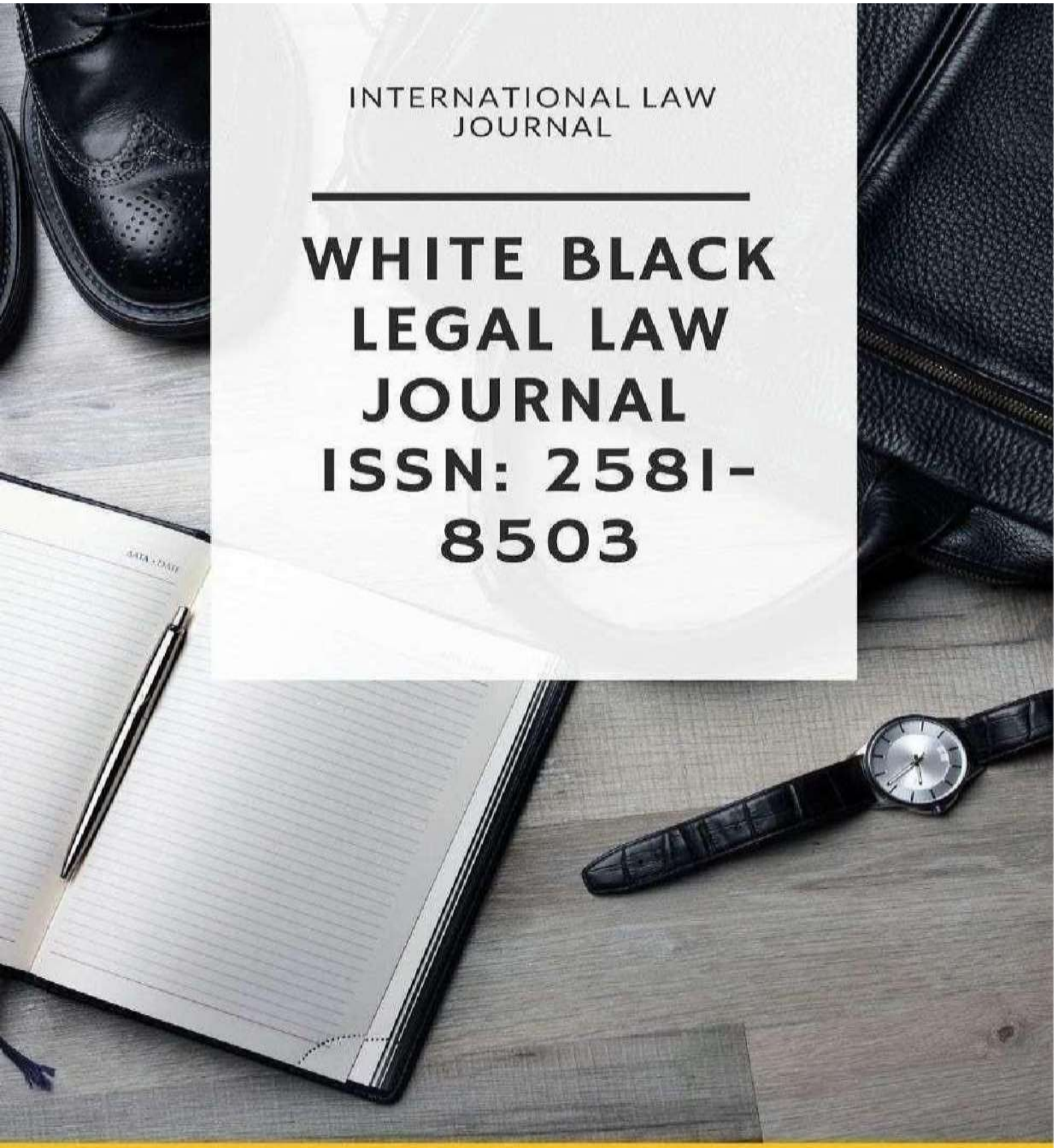

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

RIGHT TO PRIVACY IN THE DIGITAL AGE: AN INDIAN LEGAL PERSPECTIVE

AUTHORED BY - ARUL KUMAR & DR ROSHNI SRIVASTAVA
(LL.B.), Amity University, Lucknow.

