IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

The Litigation Of Ambiguity In Data Privacy Law: Why India Rejected Legitimate Interest And What It Means For System Design

Varun N. Rao (ORCiD 0000-0003-0452-1463),
Narendra Vijayasimha (ORCiD 0009-0003-9205-8882)
Rezorce Research Foundation, 111/1 II Floor 6th Main Malleswaram Bangalore 560003 India

ABSTRACT

The concept of "legitimate interest" has emerged as one of the most contested and operationally fragile legal bases in modern data protection law. Across jurisdictions, it was intended to provide flexibility for data controllers while safeguarding individual rights through proportionality and balancing. This paper demonstrates, through a comparative analysis of the European Union, Singapore, United States, and Brazil, that legitimate interest has instead become a persistent source of legal ambiguity, enforcement volatility, and architectural cost. In rights-centric regimes such as the EU and Brazil, ambiguity has been resolved through litigation and regulatory narrowing, generating high documentation and compliance burdens. In Singapore, administrative guidance and accountability frameworks have contained, but not eliminated, uncertainty. In United States, the absence of lawful bases has displaced ambiguity into definitional disputes and technical opt-out enforcement.

Against this backdrop, India's Digital Personal Data Protection Act, 2023 represents a deliberate regulatory rupture. By rejecting a general legitimate interest clause and introducing a closed list of "certain legitimate uses," the DPDP Act trades contextual flexibility for legal certainty and administrative predictability. The paper argues that this shift does not eliminate ambiguity but relocates it from legal interpretation to system architecture. Building on this insight, the paper develops concrete technology and governance strategies like consent-centric design, purpose-bound data pipelines, compliance-by-design, and auditability-first architectures, necessary to operationalize the DPDP regime. The analysis concludes that sustainable privacy governance depends less on doctrinal elegance than on the capacity of legal systems to align regulatory design with technical implementation realities.

KEYWORDS

Legitimate Interest; Digital Personal Data Protection Act (DPDP Act); Privacy by Design; Data Protection Architecture; Comparative Privacy Law

I. *INTRODUCTION*

Modern data protection regimes increasingly recognize that exclusive reliance on consent is incompatible with high-frequency, large-scale data processing environments. Digital platforms, data-driven services, and automated decision systems require lawful processing grounds that can operate continuously without imposing excessive interaction costs on individuals. In this context, the "legitimate interest" (LI) construct, most prominently articulated in Article 6(1)(f) of the GDPR, was intended to function as an operational safety valve, enabling processing where organizational interests are balanced against individual rights. From a systems perspective, LI represents an attempt to encode proportionality and contextual reasonableness into the legal layer of data-processing architectures.

In practice, however, LI has emerged as one of the most implementation-fragile elements of contemporary privacy law. The requirement to conduct a purpose, necessity, and balancing assessment introduces a high degree of subjectivity that resists automation and standardization. Within the European Union, regulatory enforcement has progressively narrowed the viable scope of LI, particularly for data-intensive activities such as behavioural advertising, profiling, and cross-context analytics. Supervisory authorities have repeatedly emphasized that processing which is structurally intrusive or economically central to a platform's business model is unlikely to satisfy the balancing threshold. As a result, organizations face significant uncertainty when attempting to encode LI into production data pipelines, often defaulting to consent as a risk-mitigation strategy despite its known scalability limitations.

Comparable implementation challenges arise in jurisdictions that do not formally recognize LI but regulate analogous activities through functional equivalents. In California, the CCPA and CPRA replace lawful-basis analysis with obligations tied to "selling," "sharing," and "legitimate business purposes." While this removes the need for subjective balancing tests, it shifts compliance complexity toward data-flow classification, real-time opt-out enforcement, and vendor contract controls. From an information-systems standpoint, the ambiguity does not disappear; rather, it migrates from legal interpretation to technical enforcement logic embedded in consent management platforms, tagging systems, and API-level controls.

Singapore's PDPA offers a more explicitly risk-engineered model. The legitimate interests' exception introduced in 2020 is viable only when organizations can demonstrate concrete mitigation measures, restricted access controls, retention limits, and documented internal assessments. This approach aligns LI with accountability-by-design principles, effectively treating it as a governance mechanism that must be supported by verifiable system safeguards. Brazil's LGPD mirrors the European LI framework but further amplifies implementation burdens through heightened transparency obligations and regulatory scrutiny of emerging uses such as AI training and large-scale analytics.

India's Digital Personal Data Protection Act represents a deliberate architectural departure from these models. The DPDP Act does not adopt an open-ended legitimate interest test for private entities. Instead, it introduces narrowly defined "legitimate uses" under Section 7, largely confined to employment-related purposes, state functions, and specified public-interest activities. The DPDP Rules (2025) reinforce this design by emphasizing notice, consent management, purpose limitation, and data minimization obligations for most private-sector processing. While this substantially reduces legal ambiguity, it shifts the compliance burden toward consent orchestration, auditable purpose binding, and lifecycle controls within information systems. Consequently, India's approach trades interpretive uncertainty for engineering complexity, making scalable consent architectures, automated retention enforcement, and policy-driven data access controls central to DPDP implementation.

In aggregate, cross-jurisdictional experience suggests that legitimate interest ambiguity is not merely a legal problem but a systems-design constraint. Where lawful bases rely on subjective balancing, compliance costs manifest as uncertainty and enforcement risk; where such bases are removed or constrained, costs reappear as architectural and operational overhead. Effective privacy governance therefore requires treating lawful-basis selection as a design decision embedded within data-processing systems, rather than as a purely legal abstraction.

