International Journal of
Science, Architecture, Technology and Environment

Why Privacy Laws Fail or Succeed: Cost, Architecture, and Governance under the DPDP Act in Comparative Perspective

Varun N. Rao[1], Narendra Vijayasimha[1*]

[1]*Rezorce Research Foundation, 111/1 II Floor 6th Main Malleswaram Bangalore 560003 India*

[*]*Corresponding author, narendra.vijayasimha@rezorce.com*

DOI: https://doi.org/10.63680/ijsate1125073.055

Abstract

The enactment of India's Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant transition toward a consent-centric and accountability-based privacy framework. However, comparative experience from the European Union (GDPR), the United States (CCPA/CPRA), Brazil (LGPD), and Singapore (PDPA) demonstrates that the effectiveness of privacy laws depends less on statutory text than on how implementation challenges are addressed in practice. This study examines four recurring implementation constraints - cost of compliance, cross-border data transfers, data mapping, and ambiguity in non-consensual processing bases, and evaluates their implications for India's DPDP regime. Methodologically, the study adopts a qualitative comparative legal and policy analysis, synthesizing regulatory enforcement decisions, court judgments, empirical economic studies, and technical governance literature across jurisdictions. The findings indicate that privacy compliance consistently evolves into an architectural problem, driven by fixed infrastructure costs, fragmented data environments, and uncertainty around lawful processing bases. India's DPDP Act mitigates some risks, particularly ambiguity around "legitimate interest", but remains vulnerable to compliance cost inflation, cross-border uncertainty, and data-inventory failures. The study concludes that effective DPDP implementation requires regulatory recognition of privacy as a systems-governance challenge. It recommends architecture-aware compliance models, automation of consent and data-flow controls, and risk-based regulatory guidance. These measures can enable India to avoid the structural failures observed in earlier regimes while supporting innovation and scalable compliance.

Keywords: Digital Personal Data Protection Act (DPDP Act); Privacy Compliance Architecture; Cross-Border Data Transfers; Data Mapping and Governance; Comparative Privacy Law

Introduction

Over the past decade, data protection laws have proliferated across jurisdictions, responding to the growing economic and social centrality of personal data. The European Union's General Data Protection Regulation (GDPR) established the global benchmark, followed by sectoral and rights-based models such as the California Consumer Privacy Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGPD), and Singapore's Personal Data Protection Act (PDPA). While these frameworks differ in structure and enforcement

philosophy, a growing body of scholarship shows that they encounter remarkably similar implementation challenges (Hoofnagle, Van der Sloot, and Borgesius 2019; Goldfarb and Que 2023).

India's DPDP Act enters this landscape with a distinct design with a strong reliance on consent, narrowly defined non-consensual "legitimate uses," and a negative-list approach to cross-border transfers. This paper asks the following research question - What structural implementation challenges are most likely to shape the real-world effectiveness of the DPDP Act? and what lessons can be drawn from comparative privacy regimes?

The objective of the study is threefold:

(1) Identify recurring implementation constraints across major privacy regimes;
(2) Assess how these constraints manifest under the DPDP Act; and
(3) Derive technical and architectural implications for Indian organizations and regulators.

Methods (Materials and Methods)

Study Design

The study employs a qualitative, comparative, doctrinal-policy research design. It is non-experimental and observational in nature, relying on secondary data sources rather than human participants.

Materials were selected using purposive sampling and include:

- Peer-reviewed economic and legal scholarship on GDPR, CCPA/CPRA, LGPD, and PDPA;
- Regulatory enforcement decisions (e.g., GDPR fines, CCPA settlements, PDPC decisions);
- Judicial rulings interpreting lawful bases for processing;
- Policy briefs and technical governance studies on privacy compliance systems.

Sources were selected based on relevance to implementation costs, data governance, cross-border transfers, and lawful-basis ambiguity.

Analytical Procedure

- Identification of implementation challenges recurring across jurisdictions.
- Jurisdiction-wise synthesis of legal, economic, and regulatory evidence.
- Mapping of these challenges onto the DPDP Act's statutory design.
- Derivation of architectural and governance implications.

The study uses comparative legal analysis, thematic synthesis, and policy-oriented qualitative reasoning. No statistical hypothesis testing is undertaken; instead, empirical findings from cited economic studies are incorporated descriptively.

Results

The analysis yields four principal findings.

(1) Cost of compliance emerges as a fixed, front-loaded burden driven by governance infrastructure rather than enforcement penalties. Empirical studies under the GDPR and CCPA show profit reductions and cost pass-through effects, particularly for SMEs (Frey and Presidente 2024; Gupta, McGowan, and Ongena 2024).

(2) Cross-border data transfers generate systemic uncertainty rather than outright prohibition. Post-

Schrems II jurisprudence demonstrates that legal permissibility alone is insufficient without continuous risk assessments and technical safeguards, disrupting global cloud-based operations (Mattoo and Meltzer 2018).

(3) Data mapping and inventory failures consistently underlie enforcement actions across regimes. Regulators treat the absence of a comprehensive data map as evidence of inadequate security and accountability, leading to breaches of access, deletion, and retention obligations (Sirur, Nurse, and Webb 2018).

(4) Ambiguity in lawful bases, particularly "legitimate interest," produces regulatory conflict and business-model instability under GDPR and LGPD. India's DPDP Act largely avoids this ambiguity by restricting non-consensual processing to defined categories, shifting compliance pressure toward consent systems (Chik 2022).

Cost of Compliance as a Central Constraint

Across jurisdictions, the implementation of modern data protection regimes has revealed that cost of compliance, rather than doctrinal ambiguity alone, constitutes the dominant constraint shaping regulatory effectiveness, firm behaviour, and innovation outcomes. Empirical evidence from the European Union's General Data Protection Regulation (GDPR), the United States' California Consumer Privacy Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGPD), and Singapore's Personal Data Protection Act (PDPA) consistently demonstrates that privacy regulation operates primarily through cost channels: organizational restructuring, technological re-architecture, legal risk management, and ongoing compliance verification. These costs disproportionately affect small and medium-sized enterprises (SMEs), data-intensive sectors, and public services, thereby influencing both economic performance and regulatory legitimacy (Frey and Presidente 2024; Koski and Valmari 2020).

India's Digital Personal Data Protection Act, 2023 and its accompanying Rules must therefore be assessed not merely as a legal framework, but as a cost-inducing institutional architecture whose success will depend on how compliance burdens are distributed, internalized, and technologically mediated.

GDPR and the Economics of Compliance

A growing body of firm-level empirical research establishes that GDPR compliance costs manifested primarily as extra expenses, not as reductions in sales or market access. Frey and Presidente (2024) estimate a 2.1 percent reduction in profits among firms exposed to EU markets, driven by increased wage bills for specialized compliance personnel, accelerated patenting activity, and investments in secure IT systems. Crucially, these expenses were largely fixed or quasi-fixed, intensifying scale disadvantages for smaller firms.

