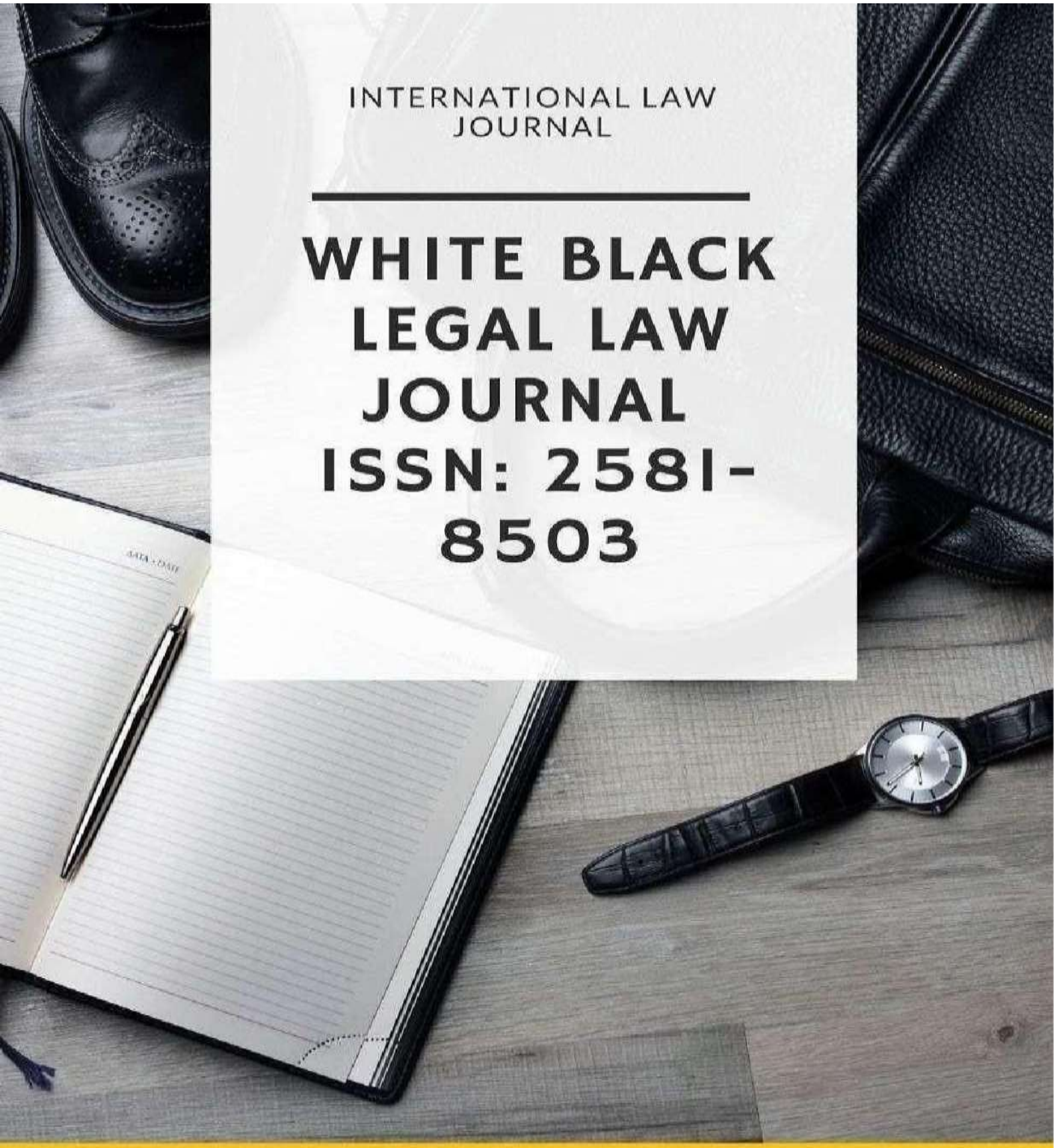

INTERNATIONAL LAW JOURNAL

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.

BRIDGING THE GAP BETWEEN DIGITAL PRIVACY RIGHTS AND CORPORATE DATA PRACTICE ANALYSIS

AUTHORED BY - A.V.THIRU KAARTHEKEYAN [1] & A.MAGESH KUMAR [2]

ABSTRACT

The rapid evolution of digital technologies has fundamentally reshaped modern society, transforming how individuals communicate, access information, and participate in economic activities. In this data-driven era, personal information has emerged as a critical asset, often described as the "new oil" powering innovation and business growth.

Corporations, particularly in the technology and digital services sectors, rely heavily on the collection, analysis, and monetization of user data to enhance operational efficiency, personalize services, and maintain competitive advantage.

However, this increasing dependence on data has raised profound concerns regarding the protection of digital privacy rights and the ethical implications of corporate data practices.

