data Security:** The security of the integrated databases is a critical concern. Ensuring that sensitive information is protected from unauthorized access and breaches is

⁷ <https://www.mha.gov.in/sites/default/files/EOI.pdf>

⁸ <https://www.nextias.com/ca/current-affairs/08-01-2026/natgrid-surveillance-india>

essential to maintaining public trust.

2.1.4 Network Traffic Analysis (NETRA)

NETRA is an internet surveillance system designed to monitor and analyze online activities, including social media, emails, and instant messages. Developed by the Defence Research and Development Organisation (DRDO), NETRA aims to detect and prevent cyber threats.⁹

Key Features of NETRA:

- **Keyword Monitoring:** NETRA scans internet traffic for specific keywords and phrases associated with potential security threats, such as terrorism and cybercrime.
- **Real-time Analysis:** The system analyzes online communications in real-time, enabling prompt identification of suspicious activities.
- **Broad Surveillance:** NETRA's capabilities extend to monitoring social media platforms, emails, chat services, and other online communication channels.

Pitfalls and Protests:

- **Privacy Violations:** The broad scope of NETRA's monitoring raises significant privacy concerns. The system's ability to track online activities without individuals' knowledge or consent infringes on the right to privacy.
- **Lack of Transparency:** The operations of NETRA are not transparent, making it difficult to assess the extent of surveillance and its impact on civil liberties. The absence of public accountability mechanisms exacerbates these concerns.
- **Potential for Abuse:** The lack of clear oversight and accountability mechanisms increases the risk of abuse. Unauthorized surveillance and misuse of the system could lead to violations of privacy and civil liberties.

⁹ <https://www.wissenbaumllp.com/netra.php>

2.2 Corporate Surveillance

In addition to government surveillance, corporations in India collect vast amounts of personal data for commercial purposes. Major technology companies, such as Google, Facebook, and Amazon, track user behavior to tailor advertisements and improve services. This data collection raises concerns about consent, data security, and the potential misuse of personal information.

2.2.1 Data Collection Practices

Corporations use various methods to collect data, including cookies, tracking pixels, and mobile applications. This data is often used to create detailed profiles of individuals, which can be sold to third parties or used for targeted advertising. The lack of transparency and user control over personal data has led to growing concerns about privacy.

Common Data Collection Methods:

- **Cookies:** Small text files stored on users' devices that track their online activities and preferences. Cookies are used to personalize user experiences and deliver targeted advertisements.¹⁰
- **Tracking Pixels:** Invisible images embedded in web pages and emails that track user interactions and behaviors. Tracking pixels help companies gather data on user engagement and activity.¹¹
- **Mobile Applications:** Apps on smartphones and tablets often collect a wide range of data, including location, contacts, and usage patterns. This data is used to enhance app functionality and target advertisements.

Privacy Concerns:

- **Lack of Consent:** Many users are unaware of the extent of data collection and do not provide informed consent. The opaque nature of data collection practices makes it difficult for users to understand how their data is being used.

¹⁰ <https://www.kaspersky.com/resource-center/definitions/cookies>

¹¹ <https://www.cookiebot.com/en/pixel-tracking/>

- **Detailed Profiling:** The aggregation of data from various sources enables companies to create detailed profiles of individuals. These profiles can be used for targeted advertising and other purposes, raising concerns about privacy and manipulation.
- **Third-party Sharing:** Data collected by corporations is often shared with third parties, including advertisers and data brokers. This sharing increases the risk of unauthorized access and misuse of personal information.

2.2.2 Data Security¹²

Data breaches and unauthorized access to personal information are significant risks associated with corporate data collection. High-profile data breaches, such as the Facebook-Cambridge Analytica scandal, have highlighted the vulnerabilities in data security practices. Ensuring robust data protection measures is essential to safeguard user privacy.

Challenges in Data Security:

- **Data Breaches:** Data breaches occur when unauthorized individuals gain access to sensitive information. These breaches can result in the exposure of personal data, leading to identity theft and other harms.
- **Inadequate Security Measures:** Many companies lack adequate security measures to protect the data they collect. Weak encryption, poor access controls, and outdated software increase the risk of data breaches.
- **Insider Threats:** Employees and contractors with access to sensitive data can pose significant security risks. Insider threats include data theft, misuse, and accidental exposure of information.

Best Practices for Data Security:¹³

- **Encryption:** Encrypting sensitive data can protect it from unauthorized access. Strong encryption protocols should be used to secure data both in transit and at rest.