Complementary evidence from Koski and Valmari (2020) demonstrates that data-intensive SMEs experienced the most pronounced decline in profit margins during the first year of GDPR enforcement. Large multinational firms, by contrast, absorbed compliance costs more efficiently, suggesting that GDPR effectively raised minimum efficient scale in data-driven markets. These findings reinforce the conclusion that privacy regulation restructures market competition by reallocating compliance capacity rather than uniformly raising consumer protection standards.

Organizational studies further show that compliance difficulties were not confined to legal interpretation. Sirur, Nurse, and Webb (2018) identify three operational bottlenecks: the breadth of regulatory obligations, the translation of qualitative standards into technical controls, and the requirement to map complex internal data flows. For organizations lacking mature data governance systems, compliance became a costly discovery process rather than a straightforward checklist exercise.

Sector-specific evidence reinforces this conclusion. Yuan and Li (2019) find that EU hospitals providing digital health services experienced measurable financial distress following GDPR implementation, reflecting the urgent and costly redesign of health IT architectures to meet heightened data protection standards.

CCPA and Fixed-Cost Regressivity

The U.S. experience under the CCPA illustrates how privacy compliance costs can propagate through markets via price effects and credit allocation. Yallen (2019) reports initial compliance costs approaching USD 55 billion, with ongoing maintenance costs estimated at USD 16 billion over a decade. These figures underscore the magnitude of compliance as a macroeconomic phenomenon rather than a firm-specific nuisance.

Micro-level evidence from mortgage markets demonstrates how these costs are internalized. Gupta, McGowan, and Ongena (2023; 2024) estimate that the CCPA increased average bank compliance expenditures by approximately USD 1 million, largely in legal, telecommunications, and data-processing functions. These fixed costs were passed on to borrowers through higher interest rates, increasing the lifetime cost of mortgages and reducing credit availability by 3.4 percent. The authors further show that economies of scale favoured large institutions and nonbank lenders with less data-intensive screening models.

Risk-management literature highlights the dual nature of compliance costs. While expensive, compliance investments are framed as rational responses to severe non-compliance risks, including regulatory penalties and class-action litigation (Garlie 2020). This dynamic reinforces a compliance arms race, in which firms overspend defensively, often without proportional improvements in substantive privacy outcomes.

LGPD, Liability, and Organizational Adaptation

Brazil's LGPD experience emphasizes the interaction between compliance costs and liability regimes. Brizolla et al. (2024) document that organizations incurred substantial expenditures on internal training, privacy policy development, contingency planning, and technical safeguards to avoid infractions and fines. These costs were particularly salient for professional services and accounting firms, where data protection capabilities were historically underdeveloped.

A systematic review by de Lucena et al. (2024) identifies recurring compliance challenges across Brazilian organizations, including limited technical expertise, unclear internal accountability structures, and difficulties operationalizing data subject rights. These challenges translated directly into increased compliance expenditure and delayed implementation.

Dresch and Faleiros Júnior (2024) further show that LGPD's strict civil liability regime amplifies compliance costs by linking financial and reputational risk directly to data handling failures. Judicial interpretations by Brazil's Superior Tribunal de Justiça have reinforced incentives for proactive investment in compliance systems, even where legal standards remain unsettled. In effect, liability risk transforms compliance from a discretionary cost into a non-negotiable operational expense.

Cost Moderation Through Reasonableness

Singapore presents a contrasting model in which compliance costs are explicitly moderated through legal design. Ter (2013) characterizes the PDPA as a pro-business framework that balances data protection with economic competitiveness by limiting prescriptive obligations. Subsequent doctrinal analysis by Chik (2022) explains how the "reasonableness" standard, expanded deemed consent, and legitimate interest exceptions reduce the need for constant transactional consent, thereby lowering administrative and technological overhead.

From a cost perspective, Singapore's approach shifts compliance from exhaustive procedural documentation toward outcome-oriented risk management. This design choice illustrates how regulatory architecture can influence not only the level of compliance costs but also their structure and predictability.

Cost Implications for DPDP Implementation

The comparative evidence yields three critical implications for India's DPDP implementation.

First, compliance costs will be front-loaded and fixed, especially for data mapping, consent management, breach response systems, and audit readiness. As in the GDPR and CCPA contexts, these costs will disproportionately affect SMEs and startups.

Second, technology architecture will determine cost sustainability. Jurisdictions that relied on retrospective compliance retrofits experienced higher expenses and operational disruption. India's DPDP Rules therefore risk escalating costs if compliance is enforced primarily through ex post penalties rather than incentivizing privacy-by-design architectures.

Third, liability and enforcement signals will shape spending behaviour. Brazil's experience demonstrates that strict liability accelerates compliance investment but also raises barriers to entry. Without calibrated enforcement thresholds or safe harbours, DPDP enforcement could replicate these effects in India's innovation-sensitive sectors.

Cross-Border Data Transfers - Next Binding Constraint

While compliance cost represents the first-order economic constraint in privacy law implementation, cross-border data transfers (CBTs) have emerged as the next critical fault line in global data governance. Unlike domestic compliance obligations, CBT rules directly confront structural features of the digital economy like cloud centralization, multinational service provision, and asymmetric state surveillance powers. Across jurisdictions, privacy regimes increasingly regulate not merely how personal data is processed, but where it may lawfully flow, transforming international data transfers into a combined legal, geopolitical, and technical problem (Mercurio and Yu 2022; Khan 2025).

Empirical and doctrinal scholarship shows that CBT rules now shape firm architecture, cloud strategy, and vendor selection as decisively as substantive privacy rights. For India's Digital Personal Data Protection Act (DPDP Act) and (DPDP Rules), this experience is especially salient because India has adopted a structurally distinct and yet functionally convergent approach to international transfers.

GDPR and the Collapse of Transfer Certainty

The EU's GDPR represents the most developed and restrictive CBT regime. Transfers of personal data outside the European Union (EU) / European Economic Area (EEA) are prohibited unless the destination jurisdiction ensures an "essentially equivalent" level of protection, operationalized through adequacy decisions, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or narrow derogations (Mattoo and Meltzer 2018).

This framework was fundamentally destabilized by the Court of Justice of the European Union's Schrems II decision, which invalidated the EU–US Privacy Shield and redefined the legal burden associated with SCC-based transfers. The Court held that US surveillance laws, particularly those enabling bulk government access without proportionate safeguards or effective judicial redress, undermined the fundamental rights guaranteed under EU law. While SCCs formally survived, the ruling imposed a new obligation on exporters and importers to conduct Transfer Impact Assessments (TIAs) assessing third-country surveillance risks on a case-by-case basis (Lin 2024).

