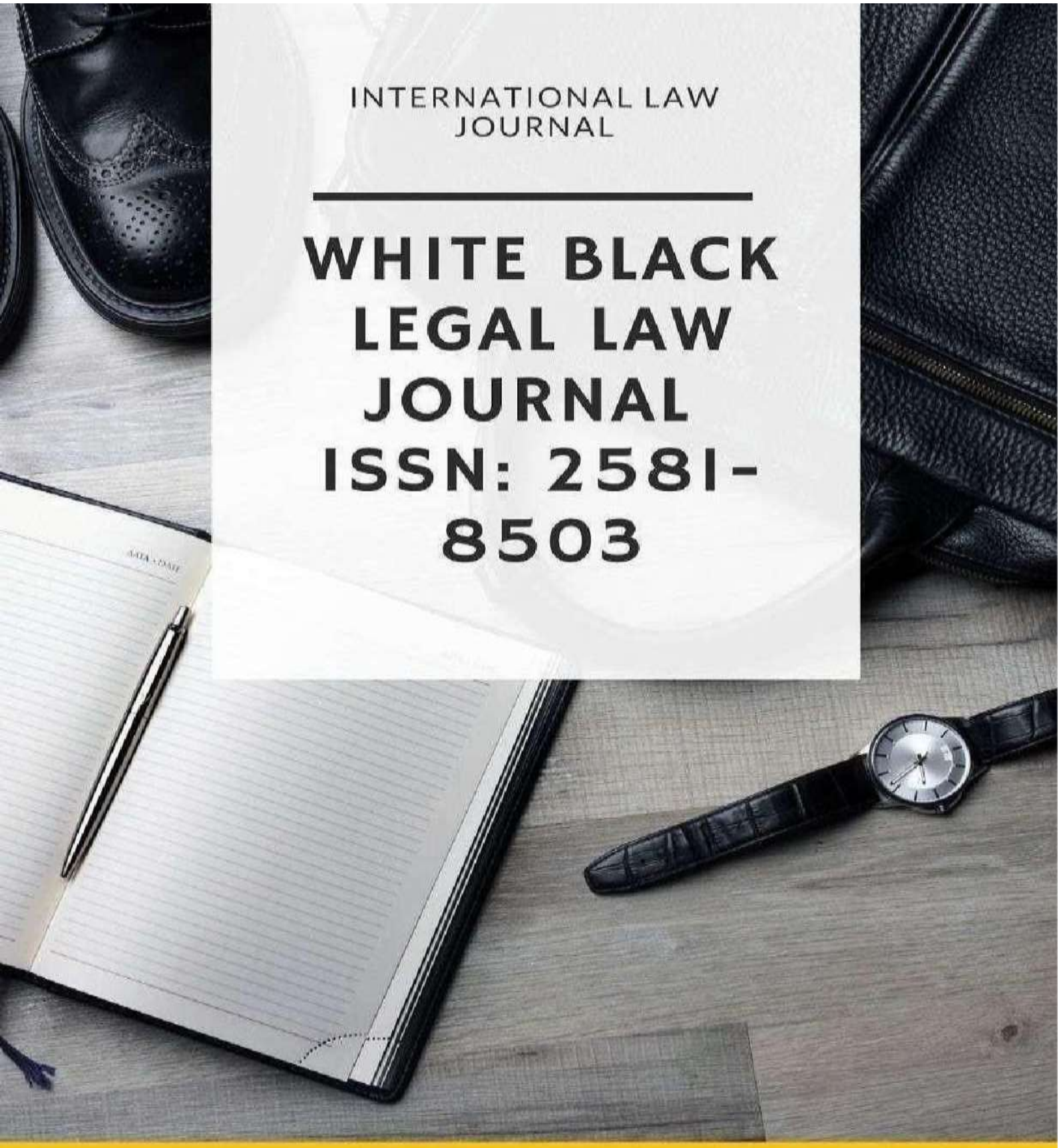

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

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.

ANALYZING THE STAKEHOLDERS AFFECTED BY DATA PRIVACY LAWS IN INDIA, THE UNITED STATES AND THE UNITED KINGDOM: A COMPARATIVE STUDY OF DATA PROTECTION

AUTHORED BY - AKSHAT KHOSLA

Abstract:

The protection of personal information and identifiable personal data has always occupied a position of immense magnitude in human life. The need for protecting such personal data is crucial in the digital age more so than ever, as online activities leave a trail of sensitive data, which can be misemployed by actors who collect and store digital information. Therefore, governments and non-state organizations across the world have introduced detailed regimens to regulate the collection and processing of digital personal data whilst seeking to foster data driven compliance and innovation. This research paper examines the stakeholders affected by data protection laws enacted in three jurisdictions, namely India's Digital Personal Data Protection Act, 2023 (DPDP), the United Kingdom General Data Protection Regulation (GDPR) and Data Protection Act 2018, and the fragmented and sector specific laws present in the United States of America. Special emphasis has been paid towards state laws, often overlapping with federal statutes in the United States, such as the California Consumer Privacy Act, 2018 (CCPA). The paper shall specifically analyze the key stakeholders and entities affected by these laws and the provisions for classifying categories of personal data, affecting the manner in which such sensitive data is processed.