¹² <https://jamoroki.com/the-covenant-on-civil-and-political-rights/#Privacy>

¹³ <https://www.cnlu.ac.in/wp-content/uploads/2025/05/Safeguarding-Privacy-In-The-Digital-Era-Balancing-Rights-Security-And-Innovation-by-Ms.-Adyasha-Behera-Mr.-Bhanu-Pratap-Singh.pdf>

- **Access Controls:** Implementing strict access controls can limit who can access sensitive information. Role-based access and multi-factor authentication can enhance security.
- **Regular Audits:** Regular security audits and assessments can identify vulnerabilities and ensure that security measures are effective. Audits should be conducted by independent third parties to ensure objectivity.

2.2.3 Legal and Ethical Considerations

Corporate surveillance raises important legal and ethical questions. Companies must navigate a complex landscape of data protection laws and regulations, while also considering the ethical implications of their data practices. Balancing commercial interests with respect for user privacy is a critical challenge for corporations.

- **Data Protection Laws:** Various laws and regulations govern data protection and privacy. In India, the proposed Personal Data Protection Bill seeks to establish comprehensive data protection standards and requirements.
- **Compliance Requirements:** Companies must comply with data protection laws, including obtaining user consent, implementing security measures, and providing mechanisms for data access and correction.
- **Penalties for Non-compliance:** Non-compliance with data protection laws can result in significant penalties, including fines and reputational damage. Companies must ensure that their data practices align with legal requirements.

Ethical Considerations:

- **Informed Consent:** Ethical data practices require obtaining informed consent from users. Companies should provide clear and transparent information about data collection and usage, allowing users to make informed decisions.
- **Data Minimization:** Collecting only the data necessary for specific purposes can reduce privacy risks. Companies should avoid excessive data collection and limit the retention of personal information.

- **Transparency and Accountability:** Being transparent about data practices and holding companies accountable for their actions can build trust with users. Companies should provide clear privacy policies and mechanisms for addressing user concerns

3. Privacy Rights in the Digital Age¹⁴

Privacy is a fundamental human right, recognized by international treaties and national constitutions. In the digital age, protecting privacy presents unique challenges due to the pervasive nature of digital surveillance.

3.1 International Human Rights Frameworks

3.1.1 Universal Declaration of Human Rights (UDHR)¹⁵

The Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly in 1948, serves as a foundational document affirming the inherent dignity and equal and inalienable rights of all members of the human family. The UDHR recognizes privacy as a fundamental human right.

Article 12 of the UDHR specifically states:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Significance:

- **Global Recognition:** The inclusion of privacy in the UDHR underscores its universal importance and the obligation of states to protect this right.
- **Legal Frameworks:** Many national constitutions and legal systems have incorporated principles from the UDHR, thereby embedding privacy protections into domestic laws.
- **Human Rights Advocacy:** The UDHR provides a basis for human rights advocacy,

¹⁴ <https://www.ohchr.org/en/privacy-in-the-digital-age>

¹⁵ <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

enabling individuals and organizations to challenge violations and seek redress.

3.1.2 International Covenant on Civil and Political Rights (ICCPR)¹⁶

The International Covenant on Civil and Political Rights (ICCPR), adopted by the United Nations General Assembly in 1966, further emphasizes the right to privacy. Article 17 of the ICCPR states:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Importance and Implications:

- **Binding Treaty:** Unlike the UDHR, the ICCPR is a legally binding treaty, obligating signatory states to uphold and protect the rights enshrined within it.
- **Judicial Interpretation:** Article 17 has been the basis for numerous judicial interpretations and rulings worldwide, strengthening legal protections for privacy.
- **State Accountability:** The ICCPR provides mechanisms for monitoring and reporting on compliance, holding states accountable for violations of privacy rights.

3.2 Indian Legal Frameworks

India's legal framework for privacy protection has evolved significantly, particularly in response to the challenges posed by digital surveillance.

3.2.1 The Constitution of India

Article 21 of the Indian Constitution¹⁷ guarantees the right to life and personal liberty. The landmark case *Justice K.S. Puttaswamy v. Union of India* (2018)¹⁸ marked a significant milestone in privacy jurisprudence. The Supreme Court of India recognized the right to privacy

¹⁶ United Nations General Assembly Resolution 2200A [XXI]. International Covenant on Civil and Political Rights (1966). 1966.