Subsequent enforcement confirmed that Schrems II was not merely doctrinal. The €1.2 billion administrative fine imposed on Meta Platforms Ireland in 2023 demonstrated that continued reliance on SCCs without effective supplementary measures constituted a direct violation of GDPR Chapter V. Regulators emphasized that contractual assurances cannot neutralize incompatible foreign public law, effectively converting CBT compliance into a hybrid legal–technical exercise involving encryption, key management, and architectural redesign.

Technology Fallout: Cloud Computing and the TIA Crisis

Post-Schrems II, CBT compliance shifted decisively from legal documentation to technical feasibility. Guidance from European regulators clarified that supplementary measures must be effective against foreign government access, not merely symbolic. This requirement rendered many conventional cloud configurations legally fragile, particularly where encryption keys remained accessible to US-based providers subject to the CLOUD Act (Khan 2025).

Academic and policy literature documents that "hold-your-own-key" (HYOK) or client-side encryption models became de facto compliance expectations, despite their incompatibility with many Software-as-a-Service (SaaS) offerings. As a result, firms faced a stark choice: accept architectural inefficiency and cost escalation, localize processing, or exit certain data-intensive services altogether (Mercurio and Yu 2022). In effect, GDPR transformed CBTs into a system design constraint, not merely a compliance checklist.

CCPA and the Purpose-Based Transfer Model

In contrast to the GDPR's geography-centric approach, the California Consumer Privacy Act (CCPA), as amended by the CPRA, regulates CBTs indirectly. The statute does not restrict transfers based on destination country adequacy. Instead, it focuses on purpose and relationship, distinguishing between "service providers," "contractors," and third parties, and regulating whether data is "sold" or "shared" (Pazhohan 2023).

From a cross-border perspective, this model shifts compliance emphasis to contractual flow-downs and consumer opt-out enforcement. Enforcement actions such as the Sephora settlement established that a business remains responsible for downstream data use by international partners, particularly in advertising and analytics ecosystems. The geographic location of the recipient is largely irrelevant; what matters is whether consumer rights travel with the data.

Scholarly analysis characterizes this approach as less disruptive to global data flows but more administratively complex due to the fragmented U.S. state-level privacy landscape. The absence of a unified federal transfer mechanism forces multinational firms to manage overlapping contractual obligations rather than rely on standardized instruments such as SCCs (Coche, Kolk, and Ocelík 2024).

LGPD and Convergent Adequacy Logic

Brazil's LGPD occupies an intermediate position. While modelled on GDPR principles, its CBT provisions are less prescriptive and more discretionary. Transfers are permitted where the destination country provides adequate protection, or where contractual and organizational safeguards exist (de Magalhães 2021).

Empirical studies of LGPD implementation reveal that CBT compliance costs arise primarily from organizational uncertainty rather than technical impossibility. Firms face ambiguity regarding adequacy determinations, regulator expectations, and liability exposure, prompting conservative compliance strategies and increased legal expenditure (Khan 2025). Judicial interpretations linking CBT failures to strict civil liability further amplify risk sensitivity, incentivizing over-compliance.

Singapore and ASEAN: Flexibility and Norm Diffusion

Singapore's PDPA exemplifies a pragmatic CBT framework. Rather than imposing adequacy-style restrictions, it requires organizations to ensure that transferred data receives a "comparable standard of protection". This standard is satisfied through contractual assurances and accountability mechanisms, significantly reducing friction for multinational data operations (Pazhohan 2023).

Research on EU external governance shows that GDPR norms nonetheless exert indirect influence in ASEAN jurisdictions, shaping reforms and compliance expectations even where formal adequacy regimes are absent (Gomes 2024). This illustrates a broader pattern - GDPR's CBT logic increasingly operates as a global reference point, regardless of local statutory design.

DPDP's Blacklisting, Uncertainty, and Extraterritorial Risk

India's DPDP Act adopts a structurally distinct negative-list (blacklisting) approach. Section 16 permits transfers to any country unless the Central Government notifies specific jurisdictions as restricted (DPDP Act). On its face, this appears more permissive than the GDPR's whitelisting model.

However, comparative analysis suggests that the primary challenge under DPDP will not be transfer mechanisms but regulatory uncertainty. Businesses lack clarity on the criteria that will govern blacklisting decisions, the role of surveillance risk, and the interaction between DPDP compliance and foreign obligations (Khan 2025).

From a technology perspective, Indian firms using US-based cloud providers may remain DPDP-compliant while simultaneously violating GDPR obligations if EU personal data is involved. Thus, Indian data fiduciaries face a dual-risk environment in which domestic legality does not guarantee international operability. This mirrors the Schrems II dilemma, but without the procedural infrastructure, such as adequacy decisions or SCCs, to manage it systematically.

Engineering Responses: Automation and Compliance Systems

Recent technical literature proposes automated compliance management systems capable of mapping heterogeneous transfer rules, visualizing data flows, and enforcing jurisdiction-specific constraints dynamically. Such architectures rely on policy engines, encryption controls, and transfer-risk identification mechanisms to operationalize legal requirements across GDPR, CCPA, LGPD, and emerging regimes (Zhuang et al. 2024).

For DPDP implementation, these systems offer a potential mitigation strategy, enabling firms to manage uncertainty through programmable governance rather than manual legal review. However, this shifts compliance cost from legal advisory to engineering investment, reinforcing the earlier conclusion that privacy regulation increasingly manifests as architectural cost.

Data Mapping as the Third Structural Bottleneck

Beyond compliance cost and cross-border transfers, data mapping emerges as the third and most operationally destabilizing constraint in the implementation of modern privacy laws. Across jurisdictions, privacy regimes assume that organizations possess a granular, continuously updated understanding of their personal data holdings. This includes information like what data exists, where it resides, how it flows, who accesses it, and for what purpose. In practice, this assumption frequently collapses under the weight of legacy systems, decentralized IT governance, and complex vendor ecosystems.

Empirical research and enforcement experience demonstrate that failures in data mapping rarely appear as

standalone violations. Instead, they materialize indirectly as breaches of security, accuracy, accountability, and data subject rights (Rocha and Canedo 2025). As a result, data mapping functions as the silent prerequisite for almost every substantive obligation under GDPR, CCPA/CPRA, LGPD, and PDPA, and, increasingly, under India's DPDP Act.

GDPR and the Discovery Problem

Under the GDPR, data mapping is not explicitly mandated as a discrete obligation, yet it is structurally embedded in multiple requirements, including Records of Processing Activities (Article 30), Data Protection Impact Assessments (Article 35), Security of Processing (Article 32), and the Fulfilment of Data Subject Rights (Articles 15–17). Scholarly reviews of GDPR implementation consistently identify the discovery phase (locating and classifying personal data across systems) as the most resource-intensive and failure-prone stage of compliance (Rocha and Canedo 2025).