II. MATERIALS AND METHODS

This study adopts a qualitative, comparative, doctrinal–policy research design with a strong emphasis on technology governance and information-systems implementation. The research is non-experimental and observational, relying exclusively on secondary sources rather than primary data collection or human subjects. The objective is not to test statistical hypotheses, but to analyse how ambiguity in lawful bases, particularly "legitimate interest", translates into implementation risk, compliance cost, and system-level complexity across jurisdictions.

2.1 Materials

Research materials were selected using purposive sampling, focusing on sources that directly address the operationalization of privacy law within digital systems. The dataset includes:

- peer-reviewed legal and economic scholarship examining the GDPR, CCPA/CPRA, LGPD, and Singapore PDPA;
- official regulatory enforcement decisions and guidance issued by supervisory authorities;
- judicial rulings interpreting lawful bases for personal data processing; and
- policy briefs and technical studies addressing privacy-by-design, compliance automation, and data governance architectures.

Sources were evaluated for relevance to implementation cost, lawful-basis uncertainty, accountability mechanisms, and cross-border data governance, ensuring alignment with an applied information-systems perspective (Voigt and von dem Bussche 2017; Solove and Schwartz 2023).

2.2 Analytical Procedure

The analysis proceeded in four stages. First, recurring implementation challenges associated with lawful-basis ambiguity were identified across jurisdictions. Second, jurisdiction-specific legal and regulatory evidence was synthesized to assess how these challenges manifest in enforcement practice. Third, the findings were mapped onto the statutory structure of India's Digital Personal Data Protection (DPDP) Act and the DPDP Rules (2025), with particular attention to consent management and "legitimate uses." Finally, the study derived architectural and governance implications for privacy-compliant system design.
The study employs comparative legal analysis, thematic synthesis, and policy-oriented qualitative reasoning. Empirical findings from cited economic and regulatory studies are incorporated descriptively to support implementation-focused conclusions rather than statistical inference (Bioni 2020; European Data Protection Board 2022).

III. CONCEPTUAL FOUNDATIONS: LEGITIMATE INTEREST AS A LEGAL CONSTRUCT

Legitimate interest occupies a distinctive position within contemporary data protection theory as a lawful basis that explicitly institutionalizes normative balancing. Unlike consent or legal obligation, legitimate interest permits personal data processing based on a controller's asserted necessity, subject to proportionality and safeguards. Early doctrinal work under Directive 95/46/EC conceptualized legitimate interest not as an automatic authorization, but as legitimacy contingent on the appropriateness of protection afforded to the data subject (Balboni et al. 2013). This conceptual separation, between the justification for processing and the level of protection required, remains central under Article 6(1)(f) of the GDPR.

The now-standard three-part test (purpose legitimacy, necessity, and balancing) has been repeatedly affirmed in EU scholarship and case law (Kamara and De Hert 2018). A critical element within this framework is the data subject's "reasonable expectations," which operate as a proxy for contextual fairness. Proportionality thus becomes the governing principle. Even lawful commercial interests may fail where processing exceeds what is contextually anticipated or minimally required.

Comparable theoretical constructs appear outside the EU, albeit under different doctrinal labels. In Singapore, the Personal Data Protection Act's "legitimate interests" exception similarly requires a structured assessment of necessity, adverse impact, and mitigation, embedding proportionality and expectation management into statutory design. In Brazil, Article 10 of the LGPD mirrors the GDPR's balancing logic, explicitly tying legitimate interest to transparency and data subject awareness. These convergences suggest that legitimate interest reflects a broader global attempt to reconcile data-driven innovation with rights-based governance, rather than a uniquely European construct.

3.1 Structural Sources of Ambiguity

Despite its theoretical coherence, legitimate interest is marked by structural ambiguity across jurisdictions. The most persistent source of uncertainty lies in the subjectivity of the balancing exercise. Data protection frameworks rarely specify how competing interests should be weighted or what degree of harm is acceptable. Ferretti (2014) characterizes this indeterminacy as an intentional feature of modern data protection law, reflecting its evolution from strict privacy protection toward a broader governance regime concerned with data power asymmetries.

A second source of ambiguity arises from the temporal mismatch between ex-ante assessments and ex-post enforcement. Controllers are required to document legitimate interest assessments prospectively, yet regulators and courts evaluate these decisions retrospectively, often under changed social, technological, or political expectations. This dynamic is evident not only in the EU, but also in Brazil, where the LGPD's legitimate interest clause has been narrowed through regulatory guidance emphasizing unforeseen secondary uses, such as advanced analytics or AI training (Bioni 2020).

In the United States, where no formal legitimate interest doctrine exists, analogous ambiguity emerges through the interpretation of "legitimate business purpose" and data-sharing constructs under the CCPA and CPRA. Although framed differently, these concepts similarly require contextual judgment and invite regulatory reinterpretation, reinforcing the view that ambiguity is inherent wherever proportionality-based privacy governance is attempted.

3.2 Legitimate Interest versus Consent and Contractual Necessity

Across jurisdictions, legitimate interest has increasingly functioned as a substitute for consent and contractual necessity, particularly in environments where consent is operationally costly or contracts do not strictly require contested processing. Scholars consistently caution, however, that this substitution was never intended to be comprehensive. Legitimate interest was designed to address residual processing contexts, such as fraud prevention, security, or limited marketing,rather than to legitimize core revenue models or highly intrusive practices (Mihăilă and Mihăilă 2020; Niedermeier and Mpame 2019).