Abstract

The right to privacy, long regarded as a cornerstone of individual liberty, has acquired an entirely new dimension in the wake of rapid digitisation. In India, the recognition of privacy as a fundamental right under Article 21 of the Constitution — firmly settled by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) — marked a historic inflection point. Yet that recognition alone does not resolve the deeply complex tensions arising from the pervasive surveillance infrastructure of the modern state, the data-hungry business models of technology corporations, and the evolving expectations of a billion-strong digitally connected population. This paper critically examines the constitutional foundations of the right to privacy in India, traces its judicial evolution, analyses the legislative response through the Digital Personal Data Protection Act, 2023, and interrogates the gaps that remain unaddressed. It argues that while India has taken commendable steps, genuine privacy protection in the digital age demands not merely formal legal recognition but a robust, independent, and enforceable framework that places the citizen — not the state or the corporation — at its centre.

Keywords: *Right to Privacy, Article 21, Puttaswamy Judgment, Digital Personal Data Protection Act, Surveillance, Informational Autonomy, Data Fiduciary, Aadhaar.*

I. Introduction

There is something quietly unsettling about living in an age where one's morning commute is tracked by a mobile application, one's purchasing habits are aggregated by an e-commerce algorithm, one's face is recognised by a surveillance camera at a railway station, and one's political opinions are inferred from social media activity — all before noon. Privacy, once a matter primarily of physical space and personal correspondence, now encompasses the entirety of one's digital existence. Every click, every search query, every biometric entry leaves a trace. And these traces, individually innocuous, collectively amount to a portrait of the individual more detailed than any government dossier in human history could ever have been.

India's engagement with privacy as a legal right has been long and, for much of its history, ambivalent. For decades following independence, the Supreme Court oscillated between recognising privacy as an implicit fundamental right and treating it as a mere common-law entitlement. The matter was not definitively resolved until 2017, when a nine-judge Constitutional Bench, in one of the most consequential decisions in Indian constitutional history, held unanimously that the right to privacy is indeed a fundamental right protected under Article 21 and the broader scheme of Part III of the Constitution. This recognition, though belated, was unequivocal and transformative.

Yet recognition is the beginning, not the end, of the conversation. The digital age presents challenges to privacy that the framers of the Constitution could not have anticipated and that the judiciary, however learned, cannot resolve through adjudication alone. It calls for legislative imagination, regulatory rigour, and a cultural shift in how India — its government, its corporations, and its citizens — understands the value of personal information. This paper attempts to map that conversation as it stands today.

II. Constitutional Foundations: Privacy as a Fundamental Right

The story of privacy in Indian constitutional law is, in many ways, a story of judicial hesitation followed by eventual conviction. In M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of U.P. (1962), the Supreme Court, then composed of eight and six judges respectively, either denied the existence of a constitutional right to privacy or gave it only the narrowest recognition. These decisions cast a long shadow, and it was only in later cases — most notably Gobind v. State of Madhya Pradesh (1975) and R. Rajagopal v. State of Tamil Nadu (1994) — that the Court began to accept privacy as an implicit facet of the liberty guaranteed by Article 21.

The definitive moment came with Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), popularly known as the Aadhaar Privacy Case. The challenge arose in the context of the Aadhaar biometric identification project, with the petitioners contending that the compulsory collection of biometric data violated their right to privacy. The nine-judge Bench, while leaving the specific validity of Aadhaar to be decided separately, addressed the foundational question and held unanimously that privacy is a constitutionally protected right. The Bench produced six separate opinions, each rich in reasoning and philosophical depth, but all converging on the same conclusion: that privacy inheres in every individual as an aspect of personal liberty under Article 21, and as a necessary condition for the exercise of other fundamental rights.

Justice D.Y. Chandrachud, writing for himself and three others, articulated perhaps the most expansive vision of privacy in the judgment. He described informational privacy — the right to control the flow of information about oneself — as a distinct and vital dimension of the right, recognising that in the digital age, data is not a neutral by-product of activity but a resource of immense power. He also acknowledged that privacy is not absolute; it may be restricted by the state on grounds of legitimate aim, rational nexus, and proportionality. This three-pronged test, borrowed from European jurisprudence, has become the touchstone for evaluating privacy intrusions in subsequent cases.

III. The Digital Surveillance Problem

India's digital landscape is staggering in its scale. With over 900 million internet users, the second-largest base in the world, the country generates an enormous volume of personal data every day. This data flows through a complex web of government systems, private platforms, and cross-border transfers, each segment presenting its own privacy vulnerabilities. The Aadhaar database alone stores biometric information — fingerprints and iris scans — of over a billion citizens, making it arguably the largest civilian biometric database in the world. The implications for surveillance, should the data be misused or breached, are profound.

