

International Journal Research Publication Analysis

Page: 01-13

CONSTITUTIONAL PROTECTION OF DATA PRIVACY IN INDIA: A COMPARATIVE ANALYSIS WITH UNITED STATES

*Sristi Smaran

India.

Article Received: 17 September 2026

*Corresponding Author: Sristi Smaran

Article Revised: 07 October 2026

India.

Published on: 27 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.7186>

ABSTRACT

As digital technologies, artificial intelligence, social media, e-commerce, and digital governance have grown, personal data has become a valuable asset for both public and private organizations. This shift has led to concerns about surveillance, profiling, data breaches, unauthorized data use, and individuals losing control over their personal information. In India, the Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as a fundamental constitutional right and highlighted informational privacy as a key part of that right. The Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025, followed as major legislative steps. In the United States, data privacy has developed through constitutional principles, especially the Fourth Amendment, along with federal sector-specific laws and state privacy laws like California's Consumer Privacy Act.

This article uses doctrinal and comparative methods to study the constitutional bases, court decisions, and laws that shape data privacy in India and the United States. It looks at cases like Puttaswamy, Riley, and Carpenter, and compares India's proportionality test with the American reasonable-expectation-of-privacy and Fourth Amendment standards. The article argues that while India and the US use different constitutional models, both struggle to apply old privacy ideas to today's widespread digital data collection.

Keywords: Data Privacy; Article 21; Informational Privacy; Fourth Amendment; Digital Personal Data Protection Act; Puttaswamy.

KEYWORDS: Data Privacy; Informational Privacy; Article 21; Fourth Amendment; Digital Personal Data Protection Act, 2023; Comparative Constitutional Law.

INTRODUCTION

The digitization of contemporary life has fundamentally changed what privacy means and how extensive it is. People regularly share personal information when using smartphones, social media, banking apps, healthcare services, online shopping sites, and government digital platforms. Personal information is gathered, handled, analyzed, kept, and occasionally moved across different jurisdictions. Data can expose not only a person's identity but also their location, relationships, financial behavior, preferences, health details, political leanings, and behavioral tendencies. As a result, safeguarding personal data has emerged as a significant constitutional and legal issue.

The traditional understanding of privacy was primarily associated with physical spaces, correspondence, family life and freedom from arbitrary governmental intrusion. Digital technologies have expanded this concept considerably. A person's digital footprint may provide a detailed picture of their private life even when the information is technically held by third-party service providers.

The way privacy is addressed in the constitutions of India and the United States differs markedly. In India, the nine-judge bench of the Supreme Court, presided over by Justice K.S. Puttaswamy (Retd.), In the case of Union of India, privacy was unanimously recognized as a fundamental right safeguarded by the Constitution. The judgment placed privacy primarily within Article 21 and also linked it to the freedoms assured under Part III. The Court recognized multiple aspects of privacy, such as bodily privacy, decisional autonomy, and informational privacy. It also held that an invasion of privacy must meet criteria such as legality, a legitimate state objective, and proportionality.

Statement of Problem

The central problem addressed by this research is the adequacy of constitutional and statutory mechanisms for protecting individuals against the collection, processing, retention and disclosure of personal data in an increasingly digital society.

Although India has constitutionally recognised privacy as a fundamental right and enacted the DPDP Act, questions remain concerning the scope of informational privacy, governmental access to personal data, statutory exemptions, enforcement and the balance between individual privacy and legitimate State interests.

The United States presents a contrasting model. Constitutional protection is largely connected with government searches and seizures under the Fourth Amendment, while private-sector data protection is substantially dependent upon federal sectoral laws and state legislation. The

resulting comparison raises an important question: whether constitutional privacy doctrines developed before the digital age can adequately address contemporary forms of data collection and surveillance.

Research Questions

1. To what extent does the Indian constitutional framework protect informational and data privacy in comparison with the constitutional framework of the United States?
2. How do the proportionality framework developed in Puttaswamy and the Fourth Amendment jurisprudence of the United States regulate governmental access to digital information?
3. How do the Indian and American statutory frameworks address personal data held and processed by private entities?
4. What legal and constitutional challenges emerge from the comparison between the Indian and American approaches to data privacy?