Regulatory pushback against overreliance on legitimate interest has therefore emerged globally, albeit through different mechanisms. In the EU and Brazil, this pushback manifests through restrictive interpretations of balancing and necessity. In Singapore, it appears through stringent mitigation and accountability requirements. In the United States, it surfaces via opt-out mandates and enforcement against expansive interpretations of business necessity. Collectively, these experiences suggest that legitimate interest operates less as a deregulatory escape from consent and more as a constrained governance tool whose ambiguity reflects the unresolved tension between scalable data processing and individual rights.

IV. GDPR AND THE LITIGATION OF AMBIGUITY

The GDPR adopts a principles-based legislative design that deliberately leaves key concepts open-ended. Article 6(1)(f), which permits processing based on the "legitimate interests" of the controller, exemplifies this approach. Rather than enumerating permissible purposes, the provision embeds a structured balancing framework that requires controllers to justify processing through necessity and proportionality. Early scholarship emphasized that legitimate interest was never intended as an automatic authorization, but as a conditional legal basis grounded in the adequacy of protection afforded to data subjects (Balboni et al. 2013). This design choice shifted interpretive authority from legislators to regulators and courts, making litigation a central mechanism for operationalizing GDPR norms.

4.1 Regulatory Narrowing Through Enforcement

Regulatory practice has progressively narrowed the scope of legitimate interest, particularly in the context of behavioural advertising and large-scale profiling. Online behavioural advertising (OBA) relies on pervasive tracking, inferred data, and cross-context aggregation, placing it in tension with core GDPR principles such as data minimization and purpose limitation (Forward 2024; Galli and Sartor 2024). Supervisory authorities have consistently questioned whether such practices can ever satisfy the necessity and balancing requirements of Article 6(1)(f), especially when less intrusive alternatives, such as contextual advertising, are available.

Empirical research supports this regulatory stance, showing that GDPR enforcement has disproportionately curtailed privacy-invasive tracking technologies while leaving less intrusive data practices largely unaffected (Lukić, Miller, and Skiera 2024). Legal analyses further highlight that algorithmic targeting mechanisms, particularly those involving minors or sensitive inferred attributes, undermine the assumption that users reasonably expect such processing as part of ordinary service provision (Basarudin and Raji 2022; Kant 2021). As a result, supervisory authorities have treated legitimate interest claims in advertising contexts with increasing scepticism, effectively pushing controllers toward explicit consent.

4.2 Judicial Clarification: Commercial Interest and Its Limits

Judicial interpretation by the Court of Justice of the European Union (CJEU) has reinforced this regulatory narrowing while preserving legitimate interest as a concept in principle. The Court has repeatedly affirmed that commercial interests may qualify as legitimate, but only when they survive strict necessity and balancing scrutiny (Petrašević and Ćosić 2023). In practice, this has meant that economically central processing activities, such as mass profiling or cross-service data consolidation, are unlikely to pass the balancing test when they materially interfere with fundamental rights.

Recent case law further illustrates how the litigation of ambiguity extends beyond Article 6 to adjacent principles such as fairness and accountability. The Court has increasingly emphasized power asymmetries, reasonable expectations, and substantive user choice, signalling a shift from procedural compliance toward values-based evaluation. This jurisprudence confirms that legitimate interest cannot be assessed in isolation, but must be read in conjunction with the GDPR's broader normative architecture.

4.3 Compliance Consequences: Documentation, Auditability, and Accountability

One of the most significant consequences of this litigation-driven clarification is the expansion of documentation and auditability obligations. Reliance on legitimate interest now requires a formal Legitimate Interest Assessment (LIA), documenting purpose legitimacy, necessity, risk evaluation, and mitigation measures (Kamara and De Hert 2018; Bamashmoos 2025). These requirements operationalize the accountability principle, transforming legal ambiguity into a sustained compliance burden.

From a governance perspective, accountability has evolved into a demand for verifiable, system-level evidence of compliance rather than mere declaratory statements (Alhadeff, Van Alsenoy, and Dumortier 2012). Technical tools such as structured data inventories and accountability systems have emerged to support this obligation, reflecting the GDPR's shift toward auditable compliance infrastructures (Becker et al. 2019). Consequently, the EU experience demonstrates that the ambiguity of legitimate interest does not reduce regulatory burden; instead, it redistributes compliance costs toward continuous documentation, monitoring, and justification within organizational data systems.

V. *MANAGED FLEXIBILITY UNDER THE PDPA*

Singapore's 2020 amendments to the Personal Data Protection Act (PDPA) marked a decisive shift away from a predominantly consent-centric regulatory model toward a more flexible, accountability-oriented framework. Prior to these amendments, organizations were generally required to obtain consent unless narrow deemed-consent exceptions applied, a structure increasingly viewed as economically inefficient and operationally rigid in data-intensive environments (Lim 2024). The introduction of the "legitimate interests" exception in the First Schedule represented a structural recalibration, allowing organizations to collect, use, or disclose personal data without consent where their legitimate interests outweigh any adverse effect on the individual (Chik 2022).

This reform was explicitly motivated by concerns that excessive reliance on consent risked transforming compliance into a bureaucratic exercise detached from substantive risk management. By introducing legitimate interests alongside expanded deemed-consent mechanisms, Singapore repositioned compliance responsibility onto organizations, requiring them to justify processing decisions through documented assessments rather than transactional consent collection (Lim 2024). In this sense, the PDPA amendments reflect a regulatory philosophy that treats lawful processing as a function of governance quality rather than formalistic authorization.