Digital privacy refers to an individual's right to control the collection, use, storage, and dissemination of their personal information. Over the past decade, governments and regulatory bodies across the world have introduced legal frameworks and policies designed to safeguard these rights, emphasizing principles such as informed consent, transparency, data minimization, and accountability. Despite these regulatory advancements, there remains a persistent and widening gap between the intended protections offered by digital privacy laws and the actual practices adopted by corporations.

1. **Author - A.V.THIRU KAARTHEKEYAN, Reg No. 21142132, B.Com., LL.B(Hons) VELS SCHOOL OF LAW VISTAS**
2. **Co-author - A.MAGESH KUMAR, ASSISTANT PROFESSOR VELS SCHOOL OF LAW, VISTAS**

Introduction:

In the contemporary digital age, the widespread use of the internet, mobile technologies, and digital platforms has significantly transformed the way individuals interact, communicate, and conduct daily activities. From social networking and online shopping to banking and healthcare services, personal data has become an integral component of modern life. As individuals increasingly rely on digital systems, vast amounts of personal information are continuously generated, collected, and processed. This shift has given rise to a data-driven economy where information is not only a resource but also a valuable commodity.

1.1 Constitutional Recognition of Privacy Rights

The recognition of privacy as a fundamental right represents a transformative development in constitutional law, particularly in jurisdictions grappling with digital transformation. In *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*[1], the Supreme Court of India unequivocally held that the right to privacy is an intrinsic part of Article 21, which guarantees the right to life and personal liberty. This judgment overruled earlier conflicting decisions and firmly established privacy as a constitutionally protected right. The Court further expanded the scope of privacy to include informational privacy, thereby acknowledging the realities of data-driven societies.

The judgment also laid down guiding principles for restricting privacy, including legality, necessity, proportionality, and procedural safeguards. However, while the decision significantly strengthened individual rights against state interference, its implications for private corporate entities remain indirect. In the absence of robust statutory enforcement mechanisms, corporations continue to operate in a relatively flexible environment, thereby creating a practical gap between constitutional ideals and real-world data practices

1.2 General Data Protection Regulation (GDPR) Framwork

The General Data Protection Regulation (GDPR) is widely regarded as the gold standard in global data protection law. It establishes a comprehensive framework governing the processing of personal data and is based on core principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, accuracy, integrity, and accountability. The GDPR also empowers individuals with strong rights, including data access, rectification, erasure, restriction of processing, and data portability.

[1] *K.S. Puttaswamy (Retd.) v. Union of India (2017)*

Despite its comprehensive nature, GDPR faces challenges in enforcement due to the complexity of modern digital ecosystems. Multinational corporations often operate across multiple jurisdictions, making uniform compliance difficult. Additionally, while GDPR mandates strict obligations, some corporations adopt a compliance-driven rather than ethics-driven approach, focusing on avoiding penalties rather than genuinely protecting user privacy. This creates a gap between regulatory intent and practical implementation.

1.3 United States Data Protection Approach (CCPA and Sectoral Laws)

The United States follows a decentralized and sector-specific approach to data protection rather than a unified privacy framework. The California Consumer Privacy Act (CCPA) is one of the most significant state-level laws, granting consumers rights such as knowing what personal data is collected, requesting deletion of data, and opting out of data sales. However, its applicability is limited geographically, leading to inconsistent privacy protections across the country.

At the federal level, privacy regulation is fragmented across sectors such as healthcare (HIPAA), finance (GLBA), and children's online privacy (COPPA). This fragmented structure allows corporations significant operational flexibility, often enabling them to design data practices that prioritize business interests. The absence of a unified national law results in regulatory gaps, making enforcement inconsistent and weakening overall consumer protection.

1.4 Indian Data Protection Framework (DPDP Act, 2023)

The Digital Personal Data Protection Act, 2023 represents India's most significant legislative step toward structured data governance. It introduces a consent-based framework for processing personal data and defines clear roles for data principals and data fiduciaries. The Act also establishes obligations related to transparency, purpose limitation, data security, and grievance redressal mechanisms.

However, despite its progressive structure, the Act has been criticized for broad exemptions granted to government agencies and limited regulation of automated decision-making systems. Furthermore, concerns exist regarding the absence of detailed provisions on data localization, algorithmic transparency, and independent regulatory oversight. These limitations suggest that while the Act strengthens legal recognition of privacy, practical enforcement challenges remain significant.

1.5 Information Technology Act, 2000 and Allied Rules

The Information Technology Act, 2000 was India's first comprehensive attempt to regulate electronic transactions and cyber activities. Section 43A introduced liability for failure to protect sensitive personal data, while Sections 66 and 72 address cyber offences and breach of confidentiality. This Act marked the beginning of India's legal recognition of digital data protection concerns.

The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 further expanded corporate obligations by requiring privacy policies and security standards. However, these provisions are now considered outdated in light of technological advancements such as artificial intelligence, cloud computing, and large-scale data analytics. The framework lacks the sophistication required to regulate modern data-driven corporate ecosystems effectively.

Government of India, *Digital Personal Data Protection Act, 2023*., Information Technology Act, 2000 (India), Sections 43A, 66, and 72., Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)Rules, 2011.