Research Objectives

The objectives of this research are:

1. To examine the constitutional foundation of the right to privacy and informational privacy in India.
2. To analyse the development of digital privacy protection through Indian judicial decisions.
3. To examine the constitutional and statutory framework governing data privacy in the United States.
4. To comparatively analyse Indian and American approaches to government surveillance and private-sector data processing.
5. To identify unresolved legal challenges and possible areas for strengthening data privacy protection.

RESEARCH METHODOLOGY

The research adopts a doctrinal and comparative legal research methodology.

The doctrinal component examines primary legal materials including the Constitution of India, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the United States Constitution, judicial decisions of the Supreme Court of India and the Supreme Court of the United States, and relevant legislation.

The comparative component examines the Indian and American approaches to constitutional privacy, government surveillance, third-party data and private-sector data processing.

Secondary sources including books, academic writings, research papers, institutional reports and governmental materials are used to identify scholarly debates and existing gaps.

The research is primarily qualitative. No questionnaire or human-participant empirical research has been undertaken because the principal research questions concern constitutional doctrine and statutory interpretation.

Research Hypothesis

The study suggests that India offers a clearer constitutional basis for informational privacy via Article 21 and the Puttaswamy doctrine, while the United States depends more on Fourth Amendment case law and statutory frameworks to safeguard digital privacy. It is further hypothesized that while both jurisdictions have incorporated traditional constitutional principles into the digital realm, notable distinctions persist regarding private-sector data handling, information held by third parties, and the level of constitutional safeguards against government access to personal data.

Literature Review

The academic discourse on privacy in India changed significantly after Puttaswamy. Previous constitutional jurisprudence was marked by ambiguity regarding whether privacy qualified as a fundamental right distinct from others. The Supreme Court's nine-judge ruling settled the constitutional dispute by acknowledging privacy as fundamental to life, liberty, dignity, and autonomy. Discussions by scholars after Puttaswamy have centered on several key themes. Scholars have first looked into the connection between privacy and dignity in the context of Article 21. Second, significant focus has been placed on informational privacy and the idea of individuals having control over their personal information. Third, academic literature has explored the implications of privacy in relation to Aadhaar, surveillance, artificial intelligence, and data-driven governance.

The passage of the DPDP Act opened up an additional area for academic research. Literature has explored consent, permissible uses of personal data, duties of Data Fiduciaries, rights of Data Principals, exemptions, and the structure of the regulatory system. American literature has followed a distinct path of development. Warren and Brandeis's landmark article, "The Right to Privacy," laid an early conceptual groundwork for viewing privacy as a legal interest.

Subsequently, American legal thought evolved from a property-centered understanding toward the "reasonable expectation of privacy" standard established in Katz. Advances in

technology have spurred additional scholarly discussion. Riley acknowledged that modern mobile phones hold vast amounts of private data, while Carpenter discussed the constitutional issues arising from government access to historical cell-site location records.

Constitutional Protection of Data Privacy in India

Evolution of the Right to Privacy

The Constitution of India does not expressly use the term “privacy”. Nevertheless, the Supreme Court gradually developed privacy protections through Articles 14, 19 and 21.

In *M.P. Sharma v. Satish Chandra*, the Supreme Court considered search and seizure in the context of criminal investigation.⁹ In *Kharak Singh v. State of Uttar Pradesh*, the Court examined police surveillance and recognised concerns relating to personal liberty, although the judgment did not establish a comprehensive independent right to privacy.¹⁰

In *Gobind v. State of Madhya Pradesh*, the Supreme Court recognised privacy interests while accepting that privacy could be subject to legitimate restrictions.¹¹ Subsequently, cases such as *R. Rajagopal v. State of Tamil Nadu* and *People’s Union for Civil Liberties v. Union of India* strengthened judicial protection relating to privacy, personal information and communications.¹² The decisive development came in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.

Justice K.S. Puttaswamy v. Union of India

The nine-judge Bench in *Puttaswamy* unanimously recognised privacy as a fundamental right protected under the Constitution.