5.1 Statutory Balancing Test and PDPC Guidance

The legitimate interests exception under the PDPA is structured around a statutory balancing test that closely parallels, but does not replicate, the GDPR model. Organizations must demonstrate that their legitimate interests (or those of a third party) clearly outweigh any likely adverse effects on individuals, and must implement measures to mitigate foreseeable harm (Chik 2022). Unlike the GDPR, the PDPA embeds this balancing logic within a broader reasonableness standard, emphasizing contextual judgment over abstract rights hierarchies.

Guidance issued by the Personal Data Protection Commission (PDPC) reinforces this approach by requiring organizations to conduct internal risk and impact assessments before relying on legitimate interests. These assessments must evaluate the benefits of processing, the probability and severity of harm, and the effectiveness of mitigation measures, such as access controls, data minimization, and retention limits (Ong 2019). The PDPC's framework thus operationalizes legitimate interests as a compliance process rather than a mere legal label.

Notably, the PDPA permits reliance on legitimate interests without notification in limited circumstances, but this exemption is narrowly construed. In practice, transparency remains central, and organizations are expected to document why notification would be impractical or counterproductive (Tan and Lee 2021). This design choice underscores Singapore's emphasis on demonstrable accountability rather than procedural formalism.

5.2 Enforcement-Led Clarification: Mitigation and Safeguards

Enforcement practice under the PDPA has played a critical role in clarifying the practical contours of legitimate interests. Rather than focusing primarily on the abstract legitimacy of organizational objectives, regulatory scrutiny has centred on whether adequate safeguards were implemented to reduce residual risk to individuals. This enforcement orientation reflects a governance logic in which lawful processing is contingent on the quality of internal controls, rather than on the intrinsic nature of the processing purpose.

Scholarly analysis highlights that the legitimate interest's exception is not intended to enable broad data mining or unrestricted analytics. Its application in contexts such as computational data analysis remains narrow, particularly where processing could be achieved through less intrusive means or where individuals would not reasonably expect such use (Tan and Lee 2021). This approach aligns with PDPC expectations that legitimate interests be invoked conservatively and supported by technical and organizational safeguards.

5.3 Comparative Insight: Accountability-by-Design in the Asia-Pacific Context

Singapore's approach contrasts sharply with the litigation-driven evolution of legitimate interests in the European Union. While EU jurisprudence has progressively narrowed legitimate interest through adversarial enforcement and judicial interpretation, Singapore has embedded flexibility directly into statutory design and administrative guidance. This model prioritizes accountability-by-design over rights absolutism, placing the burden of justification on organizations while preserving regulatory discretion.

From a regional perspective, Singapore's PDPA amendments illustrate the diffusion of GDPR-inspired principles across the Asia-Pacific, while also adapting them to local governance priorities. Comparative studies of ASEAN data protection regimes show that Singapore has selectively incorporated European concepts, such as proportionality and balancing, without adopting the EU's heavy reliance on litigation as a clarifying mechanism (Gomes 2024). This has positioned Singapore as a reference model for pragmatic data protection governance within ASEAN, influencing emerging regimes that seek to balance economic development with individual protection.

Overall, Singapore's experience demonstrates that legitimate interests need not generate the same degree of legal uncertainty observed in the EU, provided that flexibility is coupled with enforceable accountability mechanisms. The PDPA's design suggests that ambiguity can be managed through structured assessments, regulatory guidance, and enforcement focused on mitigation, offering an alternative pathway for jurisdictions seeking scalable yet responsible data governance.

VI. CCPA - FUNCTIONAL EQUIVALENTS WITHOUT LEGITIMATE INTEREST

Unlike the GDPR, California's privacy framework does not rely on enumerated lawful bases for processing personal data. The California Consumer Privacy Act (CCPA) was enacted rapidly through a ballot-driven legislative process, resulting in a statute oriented toward consumer rights rather than processing justifications (Alexander 2019). Its core principles like transparency, consumer control, and accountability, are operationalized through access, deletion, and opt-out rights rather than through ex-ante legality tests. The subsequent California Privacy Rights Act (CPRA) expanded and refined this rights-based model, but did not introduce a concept equivalent to “legitimate interest” or other lawful bases familiar to European data protection law (Bukaty 2021).

This structural choice reflects political and economic constraints within the U.S. regulatory environment. Scholars note that while the CCPA drew inspiration from the GDPR, it deliberately avoided the European architecture of lawful bases, opting instead for a market-regulatory approach that governs data flows indirectly through consumer choice mechanisms (Buresh 2022). As a result, compliance analysis in California focuses less on whether processing is justified and more on whether consumer rights are properly enabled and honoured.

6.1 Ambiguity in “Sale,” “Sharing,” and “Legitimate Business Purpose”

The absence of lawful bases does not eliminate ambiguity; rather, it relocates it. Under the CCPA and CPRA, interpretive uncertainty centres on the definitions of “sale,” “sharing,” and “business purpose.” The CPRA's introduction of “sharing” was intended to correct the CCPA's narrow focus on monetary consideration by explicitly capturing cross-context behavioural advertising (Determann and Tam 2020). Nevertheless, empirical research demonstrates that businesses continue to interpret these terms inconsistently, leading to fragmented disclosures and consumer confusion (Chen et al. 2021; Xian et al. 2025).

This ambiguity is compounded by the statute's reliance on functional distinctions, such as service providers versus third parties, that require complex contractual and technical controls. Studies of U.S. financial institutions show that overlapping regulatory regimes and inconsistent privacy notices undermine the CCPA's transparency objectives, particularly in relation to third-party data sharing for marketing and analytics (Xian et al. 2025). In practice, determining whether a data transfer constitutes a "sale" or "sharing" event often requires granular analysis of data flows rather than legal interpretation alone.