The Indian state's appetite for surveillance has grown in parallel with its digital ambitions. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, permit the interception of electronic communications by a wide range of government agencies, with limited judicial oversight. Unlike several democracies where surveillance warrants require prior judicial authorisation, Indian law places this power primarily in the hands of the executive. The absence of an independent oversight mechanism — a dedicated surveillance tribunal, for instance — has long been a lacuna in the legal framework, and it remains unaddressed.

The problem is not confined to state actors. Private corporations — social media platforms, e-commerce companies, fintech applications, and health-tech startups — collect personal data on a scale that was inconceivable even a decade ago. Much of this collection occurs without meaningful informed consent. The average Indian user, presented with a lengthy privacy policy in dense legalese as a precondition for accessing a service, has no practical choice but to click 'agree'. Consent in such circumstances is a legal fiction, not a genuine exercise of autonomy. The European Union's General Data Protection Regulation (GDPR) tackled this problem by requiring that consent be specific, informed, freely given, and unambiguous — standards that India has been slow to adopt.

IV. The Digital Personal Data Protection Act, 2023: Promise and Limitations

India's first dedicated personal data protection legislation, the Digital Personal Data Protection Act, 2023 (DPDPA), was a long time coming. It arrived after nearly a decade of consultations, draft iterations — including the Personal Data Protection Bill, 2018, and its successor, the Data Protection Bill, 2021 — and considerable public debate. The eventual legislation, though leaner than its predecessors, introduced important concepts into Indian law: the classification of entities as data fiduciaries (those who determine the purpose and means of processing) and data processors, the obligation to give individuals notice and obtain their consent before processing personal data, the rights of data principals to access information, seek correction, and demand erasure, and the establishment of a Data Protection Board to adjudicate complaints.

In terms of structural architecture, the DPDPA represents genuine progress. For the first time, Indian law explicitly acknowledges that personal data belongs to the individual and that its processing imposes duties on those who handle it. The consent framework, while not as stringent as the GDPR, is a substantial improvement over the earlier IT Act regime, where data protection was an afterthought tucked into secondary rules. The Act also introduces meaningful children's data protections, prohibiting targeted advertising directed at minors and requiring verifiable parental consent for processing the personal data of anyone under eighteen.

Yet the DPDPA has attracted sustained criticism, and not without reason. The most significant concern is the breadth of exemptions granted to the central government. Section 17 of the Act empowers the government to exempt any agency from the operation of the entire legislation in the interest of national security, public order, or the sovereignty of India. Critics, including several members of civil society and the dissenting voices in the parliamentary committee, have argued that this provision essentially hollows out the statute: a data protection law that can be suspended at will by the very entity whose conduct most needs to be constrained offers incomplete protection.

A second concern relates to the independence of the Data Protection Board. Under the Act, members of the Board are appointed by the central government, without any consultative mechanism involving the judiciary or an independent commission. This creates an obvious tension: the Board is asked to adjudicate complaints against government agencies while being itself constituted by the government. Structural independence — so essential to the credibility of any regulatory body — is difficult to claim under such an arrangement. By contrast, many democratic jurisdictions vest data protection oversight in independent constitutional authorities with security of tenure and insulation from executive pressure.

V. Privacy, Autonomy, and the Citizen-State Relationship

It is tempting to view the right to privacy in purely technical terms — as a matter of data flows, consent architectures, and regulatory compliance. But to do so would be to miss its deeper significance. Privacy is, at its heart, about power. It is about the capacity of the individual to define herself on her own terms, to form and hold opinions without interference, to make choices about her body, her relationships, her beliefs, and her identity without these being catalogued and potentially weaponised by those who hold power over her. When privacy erodes, so does the space for dissent, for difference, and for the exercise of every other right that a democratic constitution guarantees.

The chilling effect of surveillance on free expression is well-documented. When individuals know, or even suspect, that their communications are being monitored, they self-censor. They avoid visiting certain websites, they hesitate before expressing unpopular opinions, they conform. This is not merely a theoretical concern in India. Activists, journalists, lawyers, and political dissenters have repeatedly reported being subjected to digital surveillance, including through the use of sophisticated commercial spyware such as Pegasus. The Supreme Court took cognisance of these allegations in 2021 and appointed a technical committee to investigate. The right to privacy, in this context, is not a luxurious civil liberty of the elite — it is the oxygen of democratic participation.