The Marriott International enforcement action exemplifies how deficiencies in data mapping translate into regulatory liability. The UK Information Commissioner's Office determined that Marriott failed to conduct adequate post-acquisition due diligence on Starwood's legacy systems, allowing vulnerabilities to persist undetected for years. The breach was not merely a security lapse; it was rooted in the absence of a comprehensive inventory of inherited data assets, access privileges, and encryption status. The regulator's reasoning implicitly treated data mapping as a prerequisite to both privacy by design and security by default, anchoring liability under Articles 5(1)(f) and 32 (Reuters 2020)

Judicial developments reinforce this logic. In Farley v Paymaster, the UK Court of Appeal held that administrative failures, specifically the use of outdated addresses, could constitute GDPR violations even in the absence of proof of actual data misuse. By recognizing compensable harm arising from the fear of potential misuse, the court elevated data accuracy and integrity, both outputs of effective data mapping, into litigation-relevant obligations. This jurisprudence significantly lowers the threshold for liability arising from data hygiene failures (Farley v Paymaster [2025] UKSC/2025/0185)

CCPA/CPRA and Rights-Driven Mapping Failures

Under the California Consumer Privacy Act, as amended by the CPRA, data mapping assumes a different but equally central role. The statute's expansive definition of "personal information" and its rights-based enforcement model require organizations to locate, retrieve, delete, or restrict personal data across all systems in response to consumer requests. Academic and policy analyses characterize these obligations as "difficult, if not impossible" without a mature data inventory (Illman and Temple 2019).

Regulatory enforcement illustrates how mapping failures directly undermine rights compliance. The Sephora settlement demonstrated that the inability to identify and control data flows to third-party trackers rendered opt-out mechanisms ineffective. From a technical perspective, the failure was not consent management but the absence of a detailed map linking user signals (such as Global Privacy Control) to specific data disclosures. Enforcement trends further show that businesses with fragmented or opaque data architectures impose excessive identity-verification burdens on consumers, violating data minimization principles and inviting regulatory scrutiny. (California Department of Justice 2022)

Litigation under the CCPA's private right of action similarly reflects data mapping deficiencies. Courts have allowed claims to proceed where unauthorized data disclosures occurred via cookies, pixels, or APIs, even in the absence of a traditional breach. These cases conceptualize "reasonable security" as including visibility and control over outbound data flows—functions that presuppose accurate data mapping (Baker Donelson. 2025, Skadden. 2025, Parker Poe. 2025)

Sector-specific research reinforces these findings. Studies of healthcare organizations reveal that assembling a complete inventory of patient data across clinical, billing, and analytics systems is the most complex technical hurdle in CCPA compliance, exacerbated by legacy infrastructure and poor data discovery capabilities (Mulgund et al. 2021).

LGPD and Mapping as a Measure of Organizational Maturity

Brazil's LGPD, closely inspired by the GDPR, embeds data mapping within its accountability and security framework. Empirical case studies of LGPD implementation in financial and educational institutions show that organizations struggle to translate legal requirements into operational controls due to incomplete data maps (Celidonio, Neves, and Doná 2020; de Oliveira Gatto et al.).

Methodological studies mapping LGPD controls reveal that nearly half of required controls remain unmet in practice, with deficiencies concentrated around data inventory, access management, and lifecycle documentation. These findings suggest that data mapping is not merely a compliance exercise but an indicator of institutional readiness for privacy governance. Without a system-wide view of data flows, organizations are unable to conduct risk assessments, enforce retention limits, or demonstrate lawful processing (Celidonio, 2020)

PDPA Data Mapping as Accountability Infrastructure

Singapore's PDPA approaches data mapping indirectly through its Protection Obligation and Accountability Obligation. Regulatory guidance and enforcement decisions consistently treat the absence of a personal data inventory as evidence of inadequate security arrangements (PDPC, 2020). The Eatigo International decision illustrates this approach. The organization's failure to maintain an inventory of legacy databases left millions of user records exposed, leading regulators to characterize inventory management as a prerequisite for compliance (PDPC, 2021).

PDPC guidance explicitly identifies data flow mapping as a foundational tool for Data Protection Impact Assessments and accountability documentation (PDPC Guidance, 2021). Academic literature similarly frames data flow maps as essential instruments for transparency and risk management in enterprise privacy compliance. Unlike GDPR's punitive model, Singapore's framework emphasizes demonstrable control, but the underlying operational expectation—comprehensive data mapping—is substantively similar (Ter, 2013)

Technology Responses: Automation and Unified Policy Systems

Across jurisdictions, academic and technical research converges on the conclusion that manual data mapping is unsustainable at scale. Unified Policy Management Systems and automated compliance tools propose integrating data classification, flow visualization, and policy enforcement into a single architecture (Bukhari et al. 2022). These systems aim to maintain a continuously updated data map capable of supporting rights fulfilment, security controls, and regulatory reporting.

However, comparative studies caution that such tools introduce their own complexity and cost. Implementing automated mapping requires integration across heterogeneous systems, sustained governance commitment, and skilled personnel. As with cross-border transfer compliance, data mapping increasingly shifts the compliance burden from legal interpretation to systems engineering (Rocha and Canedo 2025).

Implications for Indian Users

India's DPDP Act does not explicitly mandate data mapping, Records of Processing Activities, or DPIAs in the GDPR sense. Nonetheless, core obligations, such as purpose limitation, data minimization, accuracy, security

safeguards, and data principal rights, implicitly depend on accurate and current data maps.

India's scale, rapid digitization of public services, and continued reliance on fragmented legacy systems suggest that data mapping challenges will be amplified. Banking, telecommunications, healthcare, and government departments frequently operate hybrid environments combining modern cloud platforms with decades-old databases. Without systematic mapping, fulfilling access, correction, or erasure requests risks becoming an ad hoc exercise, increasing the likelihood of delayed or incomplete responses.

From a regulatory perspective, enforcement under DPDP is likely to mirror international patterns. Failures in data mapping will surface as security incidents, inaccurate disclosures, or rights violations. From a technology perspective, Indian organizations may be forced to invest in automated discovery and inventory tools earlier in the compliance lifecycle than their counterparts in smaller jurisdictions.

Comparative experience demonstrates that data mapping is not a preliminary compliance task but the operational core of privacy law implementation. GDPR, CCPA, LGPD, and PDPA enforcement all reveal a consistent pattern: organizations that lack visibility into their data flows are structurally incapable of complying with substantive legal obligations.

For India's DPDP regime, the lesson is clear. In the absence of explicit guidance or scalable technical solutions, data mapping will emerge as the most persistent and costly compliance failure. Treating data mapping as continuous infrastructure, rather than a one-time documentation exercise, will be essential to translating statutory privacy protections into operational reality.