6.2 Enforcement as De Facto Interpretation

In the absence of doctrinal lawful bases, enforcement actions play a central role in defining the practical meaning of the CCPA and CPRA. Regulatory scrutiny has focused heavily on targeted advertising and third-party data flows, areas where consumer expectations and commercial incentives diverge most sharply. Economic studies show that privacy regulation in California has materially reduced data availability for advertisers, weakened targeting effectiveness, and altered firm behaviour throughout the advertising ecosystem (Choi and Jerath 2022; Hosseini 2025).

Enforcement has also had structural market effects. Empirical evidence indicates that CCPA implementation coincided with increased consolidation in the ad-tech sector, as firms sought to internalize data and analytics capabilities to reduce regulatory exposure associated with third-party sharing (Ghanavi, Hosseini, and Tucker 2025). These outcomes underscore how enforcement-driven interpretation can reshape market structure even in the absence of explicit processing prohibitions.

6.3 Systemic Impact: Opt-Out Engineering over Legal Balancing

A defining feature of California's model is its reliance on technical mechanisms to operationalize consumer choice. Rather than requiring organizations to perform balancing tests akin to legitimate interest assessments, the CCPA and CPRA mandate the implementation of opt-out systems, including browser-based signals such as the Global Privacy Control (GPC) (Crepax 2025). This has shifted compliance effort toward interface design, signal detection, and backend enforcement logic in what may be described as opt-out engineering.

However, research consistently demonstrates that firms have used design complexity and friction to discourage opt-outs, prompting regulatory intervention. Empirical studies document widespread use of dark patterns and inconspicuous opt-out mechanisms, leading the CPRA to explicitly prohibit such practices (O'Connor et al. 2021; Tran et al. 2025). These developments reveal that, even without lawful-basis ambiguity, compliance burdens persist and migrate into system design choices. California's experience thus illustrates that the absence of legitimate interest does not simplify privacy governance; it reconfigures it around technical enforcement of consumer rights rather than legal justification of processing.

6.4 LGPD and the Replication of GDPR Ambiguity

Brazil's Lei Geral de Proteção de Dados (LGPD) is widely characterized as a legal transplant of the European Union's General Data Protection Regulation. Comparative scholarship consistently observes that the LGPD reproduces the GDPR's core architecture, including lawful bases for processing, proportionality principles, and accountability requirements, with only limited local adaptation (Perrone and Strassburger 2018; Sombra 2020). Article 7(IX) of the LGPD introduces "legitimate interest" as a lawful basis for processing, while Article 10 conditions its use on compatibility with data subject expectations and enhanced transparency obligations. This design closely mirrors Article 6(1)(f) GDPR, thereby importing both its flexibility and its indeterminacy.

As in the European context, legitimate interest under the LGPD is framed as a conditional authorization rather than a categorical permission. Controllers must demonstrate that processing is necessary to pursue a legitimate purpose and that such processing does not override fundamental rights. Brazilian scholars note that this approach assigns significant interpretive discretion to regulators and courts, replicating the same ambiguity that has driven extensive litigation in the EU (Sombra 2020).

6.5 Transparency as a Statutory Burden

A distinctive feature of the LGPD's legitimate interest framework is the explicit statutory emphasis on transparency. Article 10 requires controllers to adopt measur es that ensure clarity regarding processing activities grounded in legitimate interest. This provision imposes a higher justificatory burden than that found in the GDPR, effectively transforming legitimate interest into a disclosure-intensive compliance pathway rather than a permissive alternative to consent.

Empirical studies of IT organizations subject to both the GDPR and LGPD show that this transparency obligation complicates requirements specification and system design. Legal ambiguity must be resolved collaboratively across development teams, legal departments, and domain experts, particularly when translating abstract legal standards into technical requirements (Netto et al. 2024). As a result, legitimate interest under the LGPD generates implementation costs similar to those observed in Europe, despite Brazil's different institutional context.

6.6 Regulatory Signals from the ANPD: High-Risk Processing

Regulatory guidance and enforcement signals from the Autoridade Nacional de Proteção de Dados (ANPD) have further narrowed the practical scope of legitimate interest, particularly for high-risk processing. Brazilian scholarship highlights that legitimate interest is increasingly scrutinized where processing involves automated decision-making, large-scale analytics, or artificial intelligence systems that generate significant inferences about individuals (Magrani and Miranda 2025).

While the LGPD does not mandate Data Protection Impact Assessments (RIPDs) for all high-risk processing, it grants the ANPD discretion to require such assessments when legitimate interest is invoked or when processing affects large populations (Garacis 2025). This discretionary model introduces regulatory uncertainty, especially for AI-driven processing, where the definition of "high risk" remains under-specified (Nwodo 2025). Consequently, controllers face a compliance environment in which legitimate interest is legally available but operationally fragile, particularly for innovative or data-intensive uses.
The emerging doctrine of "reasonable inferences" further constrains legitimate interest by linking it to data subject expectations and explainability. This approach suggests that even technically accurate processing may fail the legitimacy test if it produces unexpected or opaque outcomes for individuals, reinforcing the normative limits of legitimate interest in algorithmic contexts (Magrani and Miranda 2025).

6.7 Litigation and Collective Rights Risk

Beyond administrative enforcement, Brazil's distinctive contribution to the litigation of ambiguity lies in its robust collective enforcement mechanisms. The LGPD operates within a broader legal ecosystem shaped by consumer protection law and public interest litigation. Public civil actions, often initiated by the Ministério Público, enable collective redress for data protection violations affecting large groups of data subjects (Souza 2021; Dresch and Faleiros Júnior 2024).