¹⁷ <https://www.constitutionofindia.net/articles/article-21-protection-of-life-and-personal-liberty/>

¹⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, reported in (2019) 1 SCC 1, AIR 2018 SC 4571.

as intrinsic to the right to life and personal liberty under Article 21.

Features:

- **Constitutional Right:** The ruling elevated privacy to the status of a constitutional right, ensuring stronger legal protections against violations.
- **Judicial Precedent:** The judgment set a precedent for future cases, guiding courts in interpreting and applying privacy rights.
- **Policy Impact:** The recognition of privacy as a fundamental right influenced the development of privacy policies and legislation in India.

3.2.2 The Information Technology Act, 2000¹⁹

The Information Technology (IT) Act provides a legal framework for electronic governance and addresses issues related to cybercrime. Key provisions relevant to privacy and surveillance include:

- **Section 43A:** Mandates reasonable security practices for handling sensitive personal data. Companies and organizations must implement measures to protect personal data and prevent breaches.
- **Section 69:** Grants the government the power to intercept, monitor, and decrypt digital information under certain circumstances. This provision is intended to safeguard national security and public order.
- **Section 66E:** Penalizes the violation of privacy by capturing, publishing, or transmitting private images without consent. This provision aims to protect individuals from unauthorized use and dissemination of their personal images.

Significance and Implications:

- **Data Protection:** Section 43A encourages organizations to adopt robust data protection measures, reducing the risk of data breaches.

¹⁹ https://www.meity.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf

- **Government Surveillance:** Section 69 provides a legal basis for government surveillance but has been criticized for lacking adequate oversight and transparency.
- **Privacy Violations:** Section 66E offers recourse for individuals whose privacy has been violated, deterring misuse of personal images.

3.2.3 The Personal Data Protection Bill, 2019²⁰

The proposed Personal Data Protection (PDP) Bill aims to provide comprehensive data protection and privacy safeguards, aligning with global standards like the General Data Protection Regulation (GDPR). Key provisions include:

- **Data Processing:** Regulates the collection, storage, and processing of personal data. Organizations must adhere to principles of fairness, transparency, and accountability.
- **User Consent:** Emphasizes the need for informed and explicit consent from individuals for data processing. Users have the right to know how their data is being used and to withdraw consent.
- **Data Minimization:** Advocates for the collection of only necessary data. Organizations should limit data collection to what is required for specific purposes.
- **Data Protection Authority:** Establishes an independent authority to oversee data protection and privacy. The authority will have the power to investigate complaints, conduct audits, and impose penalties for non-compliance.

Consequence and Implication:

- **Enhanced Protections:** The PDP Bill seeks to strengthen data protection measures, providing individuals with greater control over their personal information.
- **Regulatory Oversight:** The establishment of a Data Protection Authority aims to ensure compliance with data protection laws and address violations effectively.
- **Global Alignment:** Aligning with international standards like the GDPR enhances

²⁰ https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf

India's data protection framework, facilitating cross-border data flows and fostering trust.

3.3 Challenges and Gaps

Despite the legal frameworks in place, several challenges and gaps remain in protecting privacy in the digital age.²¹

3.3.1 Enforcement and Compliance

Ensuring compliance with privacy laws and regulations is a significant challenge. Effective enforcement mechanisms and penalties for non-compliance are essential to protect privacy rights.²²

Challenges:

- **Resource Constraints:** Regulatory bodies may lack the resources and capacity to effectively monitor and enforce compliance with privacy laws.
- **Complexity of Laws:** The complexity and evolving nature of privacy laws can make it difficult for organizations to fully understand and comply with requirements.
- **Cross-border Data Flows:** The global nature of digital data flows complicates enforcement, as data may be transferred and processed across multiple jurisdictions.