Keywords: Privacy, Data Privacy, Personal Data, General Data Protection Guidelines.

Introduction:

A detailed examination of privacy laws must be preceded by a clear delineation of what constitutes privacy in the human conception. This idea is one central to our actions in our own domains and our autonomy over our activities. The University of California Privacy and Information Security Steering Committee Report of January 2013 described privacy as two intertwined concepts of autonomy and information privacy.

⇒ Autonomy is an individual's ability to conduct activities without concern of or actual observation

⇒ Information privacy is the appropriate protection, use, and dissemination of information about individuals[1]

Privacy therefore becomes a fundamental human right that acts as the most crucial accessory for an individual to enjoy their freedoms of speech, expression, and association. It includes within its ambit several rights necessary for the individual to both express himself in the way he sees fit and protect himself against unwanted intrusion, thus the right to privacy in the modern age is existent in both positive and negative forms. The importance of privacy in the human complexion has been illustrated by the French philosopher Gaston Bachelard, as he juxtaposes the concept of privacy with the structure of a house "I should say: the house shelters day-dreaming, the house protects the dreamer, the house allows one to dream in peace."[2] Privacy in human society has existed since time immemorial, however privacy as we envision it today was brought to the Americas by Europeans as the purchasing of land in the form of homesteads provided a steady platform for the furnishing of rights. In the New World therefore the home acted as the primary means for the exercising of privacy and the possession of material wealth was the barometer for the amount of privacy one possessed and by extension the very nature of the relationship one shared with the community so subsisting. In the view of David H. Flaherty, therefore, poverty signified a lack of privacy as individuals shared common dwellings with almost no separation.[3] In 1891 the right to privacy was described in a landmark article by lawyers Samuel Warren and Louis Brandeis, the latter of whom later served as an Associate Justice on the Supreme Court of the United States, titled The Right to Privacy where the authors asserted that the right to privacy entailed the "right to be let alone". Brandeis and Warren detail the existence of privacy and this "right to be let alone" through an exploration into the manner in which newspapers often circumvented the privacy of an individual through the publishing of private portraits and how " what is whispered in the closet shall be proclaimed from the house-tops" through this new menace.[4] This paper serves as a milestone in the development of privacy laws in the new century and exhorted the judiciary to protect this most sacred right of an individual. Authors who have written on this subject have often focused on

[1] University of California, "Privacy and Information Security Initiative Steering Committee Report to the President" Page no. 3 (2013).
[2] Gaston Bachelard, *The Poetics of Things*. (Penguin Classics, 2014).
[3] David H. Flaherty, "Privacy in Colonial New England", XII *Charlottesville: University Press of Virginia* (1972).
[4] Louis Brandeis, Samuel D. Warren II, "The Right to Privacy", IV *Harvard Law Review* (1890).

various intrinsic aspects of privacy law such as the need to protect privacy and the manner in which the state has contravened the private domain of the individual, especially with the existence of surveillance states in the 21st century. The particular focus of this paper however lies in the yet emerging field of data privacy and the legislation which regulates this field in India, the United Kingdom, and the United States of America. Data privacy can be defined simply as the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.[5] The protection of digital data privacy occupies paramount importance in today's digitized society as personal data can be used to uniquely identify an individual through personally identifiable information and sensitive personal information. The very nature of personal information is such that it helps in locating the identity of the individual, which includes physical and digital identity, potentially dangerous for the personal liberty of the individual if breached[6]. This is the reason why governments across the world have taken notice and made regulations to regulate this field. The congruency of data privacy laws is also seen in the fact that in a globalized world where data often seamlessly flows between jurisdictions, legislation is necessary to regulate the relationship which individuals and intermediaries share with personal data. Amongst the foremost examples of international guidelines are the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which act as minimum standards to be upheld by the OECD member states. The report very clearly states that "The principles encompass all media for the computerized processing of data on individuals (from local computers to networks with complex national and international ramifications), all types of personal data processing (from personnel administration to the compilation of consumer profiles) and all categories of data (from traffic data to content data, from the most mundane to the most sensitive)."[7] The European Union has also established the General Data Protection Regulation, a document of foremost importance in the protection of individual data.