This collective enforcement model functions as an enforcement multiplier, amplifying the consequences of ambiguous compliance decisions. Even in the absence of regulatory sanctions, organizations relying on legitimate interest may face significant litigation risk if processing practices are perceived to harm diffuse or collective interests. Brazilian courts have increasingly recognized data protection as a matter of public policy, reinforcing the judiciary's willingness to adjudicate systemic data governance failures (Doneda and Mendes 2013).

In aggregate, Brazil's experience demonstrates that replicating the GDPR's legitimate interest framework without substantially narrowing its scope reproduces both its benefits and its costs. While legitimate interest offers theoretical flexibility, its practical use under the LGPD is constrained by transparency mandates, regulatory discretion, and collective litigation risk. The Brazilian case thus reinforces a broader comparative lesson: where lawful bases rely on balancing and expectations, ambiguity becomes a structural feature of compliance rather than a transitional flaw.

VII. COMPARATIVE SYNTHESIS: PATTERNS OF LEGITIMATE INTEREST FAILURE

Across jurisdictions, the practical failure of "legitimate interest" or its functional equivalents follows a set of recurring patterns that transcend formal doctrinal differences. The first and most consistent failure mode is overuse for core commercial activities. In the European Union and Brazil, legitimate interest has repeatedly been invoked to justify business-critical processing, such as behavioural advertising, large-scale profiling, or analytics, rather than residual or ancillary purposes. Regulatory and judicial responses have made clear that where processing is economically central and highly intrusive, it is unlikely to satisfy proportionality and balancing requirements, regardless of the legitimacy of the underlying commercial objective (Balboni et al. 2013; Sombra 2020).

A second cross-cutting failure concerns inadequate management of data subject expectations. Theoretical models of legitimate interest rely heavily on the concept of "reasonable expectations," yet empirical experience shows that organizations systematically underestimate the gap between internal assumptions and user perceptions. In the EU and Brazil, courts and regulators increasingly treat unexpected secondary uses (such as cross-platform tracking or AI-driven inference) as dispositive against legitimate interest claims (Kamara and De Hert 2018; Magrani and Miranda 2025). Similar expectation gaps appear in California, where consumers frequently fail to understand or anticipate the scope of "selling" or "sharing" practices disclosed under the CCPA, undermining the effectiveness of opt-out rights (Chen et al. 2021).

The third recurring failure mode is the absence or insufficiency of technical safeguards. Legitimate interest frameworks assume that organizational mitigation measures such as data minimization, access controls, retention limits, and auditability will reduce residual harm. However, studies across jurisdictions indicate that such safeguards are often implemented unevenly or retrofitted after enforcement pressure, rather than embedded by design (Alhadeff, Van Alsenoy, and Dumortier 2012; Netto et al. 2024). Where safeguards remain weak, legitimate interest collapses into a formal justification unsupported by operational reality.

7.1 Divergent Regulatory Philosophies

While these failure modes are broadly shared, regulatory responses diverge significantly based on underlying governance philosophies. In the European Union and Brazil, legitimate interest is constrained by a rights-first proportionality model. Both regimes embed balancing tests within a constitutional or quasi-constitutional framework of fundamental rights, enabling regulators and courts to override organizational interests where power asymmetries or systemic risks are identified (Ferretti 2014; Perrone and Strassburger 2018). Litigation plays a central role in clarifying ambiguity, but this ex-post clarification comes at the cost of legal uncertainty and high compliance overhead, particularly for data-intensive sectors.

Singapore, by contrast, adopts a risk-managed accountability model. Rather than treating legitimate interest primarily as a site of rights conflict, the PDPA situates it within a broader reasonableness and governance framework. The regulatory focus is less on abstract proportionality and more on whether organizations have conducted credible risk assessments and implemented effective mitigation measures (Chik 2022; Lim 2024). This approach reduces adversarial litigation and offers greater predictability, but places substantial responsibility on organizations to internalize compliance discipline through documentation and system design.

In California, the absence of lawful bases produces a distinct regulatory logic centred on market regulation through opt-out mechanics. Instead of balancing interests' ex ante, the CCPA and CPRA regulate data processing indirectly by empowering consumers to refuse participation in certain data flows. Ambiguity persists, but it is relocated to definitions of "sale," "sharing," and "business purpose," and resolved through enforcement actions and technical mandates such as the Global Privacy Control (Determann and Tam 2020; Crepax 2025). Compliance effort thus shifts from legal reasoning to interface design, signal detection, and backend enforcement.

7.2 Comparative Implications

Taken together, these experiences demonstrate that legitimate interest ambiguity is not an isolated doctrinal flaw, but a structural feature of modern data protection governance. Where systems rely on balancing and expectations, ambiguity manifests as litigation risk and documentation burden. Where such balancing is avoided, as in California, ambiguity re-emerges as technical and behavioural complexity. Singapore's experience suggests that ambiguity can be partially managed, but not eliminated, through accountability-by-design.

The comparative lesson is therefore not that one model is categorically superior, but that ambiguity migrates across legal, organizational, and technical layers depending on regulatory design. Effective privacy governance requires recognizing legitimate interest not as a stable legal category, but as a dynamic coordination mechanism whose failure modes must be addressed through integrated legal, technical, and institutional strategies.

VIII. IMPLICATIONS FOR INDIA'S DPDP ACT

India's Digital Personal Data Protection Act, 2023 (DPDP Act) represents a deliberate and consequential departure from the European model of lawful bases. Unlike the GDPR and Brazil's LGPD, the DPDP Act does not recognize a general, open-ended "legitimate interest" ground for private entities. This omission is not accidental. Comparative scholarship characterizes the DPDP Act as an explicit response to the "litigation of ambiguity" observed in GDPR enforcement, where broad balancing standards have generated prolonged regulatory uncertainty and high compliance costs (Puthenveeti 2024). By excluding a flexible legitimate interest test, the Indian framework prioritizes legal certainty and administrative tractability over contextual discretion.