The judgment rejected the proposition that privacy could be denied constitutional status merely because it was not expressly mentioned in the constitutional text. Instead, privacy was understood as an intrinsic component of liberty, dignity and autonomy.

The judgment recognised different aspects of privacy, including:

Bodily privacy;

Informational privacy;

Decisional autonomy;

Spatial privacy; and

Protection of personal choices.

Informational privacy is particularly significant in the digital context because personal information can be aggregated to construct detailed profiles of individuals.

The Court further held that privacy is not absolute. An invasion of privacy must satisfy constitutional requirements. The Court articulated a framework involving legality, legitimate State aim and proportionality.¹³

This approach is particularly important because it establishes that State access to personal information cannot automatically be justified merely because information is technologically accessible.

Digital Personal Data Protection Act, 2023

The DPDP Act represents India's principal statutory framework for digital personal data protection.

The Act's long title expressly recognises the right of individuals to protect personal data while also recognising the need to process such data for lawful purposes.¹⁴

The statutory framework distinguishes between a Data Principal, whose personal data is processed, and a Data Fiduciary, which determines the purpose and means of processing.

The Act incorporates concepts including:

Consent;

Notice;

Lawful processing;

Reasonable security safeguards;

Personal-data breach notification;

Rights of Data Principals;

Obligations of Data Fiduciaries;

Special provisions concerning children; and

Regulatory enforcement.

The framework therefore attempts to reconcile individual control over data with legitimate data processing.

However, the Act also contains exemptions and permits certain processing without conventional consent in specified circumstances. Consequently, the constitutional proportionality standard remains significant where governmental processing interferes with fundamental privacy rights.

Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Rules, 2025 were notified in November 2025 and provide detailed implementation mechanisms under the DPDP Act. MeitY identifies the

Rules, enforcement timeline and establishment of the Data Protection Board as part of the current implementation framework.¹⁵

The Rules provide operational requirements relating to matters such as:

Notices;

Consent management;

Security safeguards;

Personal-data breach notifications;

Processing of children's data;

Obligations of Consent Managers;

Data Protection Board procedures; and

Mechanisms for exercising statutory rights.

The Rules are important because legislation containing broad principles requires detailed procedural mechanisms before individuals can effectively exercise their rights.

The current framework therefore represents an evolution from constitutional recognition of privacy towards institutional and statutory protection.

Constitutional Protection of Data Privacy in the United States

Absence of an Express General Constitutional Right

Unlike India, the United States Constitution does not expressly recognise a general fundamental right to privacy or informational privacy.

American constitutional privacy jurisprudence has developed through different constitutional provisions, particularly the Fourth Amendment.

The Fourth Amendment provides protection against unreasonable searches and seizures and requires warrants, where applicable, to satisfy constitutional requirements.

Its historical focus was strongly connected with physical spaces, property and governmental searches. Technological developments have required the Supreme Court to reconsider the application of these principles to digital information.

Katz v. United States and the Reasonable Expectation of Privacy

In *Katz v. United States*, the Supreme Court substantially expanded Fourth Amendment jurisprudence by recognising that constitutional protection is not limited to physical places.¹⁶

The case involved government interception of a telephone conversation. The Court held that the Fourth Amendment protects people rather than merely physical locations.

The resulting “reasonable expectation of privacy” framework became a central principle in American privacy jurisprudence.

However, the doctrine creates an important difficulty in the digital age. Individuals routinely provide personal information to third parties, including telecommunications companies, banks, social-media platforms and internet service providers.

This issue led to the development of the third-party doctrine.

Third-Party Doctrine

In *United States v. Miller*, the Supreme Court held that an individual did not have a Fourth Amendment privacy interest in bank records held by the bank.¹⁷

Similarly, in *Smith v. Maryland*, the Court held that the use of telephone numbers recorded by a telephone company did not constitute a Fourth Amendment search because the information had been voluntarily conveyed to the company.¹⁸

The traditional third-party doctrine therefore created a distinction between information retained personally and information voluntarily disclosed to another entity.