"Legitimate Interest" Ambiguity

After compliance cost, cross-border transfers, and data mapping, the ambiguity surrounding "legitimate interest" (LI) has emerged as a fourth major implementation challenge in modern privacy regimes. Under the EU GDPR, Article 6(1)(f) permits processing without consent where the controller's legitimate interests are not overridden by the rights and freedoms of the data subject. This provision was designed as a flexible residual basis to enable socially and economically valuable processing without excessive reliance on consent. In practice, however, LI has proven to be one of the most litigated and contested lawful bases, precisely because it depends on a context-specific, subjective balancing test rather than bright-line rules (Hoofnagle, Van der Sloot, and Borgesius, 2019).

The resulting uncertainty has forced regulators, courts, and scholars to delineate the outer boundaries of LI, particularly for data-intensive commercial practices such as behavioural advertising, analytics, and emerging AI applications. These experiences offer important lessons for jurisdictions that have adopted, modified, or deliberately avoided a broad legitimate-interest framework.

GDPR Regulatory Pushback Against Over-Broad Legitimate Interest

The EU experience illustrates how LI ambiguity can destabilize core business models. In the high-profile enforcement actions against Meta Platforms Ireland Ltd., regulators rejected the company's attempt to rely on "contractual necessity" for personalized advertising, holding that behavioural advertising is not objectively necessary to provide a social media service. While the case formally concerned Article 6(1)(b), its implications for LI were explicit: highly intrusive, large-scale profiling is unlikely to satisfy the balancing test under Article 6(1)(f), leaving explicit consent as the only viable lawful basis (Hoofnagle et al. 2019).

The European Data Protection Board and the Irish Data Protection Commission emphasized that users must be able to access the core service without being subjected to behavioural advertising. This interpretation significantly narrowed the practical scope of LI for dominant digital platforms and culminated in

administrative fines totalling €390 million. The decision clarified that controllers cannot use flexible lawful bases to circumvent consent where processing materially affects individuals' reasonable expectations and autonomy.

From a technology perspective, this regulatory stance forced firms to redesign advertising architectures, consent flows, and data-segmentation mechanisms, demonstrating how legal ambiguity around LI directly translates into costly technical re-engineering.

KNLTB Case and Conditional Acceptance of Commercial Interests

While regulators narrowed LI's scope in practice, judicial interpretation has sought to preserve its conceptual availability. In the KNLTB (Royal Dutch Tennis Association) case (C-621/22), the Court of Justice of the European Union rejected the proposition that purely commercial interests can never qualify as legitimate interests. The Court held that commercial objectives, including marketing, may constitute legitimate interests, provided the controller satisfies the three-part test of purpose, necessity, and balancing (Kun 2025).

However, the Court simultaneously reinforced the demanding nature of the balancing exercise, stressing that data subjects' reasonable expectations and the availability of less intrusive alternatives are decisive. The judgment thus confirmed that LI remains legally permissible but operationally fragile, dependent on meticulous documentation and contextual justification. In effect, the ruling preserved LI as a lawful basis in theory while reinforcing its high compliance burden in practice.

The Subjectivity of the Balancing Test

Academic literature consistently identifies the balancing test as the core source of LI ambiguity. Comparative analyses describe legitimate interest as an "undetermined legal concept," intentionally flexible but inherently uncertain (Bamashmoos, 2025). Scholars note that there are no universally accepted metrics for weighing competing interests, leading to divergent organizational practices and uneven enforcement outcomes.

Empirical studies further show that controllers often exploit this ambiguity by invoking LI in privacy notices without performing a rigorous assessment, sometimes relying on deceptive or opaque design to discourage consent withdrawal (Kramcsak 2023). This has prompted regulators to treat the absence of a documented Legitimate Interest Assessment (LIA) as evidence of non-compliance, reinforcing accountability obligations under GDPR Article 5(2).

CCPA: Functional Analogues Without a Legitimate-Interest Doctrine

The California Consumer Privacy Act (CCPA), as amended by the CPRA, does not adopt a legitimate-interest framework. Instead, it regulates processing through opt-out rights, purpose limitation, and transparency, particularly via the concepts of "selling," "sharing," and "legitimate business purpose." While this avoids the formal ambiguity of LI, it introduces functional uncertainty in determining whether data disclosures for advertising or analytics trigger opt-out obligations.

Enforcement actions, most notably the Sephora settlement, illustrate that regulators interpret behavioural advertising and third-party tracking broadly as "sales" or "sharing," effectively limiting businesses' ability to rely on implied business necessity. Although framed differently, this mirrors the EU experience: flexible justifications for intrusive commercial processing are progressively narrowed through enforcement, compelling firms to default to consumer choice mechanisms (California Department of Justice 2022).

PDPA - Legitimate Interests with Structured Accountability

Singapore's Personal Data Protection Act (PDPA) introduced a Legitimate Interests Exception in its 2020 amendments, explicitly to reduce over-reliance on consent. Unlike the GDPR, the PDPA embeds LI within a statutory framework that requires organizations to conduct and document a structured assessment demonstrating that legitimate interests outweigh residual adverse effects on individuals (Chik 2022).

Regulatory guidance provides a detailed checklist for this assessment, and early enforcement decisions illustrate the Commission's approach. In the RedMart decision, the Personal Data Protection Commission accepted the use of LI for collecting identification photographs in a warehouse security context, emphasizing the presence of mitigation measures such as access controls and strict retention limits. The decision demonstrates that LI can succeed where organizations implement robust safeguards and can evidence proportionality, reinforcing accountability rather than formal consent.

From a systems perspective, this approach demands internal risk-assessment tooling, documentation workflows, and data-minimization controls, aligning LI with operational governance rather than discretionary business judgment.

LGPD and the Narrowing of Legitimate Interest

LGPD closely mirrors the GDPR's LI provision in Article 7(IX), supplemented by Article 10's enhanced transparency requirements. Regulatory guidance from the Brazilian National Data Protection Authority (ANPD) has emphasized that LI cannot be used for sensitive data and that controllers must clearly demonstrate compatibility with data subjects' expectations (de Bastos, Bassi, and Cassi 2021).

Recent regulatory actions, including the ANPD's scrutiny of Meta's reliance on LI for AI training, indicate a narrowing trajectory similar to the EU's. The Authority questioned whether large-scale, non-obvious processing could ever meet the necessity and expectation criteria, signalling that innovative or high-risk data uses are unlikely to survive the balancing test. Academic commentary characterizes LI under the LGPD as legally available but strategically risky, pushing organizations toward explicit consent or more specific legal bases (de Pinho Gomes 2024).

Implications for Indian Scenario

India's DPDP Act adopts a markedly different approach. Instead of a broad legitimate-interest clause, it defines specific "Legitimate Uses" under Clause 7, primarily covering employment, medical emergencies, public interest, and state functions. Private commercial activities are largely excluded from these exceptions, effectively forcing reliance on consent for most data-driven business models.