This design choice aligns with a broader trend in legal-tech governance toward rule-based compliance architectures. As studies in regulatory theory observe, legal certainty reduces arbitrariness and enforcement risk, but does so by constraining the interpretive space available to decision-makers (Krajewski 2014). The DPDP Act reflects this trade-off by minimizing judicial and regulatory discretion in determining when personal data may be processed without consent.

8.1 Design Rationale for "Legitimate Uses"

Section 7 of the DPDP Act (often referred to as Clause 7 during drafting) introduces a closed list of "certain legitimate uses" for which consent and notice requirements do not apply. These uses are largely confined to state functions, public interest activities, employment-related safeguards, medical emergencies, and voluntary provision of data by individuals. Doctrinal analysis emphasizes that this structure replaces the GDPR's subjective balancing test with a binary rule-based mechanism - either the processing falls within Section 7, or consent is required (Dharod and Tauro 2023).

The rationale for this approach is closely tied to India's digital governance priorities. Scholars note that Section 7 supports the state's "Digital Public Infrastructure" vision by ensuring that welfare delivery, subsidies, judicial orders, and emergency services are not obstructed by consent friction or post-hoc legal challenges (Puthenveeti 2024; Singh and Thakur, 2025). In this sense, legitimate uses function as an infrastructural enabler rather than a commercial flexibility mechanism. Unlike the GDPR, Section 7 cannot be invoked to justify generalized commercial analytics, advertising, or profiling.

8.2 Reduction of Legal Ambiguity at the Cost of Flexibility

From a comparative perspective, Section 7 exemplifies a classic regulatory trade-off: reduction of ambiguity at the cost of flexibility. Legal and economic literature cautions that while rigid rules improve predictability, they may undermine the nuanced, context-sensitive judgments that principle-based systems enable (Burk 2019; Krajewski 2014). In the privacy domain, this concern is particularly salient.

Attempts to standardize compliance through automated tools or templates often reshape the underlying legal standard itself, transforming open-ended principles such as fairness or proportionality into narrow, machine-readable constraints (Daly 2024).

Empirical economic research on the GDPR suggests that harmonized and less ambiguous rules benefit large, resource-rich firms capable of absorbing fixed compliance costs, while simultaneously reducing the adaptive capacity of smaller firms and startups (Li et al. 2022). The DPDP Act's architecture risks producing a similar outcome, but through a different pathway: by eliminating flexible lawful bases, it channels innovation into consent engineering rather than purpose-based governance

Technical studies further indicate that regulatory clarity can generate a "chilling effect," where organizations adopt the most restrictive interpretation of the law to avoid enforcement risk, even when broader interpretations might be socially beneficial (EPRS 2019). In the Indian context, the absence of a general legitimate interest clause may lead firms to default to consent for marginal or low-risk processing, regardless of proportionality considerations.

8.3 Strategic Consequences for Indian Firms

For private-sector actors, the most immediate consequence of Section 7 is the necessity of consent-centric architectures. Unlike firms operating under the GDPR or PDPA, Indian organizations cannot rely on a balancing test to justify data reuse for analytics, service optimization, or secondary innovation. Consulting analyses emphasize that even employment-related processing under Section 7(i) is narrowly scoped to risk mitigation, such as preventing loss or liability, and does not extend to generalized workforce analytics (PwC India 2025).

This structural narrowing significantly limits opportunities for private-sector balancing. Whereas European or Singaporean firms may invest in sophisticated Legitimate Interest Assessments and mitigation frameworks, Indian firms must instead invest in scalable consent management systems, audit trails, and withdrawal mechanisms. Comparative guides note that Section 7 uses are exempt from notice, but remain subject to necessity and lawful purpose constraints, reinforcing the DPDP Act's preference for ex ante clarity over ex post adjudication (ICLG 2025).

In aggregate, India's approach reflects a conscious policy decision to localize ambiguity within legislative drafting rather than judicial interpretation. While this reduces litigation risk and enhances predictability, it also redistributes compliance costs toward technical systems for consent orchestration. The DPDP Act thus illustrates how lessons from global experiences with legitimate interest ambiguity have been selectively internalized, resulting in a privacy regime that is clearer, but also more rigid, than its international counterparts.

IX. SYSTEM-LEVEL RESPONSES: ARCHITECTING FOR CERTAINTY

Comparative experience across the GDPR, LGPD, PDPA, and CCPA demonstrates that ambiguity in lawful bases does not disappear through legislation alone; rather, it is displaced into system design, operational governance, and compliance tooling. India's DPDP Act resolves one dimension of this problem by rejecting a general legitimate interest clause in favour of a closed list of "legitimate uses" and a consent-first model. This legislative clarity, however, shifts the burden of compliance from legal interpretation to technical implementation. As regulatory theory predicts, reductions in interpretive flexibility must be offset by more deterministic and auditable system architectures (Krajewski 2014).

Consequently, DPDP compliance is best understood as an engineering problem, not merely a legal one. Organizations must encode statutory constraints, such as purpose limitation, consent withdrawal, and use-specific processing, directly into data pipelines and application logic. This mirrors broader trends in legal-tech, where open-textured legal principles are increasingly translated into machine-enforceable constraints, even at the cost of contextual nuance (Burk 2019; Daly 2024).