There is also a dimension of social privacy that Indian law has only recently begun to grapple with. The right of individuals to control sensitive information — about their caste, religion, health status, sexual orientation, or mental health — is particularly fraught in a society where discrimination on these grounds, while legally prohibited, remains pervasive in practice. A data breach exposing the HIV status of a patient, or the sexual orientation of an employee, can destroy livelihoods and rupture families. The DPDPA's category of 'sensitive personal data', while acknowledging this concern, does not yet create a sufficiently differentiated protective regime for it.

VI. Comparative Perspectives and the Path Forward

India's legislative journey has unfolded against a rich backdrop of international developments. The GDPR, which came into force in the European Union in 2018, has served as a global benchmark, introducing the principles of data minimisation, purpose limitation, storage limitation, and accountability as binding legal obligations. More recently, the EU's AI Act has begun to extend similar principles to automated decision-making, recognising that privacy concerns in the digital age are not limited to data storage but extend to algorithmic inference

and profiling. The United States, by contrast, still lacks a comprehensive federal data protection law, relying instead on a sectoral patchwork — though several states, led by California, have moved ahead with their own frameworks.

For India, the path forward requires action on several fronts simultaneously. First, the surveillance law framework demands urgent reform. The establishment of a judicial authorisation requirement for electronic surveillance, modelled on the warrant requirement in criminal procedure, would bring India into conformity with both its constitutional commitments under Puttaswamy and its international human rights obligations. The Supreme Court has repeatedly observed that the absence of such a framework is constitutionally suspect, and the legislature must respond. Second, the Data Protection Board must be reconstituted as a genuinely independent body, with members drawn from diverse backgrounds — law, technology, civil society — and protected from executive interference.

Third, digital literacy must be recognised as a prerequisite for meaningful privacy. A consent framework, however carefully designed, offers little protection to a user who cannot read the language in which a privacy policy is written, does not understand what 'processing' or 'profiling' means, and has no practical alternative to the platform demanding her data. Investment in public digital education, combined with plain-language disclosure requirements for all data fiduciaries, would help bridge this gap. Fourth, cross-border data flows — a particularly sensitive issue given India's large technology services industry — must be governed by a framework that balances economic interests with genuine privacy protection, rather than treating privacy as an obstacle to be minimised.

VII. Conclusion

The right to privacy in the digital age is not a static legal category; it is a living, contested terrain where the interests of the state, the corporation, and the individual meet — and frequently collide. India, with its extraordinary diversity, its billion-plus population navigating rapid digitalisation, and its democratic traditions anchored in constitutional liberalism, has both the greatest need for strong privacy protection and some of the most complex challenges in achieving it.

The Puttaswamy judgment gave India the constitutional foundation it needed. The DPDPA, for all its limitations, represents the first serious legislative attempt to build upon that foundation. But a foundation is not an edifice. What India needs now is the political will to construct — brick by careful brick — a privacy architecture that is independent, enforceable, and genuinely protective of the individual. Privacy is not a luxury that developing nations can afford to defer.

It is, as the nine judges of the Supreme Court recognised in 2017, an intrinsic part of human dignity, inseparable from what it means to live as a free person in a free society.

As India continues to expand its digital infrastructure — from the Aadhaar ecosystem and the Unified Payments Interface to the proposed Digital India Act — the choices made now will shape the relationship between citizen and state for generations. The question is not whether India can afford to take privacy seriously. It is whether India can afford not to.

References

Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

M.P. Sharma v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300.

Kharak Singh v. State of U.P., AIR 1963 SC 1295.

Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 [Aadhaar Five-Judge Bench].

The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

The Information Technology Act, 2000, No. 21 of 2000 (India).

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 27 April 2016.

Justice B.N. Srikrishna Committee Report, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (2018), Ministry of Electronics and Information Technology, Government of India.

Mandhata Kanwar & Shreya Tripathy, 'Privacy as a Fundamental Right: The Road from Gobind to Puttaswamy' (2018) 30 National Law School of India Review 1.

Vrinda Bhandari & Ujwala Uppaluri, 'India's Privacy Moment: Realising the Promise of Puttaswamy' (2018) 3(2) Indian Law Review 144.

Usha Ramanathan, 'A Unique Identity Bill' (2010) Economic and Political Weekly, Vol. 45, No. 30.

Sujit Choudhry (ed.), The Migration of Constitutional Ideas (Cambridge University Press, 2006).