3.3.2 Technological Advancements

Rapid technological advancements, such as artificial intelligence and big data analytics, pose new challenges to privacy. These technologies enable extensive data collection and analysis, often beyond the scope of existing legal frameworks.²³

²¹https://www.researchgate.net/publication/386181549_The_Challenges_of_Data_Privacy_Laws_in_the_Age_of_Big_Data_Balancing_Security_Privacy_and_Innovation

²²https://www.researchgate.net/publication/378779704_PRIVACY_LAW_CHALLENGES_IN_THE_DIGITAL_AGE_A_GLOBAL_REVIEW_OF_LEGISLATION_AND_ENFORCEMENT

²³ <https://ijirl.com/wp-content/uploads/2025/09/A-STEP-FORWARD-UNPACKING-THE-GAPS-AND-GOVERNMENT-OVERREACH-IN-THE-DIGITAL-PERSONAL-DATA-PROTECTION-ACT-2023.pdf>

Challenges:

- **Data Volume and Variety:** The sheer volume and variety of data collected by modern technologies can overwhelm existing data protection mechanisms.
- **Predictive Analytics:** Advanced analytics can infer sensitive information about individuals, raising concerns about profiling and discrimination.²⁴
- **IoT and Surveillance:** The proliferation of Internet of Things (IoT) devices increases the potential for pervasive surveillance and data collection.²⁵

3.3.3 Public Awareness

Public awareness and understanding of privacy rights and digital surveillance practices are limited. Enhancing digital literacy and educating citizens about their rights is crucial to empower individuals to protect their privacy.²⁶

Challenges:

- **Awareness Gaps:** Many individuals are unaware of their privacy rights and the extent of data collection and surveillance practices.
- **Complex Privacy Policies:** Lengthy and complex privacy policies can hinder understanding and informed consent.
- **Digital Divide:** The digital divide limits access to information and resources, affecting individuals' ability to protect their privacy.

4. Landmark Cases and Legal Precedents

Several landmark cases have shaped the legal landscape of digital surveillance and privacy in India.

1. **Justice K.S. Puttaswamy v. Union of India (2017)**²⁷: "Privacy is intrinsic to the right

²⁴ [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)

²⁵ <https://premierscience.com/pjds-24-359/>

²⁶ <https://www.ijfmr.com/papers/2026/3/77827.pdf>

²⁷ (2017) 10 SCC 1

to life and personal liberty”. In this landmark case, a nine-judge bench of the Supreme Court unanimously recognized the right to privacy as a fundamental right under the Indian Constitution. Chief Justice J.S. Khehar, delivering the judgment, emphasized that privacy is intrinsic to the right to life and personal liberty guaranteed by Article 21. The judgment highlighted the need for robust privacy protections in the digital age and called for comprehensive data protection laws. The court recommended that the Union Government examine and implement a robust regime for data protection, considering the risks posed by both state and non-state actors to privacy in an age of information.

2. **Shreya Singhal v. Union of India (2015)**²⁸: "The Supreme Court struck down Section 66A of the IT Act, which criminalized online speech". In this case, a two-judge bench of the Supreme Court struck down Section 66A of the Information Technology Act, 2000, which criminalized online speech. Justices J. Chelameswar and Rohinton F. Nariman, delivering the judgment, emphasized the importance of protecting freedom of speech and expression in the digital sphere. Justice Nariman noted that Section 66A was overly broad and could potentially restrict legitimate speech. The judgment underscored the need to balance restrictions on speech with the protection of individual liberties and highlighted the court's duty to strike down laws that violate constitutional rights.
3. **Kharak Singh v. State of Uttar Pradesh (1962)**²⁹: "The Supreme Court recognized the right to privacy in the context of police surveillance". In this foundational privacy case, a six-judge bench of the Supreme Court recognized the right to privacy as a fundamental right under Article 21. Chief Justice B.P. Sinha, leading the bench, emphasized that the right to personal liberty includes the right to be free from encroachments on one's private life. Justice K.C. Das Gupta noted that privacy is implicit in the right to life and liberty guaranteed by the Constitution. The judgment laid the groundwork for future privacy jurisprudence in India and established the principle that privacy is a core aspect of individual freedom and dignity.
4. **Navtej Singh Johar v. Union of India (2018)**³⁰: In this case concerning the decriminalization of homosexuality, a five-judge bench of the Supreme Court

²⁸ (2015) 5 SCC 1, AIR 2015 SC 1523

²⁹ 1963 AIR 1295, 1964 SCR (1) 332, AIR 1963 SUPREME COURT 1295

³⁰ AIR 2018 SC 4321 or 2018 INSC 790)

recognized the right to privacy and dignity of LGBTQ+ individuals. Chief Justice Dipak Misra, delivering the judgment, emphasized that sexual orientation is an essential attribute of privacy. The court ruled that discrimination against individuals based on sexual orientation is a violation of their dignity and self-worth. The judgment underscored the importance of recognizing and protecting the rights of marginalized communities, affirming that LGBTQ+ individuals have the same rights as other citizens to lead a dignified life and be treated equally under the law