Research Question:

Identifying and analyzing the key stakeholders affected by digital data protection laws in India, the United States, and the United Kingdom: Examining the ways in which individual freedom and autonomy is protected and the way in which these classifications can be widened.

[5] https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-privacy/ (last visited on 18th September, 2025.)
[6] https://www.datacamp.com/blog/what-is-data-privacy (last visited on 18th September, 2025).
[7] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1982, preface.

Discussion:

Examining the key stakeholders affected by the DPDP Act, 2023, the UK GDPR, and the CCPA, 2018:

The ecosystem of processing digital personal data in India involves a complex interplay between three stakeholders who act in concert to enforce the provisions of the DPDP Act, namely the Data Principal, Data Fiduciary, and the Data Processor. Section 2 (j) of the Act defines the Data Principal as follows:

"Data Principal" means the individual to whom the personal data relates and where such individual is—

i. a child, includes the parents or lawful guardian of such a child;
ii. a person with disability, includes her lawful guardian, acting on her behalf[8]

Data principals, also referred to as data subjects is several jurisdictions, are essentially those individuals to whom the personal data belongs and who provide the data to data fiduciaries for processing.[9] The DPDP Act furthermore regulates only the rights of natural persons and only with respect to the collection and processing of digital personal data, not covering within its ambit offline records and anonymized personal data. The Act also does not create distinctions between sensitive personal data and treats all personal data at par.[10] It is a noteworthy observation that the act shall also apply to non-citizens residing India in whose data processing "in connection with any activity related to offering of goods or services" happens outside India. So as an example a U.S. citizen residing in India who avails services from digital providers based in India or outside India will be affected by the provisions of the Act.[11] The collection of personal data can only take place after the data fiduciary informs the principal about the specific purpose for which the data is to be used and the data principal maintains the right to withdraw this consent at any stage of data processing and ask for a summary of the data being utilized by the data fiduciary. The right to erasure and correction is also possessed by the data principal as is defined in Section 12 (2-3):

[8] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[9] The Data Principal's Handbook: Navigating the DPDP Act, *available at*, https://www.azbpartners.com/bank/the-data-principals-handbook-navigating-the-dpdp-act/ (last visited on 27th September, 2025).
[10] *Ibid.*
[11] Anirudh Barman, 'Understanding India's New Data Protection Law', *Carnegie India* page number 3 (2023).

12. (2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal,—

a) correct the inaccurate or misleading personal data;
b) complete the incomplete personal data; and
c) update the personal data.
d) (3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.[12]

Any Data Fiduciary or class of Data Fiduciaries may be notified by the Union Government as Significant Data Fiduciaries (SDF) under Section 10 of the DPDP Act based upon the following considerations:

- The volume and sensitivity of personal data processed;
- The risk to the rights of the Data Principal;
- Potential impact to the sovereignty and integrity of India;
- Security of the State;
- Public order and maintenance of internal security.[13]

This enables the Central Government to classify an entity as an SDF based not on their revenue or size, but rather the risks posed to the Data Principal and the sensitivity of the data being processed. A medium scale genomics firm can be classified as an SDF if they handle extremely sensitive digitally identifiable digital personal data. Data Fiduciaries and Significant Data Fiduciaries, therefore, constitute the second set of crucial stakeholders within the Act. Data Fiduciary can be defined as any entity which is responsible for envisioning the purpose and means of the processing of personal data, including any company, individual or organization responsible for the usage, collection and storing of the Data Principal's data.[14] A misconception persists that the entity which collects personal data from the Data Principal is the Data Fiduciary, whereas the other entities that receive personal data from the data fiduciary would

[12] I*d.* Page number 3
[13] Significant Data Fiduciaries Under The DPDP Act And DPDP Rules: The New Frontier Of Risk Classification, DPIAs, And Algorithmic Accountability, *available at,* https://www.mondaq.com/india/privacy-protection/1709432/significant-data-fiduciaries-under-the-dpdp-act-and-dpdp-rules-the-new-frontier-of-risk-classification-dpias-and-algorithmic-accountability (last visited on 25th March, 2026).
[14] International Centre for Information Systems and Audit, "PursuIT: Data Protection and Data Privacy, 9th edition" page numbers 5-8.