This design choice significantly reduces interpretive ambiguity for private entities but shifts complexity elsewhere. From a legal perspective, Indian firms face a narrower set of non-consensual processing options, limiting flexibility compared to GDPR or LGPD regimes. From a technology perspective, this necessitates scalable consent-management systems, fine-grained purpose controls, and continuous monitoring of consent validity.

However, the comparative experience suggests a trade-off: by avoiding a broad LI clause, India reduces litigation and enforcement uncertainty associated with subjective balancing tests, at the cost of reduced adaptability for emerging data uses. As global experience shows, legitimate-interest ambiguity often resolves not through doctrinal clarity but through costly enforcement and architectural change. India's model pre-empts this trajectory by design.

Discussion

The findings of this study reinforce a growing consensus in comparative privacy scholarship that the effectiveness of data protection regimes is determined less by doctrinal design than by implementation architecture. Across jurisdictions, privacy compliance consistently manifests as a systems-governance challenge shaped by cost structures, technical dependencies, and organizational data complexity. The four implementation challenges identified, cost of compliance, cross-border data transfers, data mapping, and ambiguity in lawful bases, are not isolated problems but mutually reinforcing constraints that shape regulatory outcomes.

The study's emphasis on compliance costs aligns with prior economic analyses of the GDPR and CCPA, which demonstrate that privacy regulation operates primarily through increased fixed costs rather than reduced revenues (Frey and Presidente 2024; Gupta, McGowan, and Ongena 2024). This paper extends that literature by showing that these costs are not merely transitional but architectural, arising from the need to retrofit legacy systems and maintain continuous governance processes. In this respect, the findings corroborate Goldfarb and Que's (2023) argument that privacy regulation alters firms' production functions by embedding compliance into core information infrastructures.

The analysis of cross-border data transfers situates India's DPDP Act within ongoing debates on regulatory fragmentation and digital trade. Prior scholarship has focused on the extraterritorial reach of the GDPR and the destabilizing effects of Schrems II on global data flows (Mattoo and Meltzer 2018). This study contributes by highlighting that uncertainty, rather than outright restriction, is the primary risk vector. India's negative-list approach reduces immediate barriers but introduces latent regulatory risk, suggesting that clarity and predictability may be as important as formal permissiveness. These finding complements comparative governance analyses that emphasize regulatory coherence over stringency (Coche, Kolk, and Ocelík 2024).

The centrality of data mapping identified in this study is consistent with empirical and doctrinal research showing that failures in inventory and flow visibility underlie many enforcement actions across regimes (Sirur, Nurse, and Webb 2018). However, this paper advances the literature by reframing data mapping not as a compliance deliverable but as an indicator of institutional readiness for privacy governance. In this sense, the findings resonate with accountability-oriented models observed in Singapore, where regulators treat the absence of data inventories as evidence of deficient organizational control rather than isolated technical lapses (Chik 2022).

The discussion of lawful-basis ambiguity contributes to ongoing debates on the role of "legitimate interest" in privacy law. Prior analyses have documented the subjectivity and litigation risks inherent in balancing tests under GDPR and LGPD (Hoofnagle, Van der Sloot, and Borgesius 2019; Kramcsak 2023). This study highlights that India's deliberate avoidance of a broad legitimate-interest clause may reduce legal uncertainty but shifts the compliance burden toward scalable consent architectures. This trade-off suggests that statutory clarity does not eliminate complexity but redistributes it across legal and technical domains.

Several limitations of the study should be acknowledged. First, the analysis relies on secondary sources and comparative synthesis rather than primary empirical data from Indian organizations, which may limit the granularity of implementation insights. Second, the study focuses primarily on formal regulatory and economic outcomes, potentially underrepresenting informal compliance practices and sector-specific adaptations. Third, comparative inference necessarily abstracts from jurisdiction-specific institutional contexts, which may affect the transferability of certain lessons.

Future research could address these gaps by empirically examining DPDP implementation across sectors such as fintech, healthcare, and public digital infrastructure. Longitudinal studies assessing compliance costs

over time in India would be particularly valuable. Additionally, further work is needed on privacy-enhancing technologies, automated compliance systems, and the role of regulatory sandboxes in reducing implementation friction. As privacy regulation increasingly converges with digital governance, interdisciplinary research integrating law, economics, and systems engineering will be essential to inform both policy and practice.

Conclusion: From Legal Obligation to Privacy Architecture in India

This study has demonstrated that the implementation of contemporary privacy regimes is shaped less by doctrinal novelty than by four recurring structural constraints - the cost of compliance, cross-border data transfer friction, data-mapping complexity, and the ambiguity of flexible lawful bases such as legitimate interest. Comparative evidence from the GDPR, CCPA/CPRA, LGPD, and PDPA shows that these challenges interact cumulatively, transforming privacy law from a rules-based obligation into an architectural problem that must be solved through organizational design and technology systems rather than legal interpretation alone.

Cost of Compliance as an Architectural Variable

Across jurisdictions, compliance costs emerge as fixed and front-loaded, driven by investments in specialist personnel, IT re-architecture, and continuous audit readiness (Frey and Presidente 2024; Koski and Valmari 2020). These costs are not episodic but structural, reshaping firm behaviour and market dynamics. The implication for India is clear. DPDP compliance cannot be treated as a marginal legal expense. Instead, Indian firms must internalize privacy as a core systems cost, comparable to cybersecurity or financial controls.

Indian organizations should adopt privacy-by-design platforms that integrate consent management, security controls, and audit logging at the infrastructure level. Modular compliance architectures, where identity, consent, retention, and breach response are reusable services rather than bespoke workflows, can amortize compliance costs across business units and reduce long-term expenditure. Open standards for consent signalling and rights fulfilment are particularly critical for SMEs, which lack scale advantages enjoyed by large multinationals.

Cross-Border Transfers and the End of Legal Certainty

The second constraint concerns cross-border data transfers, where the collapse of transfer certainty under GDPR post-Schrems II illustrates how legal rules can destabilize global cloud architectures (Mattoo and Meltzer 2018; Lin 2024). Although India's DPDP Act adopts a negative-list ("blacklisting") approach under Section 16, comparative experience suggests that regulatory uncertainty, rather than formal prohibition, will be the dominant risk. Indian firms may be DPDP-compliant while simultaneously breaching foreign obligations when EU or other extraterritorial data is involved.

Indian companies should implement jurisdiction-aware data-flow controls. Technically, this entails tagging datasets by origin and regulatory exposure, enforcing policy-based routing, and deploying encryption and key-management schemes that can be adapted to foreign surveillance-risk assessments. Automated compliance engines, capable of visualizing data flows and enforcing destination-specific constraints, are increasingly essential. Such systems allow firms to respond dynamically to regulatory changes without repeated legal re-engineering, shifting compliance from ex post review to real-time governance.