1.6 Judicial Interpretation of Privacy Rights

Judicial interpretation has played a crucial role in shaping privacy jurisprudence in India. Courts have consistently emphasized that privacy is essential to dignity, autonomy, and liberty. The judiciary has expanded constitutional interpretation to include informational privacy, thereby adapting fundamental rights to technological realities.

CONCLUSION

This research study examined the complex relationship between digital privacy rights and corporate data practices in the contemporary digital environment. It highlights that although privacy has been widely recognized as a fundamental right under constitutional principles and supported by modern data protection laws, its practical implementation remains inconsistent and often inadequate. The rapid expansion of digital technologies, coupled with the increasing dependence on data-driven business models, has created a situation where personal data is continuously collected, processed, and monetized, often beyond the awareness and control of userA key finding of the study is the clear gap between the legal recognition of privacy rights and their real-world enforcement. Legal frameworks such as the GDPR and the Digital Personal Data Protection Act, 2023, provide a strong foundation for safeguarding personal data.

However, in practice, their effectiveness is limited due to weak enforcement mechanisms, technological complexities, and the cross-border nature of digital data flows. This gap demonstrates that legal recognition alone is insufficient unless supported by strong institutional capacity and practical implementation strategies.

The study also reveals that corporate data practices are largely driven by commercial objectives. In the modern digital economy, personal data has become a valuable economic asset. Corporations extensively engage in data collection, behavioral tracking, profiling, and predictive analytics to enhance profitability through targeted advertising and personalized services. While these practices are often justified on the grounds of improving user experience, they simultaneously raise serious concerns regarding privacy intrusion and loss of individual autonomy.

Another important aspect identified is the ineffective nature of consent mechanisms in the digital environment. Although informed consent is a foundational principle of data protection law, its practical application is often weak. Users are frequently required to accept long and complex privacy policies without genuine understanding. This results in consent fatigue, where individuals mechanically agree to terms without fully considering the implications. Consequently, consent becomes a formal requirement rather than a meaningful expression of user choice.

The study further emphasizes the role of emerging technologies such as artificial intelligence, machine learning, and big data analytics in reshaping privacy concerns. These technologies enable corporations to infer sensitive personal information from non-sensitive data, thereby expanding the scope of privacy risks. Algorithmic decision-making systems often operate as opaque "black boxes," making it difficult for users to understand or challenge decisions that affect them. This lack of transparency raises concerns about accountability, fairness, and potential discrimination.

SUGGESTIONS

Suggestions and Recommendations

1. **Strengthening Data Protection Laws and Enforcement**

   Robust implementation of comprehensive data protection legislation, such as the *Digital*

Personal Data Protection Act, 2023 in India, is essential.

Regulatory authorities must be empowered with enforcement capabilities, including audits, penalties, and corrective directives to ensure corporate compliance.

2. **Privacy-by-Design and Default**

   Corporations should be legally mandated to adopt privacy-by-design principles, embedding data protection measures into technologies and business processes from the outset. Default settings must prioritize minimal data collection and user privacy.

3. **Transparent and Informed Consent Mechanisms** Companies must simplify privacy policies and ensure that consent is informed, specific, and freely given. The use of dark patterns that manipulate user choices should be explicitly prohibited.

4. **Data Minimization and Purpose Limitation**

   Organizations should collect only the data necessary for clearly defined purposes and avoid excessive or indefinite data retention. Regular data audits should be conducted to enforce this principle.

5. **Independent Data Protection Authorities (DPAs)**

   Establishing and strengthening independent regulatory bodies with adequate resources and autonomy will ensure impartial oversight of corporate data practices and swift grievance redressal.

6. **Corporate Accountability and Liability Frameworks** Companies must be held accountable through strict liability standards for data breaches and misuse. This includes mandatory breach notification requirements and compensation mechanisms for affected individuals.

7. **User Empowerment and Rights Awareness**

   Individuals should be educated about their digital rights, including the right to access, correction, erasure, and data portability. Awareness campaigns can bridge the knowledge gap between users and corporations.

8. **Ethical Data Governance and Self-Regulation** Corporations should adopt internal ethical frameworks, appoint data protection officers, and conduct regular impact assessments to ensure responsible data handling beyond mere legal compliance.

9. **Technological Safeguards and Cybersecurity Investments** Investment in encryption, anonymization, and advanced cybersecurity infrastructure is critical to protecting user data from breaches and unauthorized access.

10. **Global Cooperation and Standardization**

    As data flows transcend borders, harmonization with international frameworks such as

the GDPR can help create consistent standards and facilitate cross-border data protection.

11. **Regulation of Emerging Technologies**

    Special attention should be given to AI, big data analytics, and surveillance technologies, ensuring that their deployment does not infringe upon individual privacy rights.

12. **Grievance Redressal and Dispute Resolution Mechanisms** Efficient, accessible, and time-bound mechanisms should be established for users to report privacy violations and seek remedies without procedural complexities.