5. **R. Rajagopal v. State of Tamil Nadu (1994)**³¹: This landmark case arose from a conflict between the right to privacy and the freedom of the press. The Supreme Court, in its judgment, recognized privacy as a fundamental right implicit in the right to life and personal liberty under Article 21 of the Constitution. The court held that individuals have the right to control the dissemination of information regarding their private lives, emphasizing the need to protect personal autonomy and dignity. This case laid the foundation for the recognition of privacy as a fundamental right in India.
6. **PUCL v. Union of India (1996)**³²: In this case, the Supreme Court addressed the issue of telephone tapping and its implications for privacy rights. The court held that telephone tapping violates the right to privacy unless it is authorized by law and is necessary in a democratic society. The court laid down detailed guidelines for lawful interception, emphasizing the importance of procedural safeguards such as the authorization of a high-ranking official and the necessity of the interception. This judgment established important safeguards to prevent arbitrary or excessive surveillance by the state.
7. **State of Maharashtra v. Bharat Shantilal Shah (2000)**³³: This case dealt with the admissibility of evidence obtained through unauthorized telephone tapping. The Supreme Court held that evidence obtained in violation of the right to privacy cannot be used in court proceedings, as it would violate the principles of fairness and justice. The court emphasized the need to protect privacy rights even in the context of law enforcement activities, highlighting the importance of upholding fundamental rights in

³¹ (1994) 6 SCC 632, AIR 1995 SC 264.

³² (1997) 1 SCC 301 (or AIR 1997 SC 568)

³³ (2008) 13 SCC 5

all circumstances.

8. **Selvi v. State of Karnataka (2010)**³⁴: In this case, the Supreme Court addressed the admissibility of evidence obtained through narcoanalysis, brain mapping, and lie detector tests. The court held that these tests violate the right against self-incrimination and the right to privacy, as they compel individuals to reveal information against their will. The court ruled that these tests cannot be conducted forcibly and must be voluntary, respecting the individual's autonomy and dignity. This judgment reaffirmed the importance of protecting fundamental rights, even in the context of criminal investigations.
9. **K.S. Puttaswamy (Retd.) v. Union of India (2019)**³⁵: Commonly known as the Aadhaar case, this landmark judgment reaffirmed the right to privacy as a fundamental right under the Constitution. The five-judge bench of the Supreme Court upheld the constitutional validity of the Aadhaar scheme, which required individuals to link their biometric information to a unique identification number, was constitutional but imposed several restrictions to protect privacy rights. Chief Justice Dipak Misra, while delivering the judgment, emphasized the importance of data protection and privacy in the digital age, highlighting the need for robust safeguards to prevent abuse of personal data. This judgment set a precedent for privacy protection in the context of digital identity systems and government surveillance programs

5. Balancing National Security and Privacy

The tension between national security and privacy is a significant challenge in the digital age. The Indian government faces the task of ensuring security without infringing on individual rights.³⁶

5.1 Legal Safeguards³⁷

Effective legal safeguards are essential to balance surveillance and privacy in India.

³⁴ AIR 2010 SUPREME COURT 1974, 2010 (7) SCC 263, 2010 AIR SCW 3011

³⁵ (2019) 1 SCC 1, AIR 2018 SC 4571

³⁶ <https://wbnujsels.wordpress.com/2025/08/05/the-ghost-of-puttaswamy-absence-of-a-real-privacy-legislation-still-haunts-india/>

³⁷ <https://techlawforum.nalsar.ac.in/digital-sovereignty-or-digital-surveillance-examining-sanchar-saathi-under-indias-dpdp-act/>

The proposed Personal Data Protection Bill aims to address these concerns by introducing checks and balances on data collection and processing. This bill is a significant step towards enhancing privacy protections, but it must be implemented effectively to achieve its objectives.

5.1.1 Proportionality and Necessity

Surveillance measures must be proportionate and necessary to achieve legitimate objectives. This principle, upheld by the Supreme Court in the Puttaswamy judgment, ensures that surveillance practices do not unduly infringe on privacy rights.³⁸ It is essential for the government to adhere to these principles to protect individual privacy while ensuring national security.

5.1.2 Judicial Oversight

Judicial oversight of surveillance activities can help prevent abuse and ensure accountability. Independent judicial review of surveillance requests can safeguard against arbitrary or excessive surveillance. However, there is a need to strengthen judicial oversight mechanisms to ensure their effectiveness.

