

International Journal Research Publication Analysis

Page: 01-05

THE RIGHT TO PRIVACY IN THE DIGITAL AGE: A CONSTITUTIONAL AND HUMAN RIGHTS ANALYSIS

***Sheetal Yadav**

LL.B. Student, Haveli Institute of Legal Student and Research.

Article Received: 13 August 2026

*Corresponding Author: Sheetal Yadav

Article Revised: 03 September 2026

LL.B. Student, Haveli Institute of Legal Student and Research.

Published on: 23 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.2319>

ABSTRACT

The right to privacy has undergone a profound transformation since its early conception as ‘the right to be let alone.’ In an era of pervasive digital surveillance, algorithmic profiling, and mass data collection, courts and legislatures worldwide have been compelled to re-examine what privacy means as a constitutional and human right. This article traces the doctrinal evolution of privacy from a common-law tort to a recognised fundamental right, examines how leading constitutional courts and human rights instruments have responded to digital-age challenges, and considers the adequacy of existing legal frameworks in balancing individual autonomy against state and corporate interests in data. It argues that while judicial recognition of informational privacy has advanced significantly, meaningful protection now depends less on declaring the right and more on building enforceable, technology-responsive mechanisms to give it effect.

KEYWORDS: Right To Privacy, Data Protection, Constitutional Law, Human Rights, Surveillance, Informational Autonomy.

I. INTRODUCTION

Privacy was once understood primarily as a spatial concept — protection of the home, correspondence, and the body from unwarranted intrusion. The digital age has dissolved those spatial boundaries. A person's location history, browsing habits, biometric data, financial transactions, and social relationships are now continuously recorded, aggregated, and analysed, often without meaningful awareness or consent. This shift has forced constitutional courts to move from protecting privacy as a narrow liberty against physical

intrusion to recognising it as a broader right of informational self-determination: the ability of an individual to control how personal data about them is collected, used, and shared.

This article proceeds in four parts. Part II traces the doctrinal history of privacy as a legal right. Part III examines how major jurisdictions and international human rights instruments have constitutionalised privacy in response to digital-age pressures. Part IV identifies the central tensions the law must now resolve — state surveillance, corporate data practices, and the challenge of artificial intelligence. Part V offers concluding observations on the direction the law should take.

II. From Tort to Fundamental Right: A Doctrinal History

The modern legal concept of privacy is often traced to the 1890 Harvard Law Review article by Samuel Warren and Louis Brandeis, which argued for a common-law right against unwarranted publication of private facts, describing privacy as the right ‘to be let alone.’ For much of the twentieth century, privacy remained largely a tort-law concept in common-law jurisdictions, protecting against specific intrusions such as unauthorised publication or trespass, rather than a freestanding constitutional guarantee.

The constitutionalisation of privacy accelerated in the latter half of the twentieth century. In the United States, the Supreme Court read a right to privacy into the ‘penumbras’ of the Bill of Rights in *Griswold v. Connecticut* (1965), later extending it to reproductive autonomy in *Roe v. Wade* (1973). The European Convention on Human Rights took a more direct approach: Article 8 expressly guarantees the right to respect for private and family life, home, and correspondence, subject to narrowly defined exceptions. India's Supreme Court, in *Justice K.S. Puttaswamy v. Union of India* (2017), unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 of the Constitution, explicitly recognising informational privacy as a distinct facet of the right. What unites these developments is a common trajectory: privacy moved from a residual protection against specific harms to a recognised precondition for individual dignity and autonomy.

III. Constitutional and Human Rights Responses to the Digital Age

A. Informational Privacy as a Distinct Right

Digital technology exposed a gap in classical privacy doctrine: harms no longer arise only from physical intrusion or defamatory publication but from the silent aggregation of data points that, individually, seem innocuous. A single purchase record reveals little; a decade of purchase records, browsing history, and location data, cross-referenced, can reveal health

conditions, political views, and relationships the individual never chose to disclose. Courts have increasingly recognised that this aggregation itself constitutes a distinct privacy harm. The Puttaswamy judgment explicitly identified informational privacy as one of several distinct zones of the right, alongside bodily and decisional privacy, and directed the state to put in place a robust data protection framework — a directive that led to India's Digital Personal Data Protection Act.