Data Mapping as the Operational Core of Compliance

The third and most operationally destabilizing challenge is data mapping. Enforcement experience under GDPR, CCPA, LGPD, and PDPA demonstrates that failures in data inventory and flow visibility surface

indirectly as security breaches, rights-fulfilment failures, or accountability violations (Illman and Temple 2019; Rocha and Canedo 2025). Data mapping is therefore not a preliminary exercise but the continuous infrastructure upon which all other obligations depend.

For India, this challenge is amplified by scale, legacy systems, and fragmented digitization, particularly in banking, telecommunications, healthcare, and government services. Without accurate and continuously updated maps of personal data, Indian firms will struggle to fulfil access, correction, and erasure requests within statutory timelines, increasing enforcement exposure.

Indian organizations should invest in automated discovery and classification tools that maintain live data inventories across structured and unstructured environments. Unified Policy Management Systems, integrating data classification, flow visualization, and policy enforcement, offer a scalable solution (Bukhari et al. 2022). Crucially, data mapping must be embedded into change-management processes: mergers, system migrations, and vendor onboarding should trigger mandatory remapping and risk review. Treating data maps as static documentation guarantees obsolescence; treating them as operational telemetry enables sustainable compliance.

Legitimate-Interest Ambiguity and the Indian Design Choice

The fourth challenge—legitimate-interest ambiguity—illustrates the cost of legal flexibility. Under GDPR and LGPD, the subjective balancing test inherent in legitimate interest has generated regulatory conflict, litigation, and costly redesigns of advertising and analytics systems (Hoofnagle, Van der Sloot, and Borgesius 2019; Kramcsak 2023). Singapore's PDPA demonstrates a more structured approach, but still requires extensive documentation and mitigation measures (Chik 2022).

India's DPDP Act deliberately avoids a broad legitimate-interest clause for private entities, opting instead for narrowly defined "Legitimate Uses" under Clause 7. This design reduces interpretive uncertainty but shifts the burden onto consent-centric architectures.

Indian firms must therefore build scalable consent-lifecycle management systems. These systems should support granular purpose binding, consent versioning, withdrawal propagation, and downstream enforcement across vendors and processors. Consent should not be implemented as a front-end checkbox but as a back-end control plane that governs data access and processing logic. Where legitimate uses apply (e.g., employment or emergencies), firms should maintain internal assessment documentation analogous to Legitimate Interest Assessments, both to demonstrate accountability and to future-proof against regulatory expansion.

Privacy as Systems Engineering

Taken together, the four challenges converge on a single conclusion: privacy compliance has become a systems-engineering problem. Legal compliance without architectural alignment produces unsustainable costs, operational fragility, and enforcement risk. Conversely, jurisdictions that emphasize accountability and demonstrable control, such as Singapore, illustrate how regulatory objectives can be met with greater predictability and lower friction.

For India, the DPDP Act's success will depend less on statutory text than on implementation pathways. If enforcement emphasizes ex post penalties without encouraging privacy-by-design adoption, compliance costs will escalate unevenly, disadvantaging SMEs and innovation-driven sectors. Conversely, regulatory guidance that recognizes automated governance systems, standardized consent frameworks, and risk-based enforcement can distribute costs more equitably and enhance substantive privacy outcomes.

Policy and Industry Implications

From a policy perspective, Indian regulators should consider issuing technical codes of practice that clarify acceptable architectures for consent management, data mapping, and cross-border risk mitigation. Safe-harbour provisions for firms adopting certified privacy-engineering frameworks could further reduce defensive over-spending. From an industry perspective, boards and senior management must recognize privacy as a strategic infrastructure investment, not a compliance afterthought.

In conclusion, the comparative evidence shows that privacy law implementation fails when treated as a purely legal exercise. It succeeds when translated into durable technical architecture. For India's DPDP regime, embracing this lesson early offers the opportunity to avoid the cost spirals and regulatory uncertainty experienced elsewhere, while embedding privacy governance into the digital foundations of its economy.

Conflict of Interest Statement

The authors declares that there are no known financial interests, personal relationships, or institutional affiliations that could have influenced the research reported in this study.

Ethics Statement

This study did not involve human participants, animals, or the use of identifiable personal data. Ethical approval and informed consent were therefore not required.

Funding

The authors have received no financial support for the research, authorship and publication of this article

References

"ICO Fines Marriott International, Inc. £18.4 million for Security Breach." GDPRRegister.eu. Accessed via GDPRRegister. https://www.gdprregister.eu/news/ico-fine-marriot/

Baker Donelson. 2025. "Recent CCPA Decision Portends Potential Expansion of Class Action Liability Exposure for Cookies, Pixels, and Tracking Technologies." Baker Donelson Publications, May 2, 2025. https://www.bakerdonelson.com/recent-ccpa-decision-portends-potential-expansion-of-class-action-liability-exposure-for-cookies-pixels-and-tracking-technologies

Bamashmoos, Ahmed M. 2025. "The Legal Framework of Legitimate Interests: A Comparative Analysis." Scientific Journal of King Faisal University, Humanities & Management Sciences 26 (2).

Brizolla, Maria Margarete Baccin, Neusa Maria Gonçalves Salla, Arielli Castanho Da Silva, Jéssica Estela Bender, and Grace Kelly Holtz Scremin. "EFFECTS OF THE GENERAL DATA PROTECTION LAW (LGPD) ON FOR-PROFIT ORGANIZATIONS." Revista de Gestão Social e Ambiental 18, no. 11 (2024): 1-15.

Bukhari, Tahir Tayor, Oyetunji Oladimeji, Edima David Etim, and Joshua Oluwagbenga Ajayi. 2022. "Harmonizing International Data Privacy Standards Through Unified Policy Management Systems." Journal of Data Privacy 5 (1): 88–104.