Digital technology, however, challenged the practical validity of this distinction because modern life requires individuals to disclose enormous quantities of information to service providers.

Riley v. California

In *Riley v. California*, the Supreme Court considered whether police could search digital information contained on a mobile phone seized during an arrest.¹⁹

The Court recognised that modern mobile phones differ fundamentally from ordinary physical objects because they can contain vast quantities of personal information.

The Court therefore held that police generally require a warrant before searching digital information on a mobile phone seized from an arrested person.

Riley is significant because it demonstrates the Supreme Court’s willingness to adapt Fourth Amendment doctrine to technological realities.

It also illustrates a fundamental principle of contemporary digital privacy law: the quantity and qualitative nature of information contained in a technological device can alter the constitutional analysis.

Private-Sector Data Privacy in the United States

A major distinction between India and the United States concerns private-sector regulation.

The US constitutional framework principally regulates government action. Constitutional Fourth Amendment protection therefore does not automatically create a comprehensive set of rights against every private company that collects personal data.

Private-sector privacy is instead regulated through a combination of federal statutes, sectorspecific legislation, consumer-protection law and state privacy laws.

Examples of federal sectoral regulation include:

The Health Insurance Portability and Accountability Act (HIPAA);

The Gramm-Leach-Bliley Act (GLBA);

The Children's Online Privacy Protection Act (COPPA); and The Fair Credit Reporting Act (FCRA).

This produces a more fragmented regulatory structure than the Indian DPDP framework.

Comparative Analysis: India and the United States

Constitutional Foundation

The first major difference concerns constitutional foundations.

India recognises privacy as a fundamental right through constitutional interpretation, particularly Article 21. Puttaswamy provides a broad conception encompassing informational privacy, dignity and autonomy.

The United States has no equivalent express constitutional right to data privacy. Protection arises primarily through constitutional provisions such as the Fourth Amendment and judicial doctrines.

Consequently, the Indian constitutional model is more directly oriented towards privacy as an aspect of individual liberty and dignity, whereas the American constitutional model has historically developed around protection against unreasonable government searches and seizures.

Government Surveillance

The two systems nevertheless share an important feature: governmental interference with privacy is subject to constitutional limitations.

India applies the legality-legitimate aim-proportionality framework established in Puttaswamy.²³

The United States applies Fourth Amendment principles, including the reasonable-expectationofprivacy doctrine and warrant requirements.

Carpenter demonstrates the American judiciary's willingness to modify traditional doctrine where technological data creates an unusually detailed record of individual life.

The difference lies principally in doctrinal formulation. India's approach begins with a broadly recognised fundamental right to privacy and asks whether interference satisfies constitutional requirements. The American approach generally asks whether particular government conduct constitutes a search or seizure protected by the Fourth Amendment and whether that conduct is reasonable.

Third-Party Data

Third-party data presents a particularly important comparative issue.

Traditional US doctrine suggested that information voluntarily disclosed to a third party could lose Fourth Amendment protection. Miller and Smith illustrate this approach.

However, Carpenter demonstrates a more technologically sensitive approach. Historical location information was treated differently because of the comprehensive nature of the information that could be derived from it.

Indian privacy doctrine does not depend upon exactly the same third-party doctrine. The constitutional recognition of informational privacy focuses more broadly on the individual's interest in personal information and the legitimacy and proportionality of State interference.

Private Companies

The regulatory position is substantially different.

India's DPDP Act establishes a national statutory framework governing digital personal data processing by Data Fiduciaries, subject to the Act's scope and exemptions.

The United States lacks a single comprehensive federal law governing all private-sector personal data. Instead, federal sectoral statutes coexist with state laws.

California's CCPA provides a broader model of consumer rights, including rights of access, deletion, correction and opting out of sale or sharing.²⁴

Therefore, a person in India may approach data protection primarily through the national DPDP framework, whereas the applicable US protection may depend substantially upon the type of data, industry, entity involved and state in which the person is protected.

FINDINGS

The comparative study produces several findings.