5.1.3 Transparency and Accountability

Transparency in surveillance practices and accountability mechanisms can build public trust. The government should provide clear guidelines on data collection, storage, and use, ensuring that individuals are aware of their rights³⁹. Additionally, regular audits and reporting on surveillance activities can enhance transparency and accountability.

5.2 Technological Solutions⁴⁰

Technological solutions, such as encryption and anonymisation, can enhance privacy protections while enabling effective surveillance. The government and private sector should invest in developing and deploying technologies that protect data security and privacy. However, it is essential to ensure that these technologies are used responsibly and do not

³⁸ <https://ignited.in/index.php/jasrae/article/view/15507/30610>

³⁹ <https://forum.nls.ac.in/nlsir-online-blog/surveillance-backdoors-and-the-data-protection-regime-in-india/>

⁴⁰ <https://fiveable.me/digital-ethics-and-privacy-in-business/unit-9/balancing-security-privacy-organizations/study-guide/wg2T6LHIcXQpOnFs>

infringe on individual rights.

5.2.1 Encryption

Encryption is a powerful tool for protecting data privacy. By encrypting sensitive information, individuals and organizations can prevent unauthorized access and ensure data security. The government should promote the use of encryption technologies and provide guidelines for its implementation.⁴¹

5.2.2 Anonymization

Anonymization techniques, such as data masking and aggregation, can protect individual privacy while allowing for data analysis. By removing or obscuring personal identifiers, anonymization can mitigate privacy risks. However, it is important to ensure that anonymization techniques are effective and do not compromise the utility of the data.⁴²

5.3 International Best Practices

India can learn from international best practices in balancing national security and privacy. Countries like the United States and the European Union have implemented robust legal frameworks and oversight mechanisms to protect privacy while ensuring security. By studying these practices, India can develop its own framework that aligns with global standards and best practices.⁴³

5.3.1 General Data Protection Regulation (GDPR)⁴⁴

The GDPR, enacted by the European Union, sets high standards for data protection and privacy. It emphasizes user consent, data minimization, and accountability, providing a model for privacy legislation. India can draw inspiration from the GDPR and incorporate similar principles into its legal framework to enhance privacy protections.

By implementing these recommendations, India can strengthen its legal and regulatory

⁴¹ <https://paramountassure.com/glossary/what-is-encryption/>

⁴² <https://medium.com/@RocketMeUpCybersecurity/data-anonymization-techniques-can-we-truly-protect-user-privacy-2de7d6584831>

⁴³ https://www.researchgate.net/publication/378106122_GDPR's_impact_on_cybersecurity_A_review_focusing_on_USA_and_European_practices

⁴⁴ Ibid.

framework for privacy protection, thereby safeguarding individual rights in the digital age.

6. Recommendations for Enhancing Privacy Protections

6.1 Implementing the Legal Framework (DPDP Act, 2023)

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, establishes India's statutory framework for data privacy. The framework enforces strict obligations on data fiduciaries, mandates explicit user consent, and outlines heavy financial penalties for non-compliance. Central to this framework is the operationalization of the Data Protection Board of India (DPBI) to adjudicate grievances and enforce compliance.⁴⁵

6.1.1 Comprehensive Data Protection

The DPDP Act covers the processing of digital personal data within India, as well as offshore processing if it involves offering goods or services to individuals in India. It mandates that data fiduciaries implement technical and organizational safeguards to prevent data breaches. In the event of a personal data breach, fiduciaries are legally required to notify both the DPBI and each affected individual.⁴⁶

6.1.2 Principal Rights (User Rights)

The law shifts control back to the individual, termed the "Data Principal". It enshrines core rights, including:

- **Right to Access:** Users can request a summary of their processed data and a list of third parties shared with⁴⁷.
- **Right to Correction and Erasure:** Users can update inaccuracies or demand the deletion of data no longer necessary for its original purpose⁴⁸
- **Right to Grievance Redressal:** Users have access to readily available mechanisms to

⁴⁵ <https://authbridge.com/blog/dpdp-act-key-highlights/>

⁴⁶ <https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/>

⁴⁷ <https://secureframe.com/blog/digital-personal-data-protection-act-dpdp/>

⁴⁸ <https://securiti.ai/india-digital-personal-data-protection-bill-pdpb-2023/>

resolve complaints before escalating them to the DPBI⁴⁹.