California Department of Justice. 2022. "Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act." August 24, 2022.

https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement

Celidonio, Tiago, Paulo Sergio Neves, and Claudio Melim Doná. 2020. "Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil Número 13.709/18) e sua adequação perante a lei em uma instituição financeira — Um estudo de caso." Brazilian Journal of Business 2 (4): 3626–3648. https://ojs.brazilianjournals.com.br/index.php/BJB/article/view/18382

Chik, Warren B. 2022. "The Reasonableness Standard of Compliance in the Singapore Personal Data Protection Act." Singapore Academy of Law Journal 34: 352–380

Coche, Eugénie, Ans Kolk, and Václav Ocelík. 2024. "Unravelling Cross-Country Regulatory Intricacies of Data Governance." Journal of International Business Policy 7 (1): 112–127.

de Bastos, Fernanda Aline, Maria Carolina Poholink Cabral Bassi, and Guilherme H. Galino Cassi. 2021. "Legítimo Interesse como Excludente de Responsabilidade Civil à Luz da LGPD." Brazilian Journal of Development 7 (7): 71582–71607

de Lucena, Beluze Andrade, I. V. B. W. Neves, Juliana Barbosa de Alcântara, Maria Emilia Camarago, and Aprígio Teles Mascarenhas Neto. "Systematic review in the implementation of the general data protection law in Brazil." Multidisciplinary studies: management and legal Sciences (2024): 20.

de Magalhães, Marcus Abreu. 2021. "Data Protection Regulation: A Comparative Law Approach." International Journal of Digital Law 2 (2): 33–53.

de Oliveira Gatto, Dacyr Dante, Nityananda Portellada, Maria Sheila Carneiro, Maria Fátima Baptista Marques, and Renato José Sassi. 2025. "Data Mapping and Data Inventory of Children and Adolescents: Identification of Critical Points in the Process of Compliance with LGPD in an Educational Institution." Observatório de la Economía Latinoamericana 23 (1): e8629. https://doi.org/10.55905/oelv23n1-094

de Pinho Gomes, Rodrigo Dias. 2024. Legítimos Interesses na LGPD—Trajetória, Consolidação e Critérios de Aplicação. São Paulo: Editora Foco

Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. "Special strict civil liability in Brazil's General Data Protection Law." Brazilian Journal of Law, Technology and Innovation 2, no. 2 (2024): 98-128.

Farley v Paymaster (1836) Ltd [2025] UKSC/2025/0185 (United Kingdom Supreme Court). https://www.supremecourt.uk/cases/uksc-2025-0185

Frey, Carl Benedikt, and Giorgio Presidente. 2024. "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally." Economic Inquiry.

Garlie, Michael. 2020. California Consumer Privacy Act of 2018: A Study of Compliance and Associated Risk. Utica College.

Goldfarb, Avi, and Verina F. Que. 2023. "The Economics of Digital Privacy." Annual Review of Economics 15: 267–286.

Gomes, Sofia Mira Pereira Jesus. 2024. EU Personal Data Protection Standards Beyond Its Borders. Master's thesis, ISCTE–Instituto Universitário de Lisboa.

Gupta, Manish, Danny McGowan, and Steven Ongena. 2023. "The Cost of Privacy: The Impact of the California Consumer Protection Act on Mortgage Markets." SSRN.

Gupta, Manish, Danny McGowan, and Steven Ongena. 2024. "The Cost of Data Privacy Law." Swiss Finance Institute Research Paper 23–25

Hoofnagle, Chris Jay, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius. 2019. "The European Union General Data Protection Regulation: What It Is and What It Means." Information & Communications Technology Law 28 (1): 65–98

Illman, Erin, and Paul Temple. 2019. "California Consumer Privacy Act." The Business Lawyer 75 (1): 1637–1646.

Khan, Md Nazrul Islam. 2025. "Cross-Border Data Privacy and Legal Support." SSRN.

Koski, Heli, and Nelli Valmari. 2020. Short-Term Impacts of the GDPR on Firm Performance. ETLA Working Papers No. 77.

Kramcsak, Pablo Trigo. 2023. "Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?" Computer Law & Security Review 48: 105765.

Kun, Eyup. "Searching for the appropriate legal basis for personal data processing for cybersecurity purposes under the NIS 2 Directive: Legal obligation and/or legitimate interest?" Computer Law & Security Review 56 (2025): 106098.

Lin, Yiran. 2024. "More Than an Enforcement Problem." Columbia Journal of Transnational Law 62 (1).

Mattoo, Aaditya, and Joshua P. Meltzer. 2018. "International Data Flows and Privacy." Journal of International Economic Law 21 (4): 769–789.

Mercurio, Bryan, and Ronald Yu. Regulating Cross-Border Data Flows: Issues, Challenges and Impact. Anthem Press, 2022.

Ministry of Electronics and Information Technology. 2025. Digital Personal Data Protection Rules, 2025. New Delhi: Government of India. PDF accessed from Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Ministry of Law and Justice. 2023. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Government of India. PDF accessed from Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Mulgund, Pavankumar, Banashri Pavankumar Mulgund, Raj Sharman, and Raghvendra Singh. 2021. "The Implications of the California Consumer Privacy Act on Healthcare Organizations." Health Policy and Technology 10 (3): 100543.

Parker Poe. 2025. "Court Expands Scope of Private Actions Under California CCPA to Include Tracking Pixels." Parker Poe Privacy Law Update, April 29, 2025. https://www.parkerpoe.com/news/2025/04/court-expands-scope-of-private-actions-under-california

Pazhohan, Helia. 2023. "Global Data Protection Standards." Legal Studies in Digital Age 2 (3): 1–12.

"Personal Data Protection Commission (PDPC). 2020. Advisory Guidelines on Key Concepts in the Personal Data Protection Act. Singapore: PDPC.

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts-in-the-PDPA-1-Oct-2020.pdf

"Personal Data Protection Commission (PDPC). 2021. Grounds of Decision: Eatigo International Pte. Ltd. Case No. DP-2010-B7267.

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Decisions/2021/20210428_Eatigo_Grounds-of-Decision.pdf

Personal Data Protection Commission (PDPC). 2021. Guide to Data Protection Impact Assessments. Singapore: PDPC.

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Protection-Impact-Assessments.pdf

Rocha, Lucas Dalle, and Edna Dias Canedo. 2025. "Optimizing Compliance: Comparative Study of Data Laws and Privacy Frameworks." Journal of Internet Services and Applications 16, no. 1: 431–452. https://doi.org/10.5753/jisa.2025.5247

Sirur, Surya, Jason R. C. Nurse, and Helena Webb. 2018. "Are We There Yet?" In Proceedings of the 2nd International Workshop on Privacy Engineering.

Skadden. 2025. "District Court Rulings Could Signal Expansion of California Consumer Privacy Right of Action." Skadden Insights

https://www.skadden.com/insights/publications/2025/04/district-court-rulings-could-signal-expansion

Ter, Kah Leng. 2013. "Singapore's Personal Data Protection Legislation: Business Perspectives." Computer Law & Security Review 29 (3): 264–273. https://doi.org/10.1016/j.clsr.2013.03.002"

Yallen, Jordan. 2019. "Untangling the Privacy Law Web." Loyola of Los Angeles Law Review 53: 787–824.

Yuan, Bocong, and Jiannan Li. 2019. "The Policy Effect of the GDPR on the Digital Public Health Sector." International Journal of Environmental Research and Public Health 16 (6): 1070.

Zhuang, Z., et al. 2024. "A Compliance Management System for Cross-Border Data Transfers." arXiv:2412.08993.