First, India and the United States recognise privacy through substantially different constitutional routes. India's approach is founded on the constitutional status of privacy as a

fundamental right, whereas US constitutional protection is principally developed through the Fourth Amendment.

Second, Puttaswamy has significantly strengthened the constitutional status of informational privacy in India. Its legality, legitimate-aim and proportionality framework provides a constitutional basis for reviewing State interference with personal data.

Third, US jurisprudence demonstrates an incremental technological adaptation of existing constitutional doctrine. Riley recognised the unique quantity of information contained in smartphones, while Carpenter limited the traditional implications of the third-party doctrine for historical location information.

Fourth, India and the United States differ substantially in private-sector regulation. India has adopted a national statutory framework through the DPDP Act, whereas the United States combines federal sectoral laws with state-level privacy legislation.

Fifth, California's CCPA demonstrates that comprehensive private-sector privacy rights can develop within the American federal system even in the absence of a general federal privacy statute.

Finally, both jurisdictions face similar technological challenges despite their doctrinal differences. Data aggregation, artificial intelligence, mass surveillance, location tracking and private-sector profiling require privacy principles to remain technologically adaptable.

CONCLUSION

Protecting data privacy constitutionally has grown more critical as personal information now plays a central role in modern social, economic, and governmental functions. India's constitutional framework experienced a pivotal shift as a result of the case Justice K.S. Puttaswamy v. Union of India. By treating privacy as a fundamental right and viewing informational privacy as one of its key aspects, the Supreme Court established a constitutional basis for safeguarding personal data. The passage of the DPDP Act, 2023, and the issuance of the DPDP Rules, 2025, mark the transition from constitutional principles to statutory implementation. The present framework aims to balance individual data protection with the lawful processing of personal data.

The American approach has followed a different trajectory. Rather than recognising a general constitutional right to informational privacy, the US Supreme Court has developed protection through constitutional doctrines, particularly the Fourth Amendment. Katz shifted attention towards reasonable expectations of privacy, while Riley recognised the extraordinary quantity of personal information contained in mobile phones. Carpenter further demonstrated

that digital information held by third parties may attract constitutional protection when it provides an extensive record of a person's movements.

The comparison demonstrates that constitutional data privacy cannot be understood solely through traditional notions of physical privacy. Digital technology has changed the nature of personal information and the scale at which it can be collected and analysed.

Bibliography

A. Primary Sources — India

1. Constitution of India.
2. Digital Personal Data Protection Act, 2023.
3. Digital Personal Data Protection Rules, 2025.
4. Information Technology Act, 2000.
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1.
7. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
8. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
9. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
10. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
11. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
12. District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496.

B. Primary Sources — United States 1. Constitution of the United States, Fourth Amendment.

13. Katz v. United States, 389 U.S. 347 (1967).
14. United States v. Miller, 425 U.S. 435 (1976).
15. Smith v. Maryland, 442 U.S. 735 (1979).
16. United States v. Jones, 565 U.S. 400 (2012).
17. Riley v. California, 573 U.S. 373 (2014).
18. Carpenter v. United States, 585 U.S. 296 (2018).
19. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.
20. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.
21. Health Insurance Portability and Accountability Act.
22. Gramm-Leach-Bliley Act. 12. Fair Credit Reporting Act.

C. Books and Academic Literature

23. M.P. Jain, Indian Constitutional Law, LexisNexis.

24. H.M. Seervai, Constitutional Law of India, Universal Law Publishing.
25. V.N. Shukla, Constitution of India, Eastern Book Company.
26. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
27. Daniel J. Solove, Understanding Privacy, Harvard University Press.
28. Daniel J. Solove & Paul M. Schwartz, Information Privacy Law, Wolters Kluwer.
29. Alan F. Westin, Privacy and Freedom, Atheneum.
- D. Government and Institutional Materials
30. Ministry of Electronics and Information Technology, Government of India, materials concerning the Digital Personal Data Protection Act and Rules.
31. India Code, Digital Personal Data Protection Act, 2023.
32. Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025.
33. California Department of Justice, California Consumer Privacy Act materials.
34. Supreme Court of the United States, opinions in Riley and Carpenter.