B. The European Model: Data Protection as a Codified Right

The European Union has gone furthest in translating constitutional privacy principles into detailed statutory obligations. The General Data Protection Regulation (GDPR) operationalises Article 8 of the EU Charter of Fundamental Rights by imposing obligations of lawfulness, purpose limitation, data minimisation, and accountability on any entity processing personal data, and by granting individuals enforceable rights of access, correction, and erasure. The Court of Justice of the European Union has reinforced this framework through decisions such as *Google Spain* (2014), which recognised a qualified 'right to be forgotten,' and *Schrems* (2015 and 2020), which struck down transatlantic data-transfer arrangements found not to guarantee EU-equivalent protection. The European approach illustrates a broader lesson: a constitutional right to privacy, without a statutory and regulatory apparatus to enforce it against both state and private actors, risks remaining largely aspirational.

C. State Surveillance and Constitutional Limits

Mass surveillance programmes have tested the limits of privacy doctrine most directly. Revelations of bulk data collection by intelligence agencies prompted litigation and legislative reform across multiple jurisdictions, with courts increasingly requiring that surveillance be authorised by law, pursue a legitimate and clearly defined aim, and be proportionate to that aim — the same structure of justification found in Article 8(2) of the European Convention and adopted by the Indian Supreme Court in *Puttaswamy* through its own three-part test of legality, legitimate aim, and proportionality. The consistent judicial insistence on proportionality reflects a recognition that the mere existence of a legitimate security interest cannot, by itself, justify indiscriminate data collection.

IV. Unresolved Tensions

A. Consent in an Asymmetric Digital Marketplace

Data protection frameworks generally rely on individual consent as the primary legitimising mechanism for data processing. In practice, consent obtained through lengthy terms-of-service agreements, take-it-or-leave-it platform access, and deliberately complex privacy settings does little to reflect genuine, informed choice. This gap between formal consent and substantive autonomy remains one of the most significant unresolved problems in privacy law, and has led some scholars and regulators to argue for shifting the burden onto data controllers through default privacy-protective design rather than relying on user-initiated opt-outs.

B. Artificial Intelligence and Algorithmic Profiling

Automated decision-making systems that determine creditworthiness, employment suitability, or insurance risk from personal data raise privacy concerns that existing doctrine addresses only imperfectly. Such systems can produce discriminatory or opaque outcomes without any single identifiable act of unauthorised disclosure, meaning traditional privacy remedies — built around unauthorised access or publication — are not well suited to the harm. Regulatory responses such as the GDPR's limited right to human review of automated decisions, and the EU's more recent Artificial Intelligence Act, represent early attempts to extend privacy-adjacent protections into this space, but the doctrinal fit between classical privacy rights and algorithmic harm remains unsettled.

C. Horizontal Application Against Private Actors

Constitutional privacy rights were historically conceived as protections against the state. The dominant threat to informational privacy today, however, comes at least as much from private corporations that collect and monetise personal data. Jurisdictions differ in how far constitutional rights apply horizontally, between private parties, as opposed to only vertically, against the state. Where constitutions do not extend privacy obligations to private actors directly, statutory data protection law becomes the primary — and in many jurisdictions the only — mechanism through which individuals can assert control over their data against corporate processors.

V. CONCLUSION

The constitutional recognition of privacy as a fundamental right has kept pace, in doctrinal terms, with the challenges posed by the digital age: courts in multiple jurisdictions have

extended privacy protection to cover informational autonomy, required proportionality in state surveillance, and, in some cases, obliged legislatures to enact comprehensive data protection statutes. What remains incomplete is the translation of that doctrine into mechanisms capable of addressing the realities of an asymmetric digital marketplace, opaque algorithmic decision-making, and privacy harms caused primarily by private rather than state actors. The next stage in the development of privacy as a human right will likely be measured less by further declarations of its constitutional status, which is now well established in most major jurisdictions, and more by the practical adequacy of the statutory and regulatory frameworks built to enforce it.

REFERENCES (SELECT)

1. Warren, S. and Brandeis, L., 'The Right to Privacy' (1890) 4 Harvard Law Review 193
2. Griswold v. Connecticut, 381 U.S. 479 (1965)
3. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
4. European Convention on Human Rights, Article 8
5. Charter of Fundamental Rights of the European Union, Article 8
6. Regulation (EU) 2016/679 (General Data Protection Regulation)
7. Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12 (2014)
8. Schrems v. Data Protection Commissioner, Case C-362/14 (2015) and Case C-311/18 (2020)