- **Right to Nominate:** Users can appoint an individual to exercise their rights in the event of death or incapacity.⁵⁰

6.1.3 Regulatory Oversight

The Data Protection Board of India (DPBI) serves as the independent regulatory authority. The Board holds the power to investigate data breaches, summon witnesses, examine evidence, and levy financial penalties. It functions as a digital-first adjudicatory body to ensure rapid resolution of privacy disputes.⁵¹

6.2 Enhancing Cybersecurity Measures

Strengthening cybersecurity infrastructure is a prerequisite to securing personal data from unauthorized access and sophisticated cyberattacks.

6.2.1 Cybersecurity Infrastructure

Securing national and commercial data requires sustained investment in zero-trust architectures, advanced intrusion detection systems, and end-to-end encryption. Organizations must adopt a "privacy by design" approach, embedding security protocols directly into the architecture of software, apps, and cloud storage systems.⁵²

6.2.2 Incident Response

Minimizing the impact of data breaches requires rapid incident response protocols. Organizations must establish automated threat-detection mechanisms and maintain clear internal workflows for isolating compromised networks. Regular stress-testing and simulation drills ensure that IT teams can contain breaches within the mandatory reporting windows.

6.2.3 Public-Private Partnerships

Defending against systemic cyber threats requires collaboration between state agencies and

⁴⁹ <https://www.dpo-india.com/Blogs/understanding-india-dpdp/>

⁵⁰ <https://sfic.in/major-highlights-of-the-digital-personal-data-protection-bill-2023/>

⁵¹ <https://www.manageengine.com/products/eventlog/compliance/understanding-dpdp-framework.html>

⁵² <https://www.lexology.com/library/detail.aspx?g=ff727ea8-2fb8-4022-a867-a027b41ec250>

private enterprises. Public-private partnerships facilitate real-time sharing of threat intelligence through hubs like the Indian Computer Emergency Response Team (CERT-In). The government can further incentivize compliance by establishing standardized security certifications for businesses.⁵³

6.3 Promoting Digital Literacy

Educating citizens about data privacy and digital rights is crucial to building a secure digital economy.⁵⁴

6.3.1 Awareness Campaigns

National awareness campaigns must educate the public on data risks, emphasizing safe online behaviors like identifying phishing attempts and managing app permissions. These initiatives should use multilingual digital media to reach diverse demographics, including rural populations and senior citizens who are highly vulnerable to digital fraud.⁵⁵

6.3.2 Educational Programs

Integrating digital safety and privacy principles into school and university curricula equips the younger generation with critical navigation skills. Educational modules should explicitly teach the concept of digital footprints, the mechanics of online consent, and basic cybersecurity hygiene like multi-factor authentication.

6.3.3 Community Engagement

Grassroots community initiatives can foster a localized culture of privacy awareness. Workshops, local seminars, and accessible online toolkits provide citizens with practical steps to safeguard their data. These forums also allow public feedback to reach local leaders, bridging the gap between national policy and community reality⁵⁶.

⁵³ <https://www.theelephant.info/analysis/2025/03/07/safeguarding-data-rights-in-the-information-age/>

⁵⁴ https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/

⁵⁵ <https://www.amnestykenya.org/amnesty-international-kenya-launches-landmark-study-and-guidelines-on-data-protection-to-strengthen-digital-rights-and-accountability-in-kenya/>

⁵⁶ <https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140/>

6.4 Encouraging Public Participation

Developing balanced and durable privacy rules requires continuous public participation in legislative processes. The government actively seeks feedback from civil society, industry stakeholders, and tech experts through public consultation papers, draft rule reviews, and open forums. This democratic approach ensures that evolving digital policies address practical business constraints while protecting citizen rights.

7. Conclusion

In conclusion, the digital era in India presents a dual challenge and opportunity in the realms of surveillance, privacy, and human rights. While digital surveillance offers potential benefits for security and governance, it must be accompanied by robust privacy protections to safeguard individual rights. Strengthening legal frameworks, enhancing cyber security measures, promoting digital literacy, and encouraging public participation are vital steps. India can also benefit from international collaborations and adopting global best practices to address privacy concerns. Emphasizing transparency, accountability, and independent oversight in surveillance practices, along with promoting a culture of data protection and privacy awareness, is crucial. Striking a balance between security imperatives and privacy rights is paramount for India to effectively navigate the digital era while upholding fundamental human rights and democratic values.