only be considered as data processors. Such a notion stems from the belief that the recipient entities are merely rendering a service to the data fiduciary, neither enjoying privity of contract nor directly engaging with the Data Principal. Since the recipient entities are at an arms' length from the Data Principal, the belief exists that such recipient entities are merely Data Processors, whereas the entity receiving personal data from the Data Principal would be considered as Data Fiduciary. However, this is not the true intent of the statute and involves a complicated assessment of the role, responsibilities and degree of influence that one party exercises over the processing of personal data by another.[15] Data Processors simply process data on behalf of Data Fiduciaries. The relationship between a Data Fiduciary and Data Processor can be understood clearly with the analogy of the puppeteer and the puppet. It can be stated that a Data Fiduciary has determined the purpose and means of processing personal data when the Data Processor is following detailed and specified instructions from the Data Fiduciary. Only when the Data Processor does not exercise significant autonomy or independence with respect to processing of such data and when the latter can be considered as extra arms and limbs for the Data Fiduciary to process personal data - can it be said that the Data Processor is processing data on behalf of the Data Fiduciary. Only when the puppeteer works the puppet, can it be said that the puppeteer is the Data Fiduciary, and responsible for working the puppet, the Data Processor.[16]

The data privacy regimen in the United States is not one identified with any sector specific law but rather a complex patchwork of federal, state, and local regulations which are often sector specific, as can be said about several other sectors of prominence in the economic sphere.[17] Federal laws and regulations include those that apply to financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, online privacy of children, telemarketing, email marketing, biometrics, and communications privacy laws. There are also a number of state privacy and data security laws that can overlap with federal statutes, some of these state privacy laws are preempted in part by federal laws, while others are not.[18] California became the first state in the United States to pass a law regulating the digital personal information of consumers with the California

[15] Data Fiduciary versus Data Processor – An Identity Crisis, *available at*, https://www.azbpartners.com/bank/data-fiduciary-versus-data-processor-an-identity-crisis/ (last visited on 28th September, 2025).
[16] *Ibid.*
[17] Data protection laws in the United States *available at* https://www.dlapiperdataprotection.com/?c=US (last visited on 28th September, 2025).
[18] Conor Murray, "U.S. Data Privacy Protection Laws: A Comprehensive Guide", *Forbes*, April 21st, 2023.

Consumer Privacy Act of 2018, which took effect on 1st January, 2020. The CCPA grants California residents comprehensive rights regarding identifiable personal information. It imposes data protection duties on entities and organizations conducting business in California and deals expressly with personal data privacy.[19] The CCPA provides protections for consumers, broadly defined as any California residents who are either in California for a purpose which is not transitory or temporary, or living in California but currently out of state for a temporary or transitory purpose.

The CCPA expands upon the definition of sensitive personal information provided in other California state laws. It includes any information that directly or indirectly:

- Identifies, relates to, or describes a particular consumer or household;
- Is reasonably capable of being associated with or linked to a particular consumer or household. The CCPA shall also protect data even if it does not relate to an individual because it covers households and devices, and it protects information connected to a unique identifier instead of a person's name.[20]

The Act also defines clearly the organizations that must comply with the CCPA. For-profit entities must ensure compliance with the CCPA if they collect a consumer's personal information and determine the purposes and means of processing, and do business in California and meet one of these thresholds:

- Annual gross revenue that exceeds $25 million (adjusted for inflation);
- Annually buy, share, or sell the personal information of more than 100,000 consumers or households; or
- Derive 50% or more of annual revenues from selling or sharing consumers' personal information.

There are several exceptions to the CCPA. For example, entities do not have to comply with the Act if:

- Every aspect of the commercial conduct takes place wholly outside of California;
- The sale of personal information is part of a merger or acquisition;
- There are legal or conflicts-of-laws issues.

[19] What is the California Consumer Privacy Act (CCPA)?, *available at*, https://www.ibm.com/think/topics/ccpa-compliance (last visited on 25th March, 2026).
[20] Marjorie Richter, "The California Consumer Privacy Act (CCPA) — Legal Glossary", *Thomson Reuters*, December 15th, 2025.

The CCPA does not apply to non-profit and public entities, which are covered by other laws. This aspect is normatively different from the definition of a Data Fiduciary provided in the DPDP Act, which does not restrict itself to for-profit organizations and covers all entities and individuals processing digital personal data of any kind. The state of California has historically been a hotbed of commercial activity and Silicon Valley, located in the Bay Area of Northern California, houses several information technology companies which collect digital personal information on a vast scale. The objective of the CCPA is not to regulate every single aspect of data collection, but simply to ensure compliance amongst for-profit corporations involved in data processing and enhance privacy rights for California residents. In stark contrast to the United States, India possesses a fragmented and nascent data processing framework, where individuals often provide their personal information to several intermediaries and data brokers. The objective of the DPDP Act, therefore, is to enhance regulatory frameworks and mandate data security. The frameworks created by the Act seek to build a safe digital ecosystem for growth and innovation.

The United Kingdom General Data Protection Regulation borrows several key principles from the European Union General Data Protection Regulation and defines the manner in which businesses must engage with the data of UK residents – whether it be consumer analytics or online marketing. It regulates how organizations collect, store, secure, and process the personal data of UK residents, and aims to ensure that individuals maintain control over their digital information. Article 4 of the GDPR establishes the key stakeholders and defines the boundaries within which organizations can collect and process data.

Article 4. (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[21]

The UK GDPR defines the Data Subject, a natural person who can be identified, either directly or indirectly, through information such as their name, Government issued ID number, location data or any other online identifier. Notably, the UK GDPR does not place all personal data on

[21] "General Data Protection Regulation" as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

the same plane, laying down special categories of personal data based on its sensitivity. Certain kinds of sensitive personal data act an identifier of racial or ethnic origin, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership. Article 9 of the GDPR expressly prohibits the processing of such data, with certain exceptions.

Article 9. (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[22]

The GDPR clearly stipulates that the jurisdiction of the Regulation shall be territorial in nature, applying to individuals in the United Kingdom, whether they are natural citizens or residing for a transitory period. The Regulation shall also have extra-territorial effect, as is the case with the EU GDPR. An organization that it is not established within the territorial confines of the United Kingdom will be subject to the UK GDPR if it processes the personal data of those Data Subjects who are in the United Kingdom, where the processing of data is related "to the offering of goods or services" [Article 3(2)(a)] to such data subjects in the United Kingdom or "the monitoring of their behaviour" [Article 3(2)(b)] as far as their activities take place within the United Kingdom.[23] The bar which has been set for "identifiable" is a low one, and simply means "all means reasonably likely to be used" according to Recital 26 of Article 4. Processing too has been accorded an extremely wide ambit, and includes any operations on data, including storage, deletion or modification.

India's DPDP Act creates no distinction between "sensitive" or "general" data, and all information procured by Data Fiduciaries or Data Processors is subject to the same standards of consent and compliance. This can be observed in stark contrast to Article 9 of the UK GDPR which prohibits the processing of sensitive personal data, such as information relating to an individual's sexual orientation or health status. Marginalized individuals are subjected to cyber-crimes at a greater rate, and their personally identifiable information is more vulnerable to online threats. The data protection framework in India shall evolve in a more comprehensive manner once it recognizes the varied and comprehensive needs of different social groups, and

[22] *Ibid*.
[23] https://www.dlapiperdataprotection.com/?c=GB (last visited on 26th March, 2026).

different categories of sensitive data.

Conclusion:

The divergences present in the evolution of digital data protection legislation in India, the United Kingdom, and the United States have evolved as a result of evolving policy considerations and legal cultures, shaped by the nature of the polity and socioeconomic order. Policy debates in India around privacy law in general and data privacy laws more specifically have evolved after a close examination of the General Data Protection Regulation, and especially the provisions in the DPDP Act relating to consent of the Data Principals and the processing of personal data by Data Fiduciaries, have evolved in the Indian jurisprudential sphere following the strict patterns present in European and British legislation around the protection of personal digital data.

There are certain provisions relating to the classification of stakeholders present in the UK GDPR which are not present in the Indian DPDP Act, these terms are present in Article 9 of the UK GDPR, having been explicated in this paper previously. The researchers suggest that the DPDP Act evolves specific methods of ensuring the free and efficacious obtaining and withdrawal of consent, and especially concerning the stratifications around sensitive personal data present in the UK GDPR.

Finally, Indian data privacy legislation has also not adopted sufficient provisions regarding cross border data transfers, although these transfers are not prohibited by the government, the absence of clear adequacy frameworks and standardized contractual clauses creates great uncertainty for multinational companies. Corporate organizations today organize the transfer of personal data across several different jurisdictions and the lack of binding corporate rules and clearly defined provisions hinders the development of corporate entities in India. The United Kingdom regulates international data flows more in a smooth and streamlined manner by allowing transfers to countries which have been recognized as providing adequate data protection, or through binding corporate rules and standard contractual clauses. Legislation in the United States generally permits free and equitable cross-border data transfers although certain state laws may impose restrictions, and multinational entities often question the adequacy of privacy protections in the United States. Adopting these principles and best practices shall allow for the DPDP Act to comprehensively reflect the reality of data transfers in a more globalized world, and protect individual freedom and autonomy.