9.1 Consent-Centric System Architecture

The most immediate architectural implication of the DPDP Act is the necessity of consent-centric design. In the absence of a balancing test akin to legitimate interest, consent becomes the primary lawful basis for most private-sector processing. This requires organizations to move beyond static privacy notices toward dynamic consent management systems capable of capturing, storing, updating, and enforcing user preferences in real time.

Such systems must support granular consent tied to specific purposes, data categories, and processing contexts, rather than blanket authorization. Empirical research on GDPR compliance indicates that overly broad or generic consent mechanisms increase enforcement risk and reduce user trust (Li et al. 2022). Under the DPDP Act, this risk is heightened, as invalid consent cannot be cured through fallback reliance on legitimate interest. Architecturally, this necessitates purpose-bound data tagging, consent-aware APIs, and automated checks that prevent downstream processing when consent is absent or withdrawn.

9.2 Purpose Limitation and Data Flow Segmentation

A second critical strategy involves purpose limitation enforcement at the system level. Section 7 of the DPDP Act introduces narrowly defined legitimate uses, while all other processing requires explicit consent for a specified purpose. To operationalize this distinction, organizations must segment data flows according to legal basis, ensuring that data collected under consent is not inadvertently reused for incompatible purposes.

Comparative studies of IT organizations subject to GDPR and LGPD show that ambiguity in legal requirements often arises at the requirements-specification stage, where legal purposes are loosely mapped to technical functions (Netto et al. 2024). The DPDP Act's rigidity reduces legal ambiguity but increases the importance of accurate purpose modelling. Best practice architectures therefore employ policy-driven data routing, where processing rules are enforced through metadata and access controls rather than manual oversight.

9.3 Automation of Compliance and Auditability

The DPDP Act's emphasis on accountability and demonstrability aligns with a broader shift toward automated compliance validation. As seen in European accountability frameworks, documentation and auditability are no longer peripheral obligations but core system requirements (Alhadeff, Van Alsenoy, and Dumortier 2012). Indian organizations must similarly prepare for regulator-facing audits that demand traceable evidence of lawful processing.

Technical responses include automated logging of consent events, immutable audit trails for data access, and real-time monitoring of policy violations. Patented systems for dynamic compliance validation illustrate how legal rules can be translated into testable operational boundaries, effectively converting flexible standards into pass/fail checks (Citibank NA 2024). While such automation improves predictability and reduces human error, it also reinforces the DPDP Act's preference for certainty over discretion.

9.4 Managing Trade-Off between Standardization and Innovation

A recurring concern in the literature is that standardized compliance architectures may inadvertently suppress innovation. Studies of GDPR's economic impact suggest that rigid compliance regimes disproportionately advantage large firms with the resources to build sophisticated governance systems, while constraining smaller actors and startups (Li et al. 2022). The DPDP Act risks replicating this effect by channelling innovation effort into compliance engineering rather than data-driven experimentation.

To mitigate this, system architects should adopt modular compliance designs that decouple consent and purpose enforcement from core business logic. Such modularity allows firms to adapt to future regulatory change without rebuilding entire systems. It also preserves limited flexibility for low-risk innovation within the bounds of explicit consent, avoiding the "chilling effect" observed in highly risk-averse regulatory environments (EPRS 2019).

9.5 High-Risk Processing and Impact Assessment by Design

Although the DPDP Act does not mandate data protection impact assessments (DPIAs) in the same manner as the GDPR, comparative experience from Brazil and the EU demonstrates that regulators increasingly scrutinize high-risk processing, particularly involving AI and large-scale analytics. System-level responses should therefore anticipate future rulemaking by embedding risk assessment workflows into development lifecycles.

This includes automated classification of processing activities by risk level, internal review gates for new data uses, and documentation of mitigation measures. Scholarship on algorithmic governance emphasizes that technical systems are ill-suited to capture open-ended notions of fairness, yet procedural safeguards, such as human oversight and explainability checkpoints, remain essential to legitimate processing (Daly 2024). Designing these safeguards proactively reduces regulatory shock and aligns with emerging global norms.

9.6 Strategic Implications for Indian Firms

Taken together, these architectural strategies reflect a fundamental shift in compliance posture. Under the DPDP Act, firms cannot rely on post-hoc justification through balancing tests. Instead, legality must be pre-engineered into systems. This reorientation favours organizations capable of integrating legal requirements into software development, data engineering, and governance workflows.

At a strategic level, Indian firms must treat privacy compliance as a core infrastructure investment rather than a legal afterthought. While this increases upfront costs, it also offers long-term benefits in predictability, scalability, and cross-border interoperability. As comparative evidence shows, ambiguity does not vanish when removed from law; it reappears in technology. The DPDP Act's contribution lies in making this trade-off explicit, compelling organizations to confront the architectural consequences of legal certainty head-on

X. POLICY AND REGULATORY IMPLICATIONS

The comparative analysis undertaken in earlier sections demonstrates that privacy regulation increasingly functions as an instrument of systems governance rather than as a purely rights-allocating legal framework. The Indian DPDP Act crystallizes this shift by replacing open-ended balancing with rule-based certainty. While this approach reduces interpretive ambiguity and litigation risk, it reassigns responsibility to organizations to operationalize compliance through deterministic architectures. For policymakers, this underscores a critical lesson from the GDPR, LGPD, PDPA, and CCPA experiences: regulatory clarity does not eliminate compliance cost; it reallocates it across institutional and technical layers (Krajewski 2014; Li et al. 2022).

As a result, the effectiveness of the DPDP regime will depend less on statutory text and more on whether regulators, firms, and technology vendors converge on interoperable compliance practices. Without such convergence, even a rule-based framework risks producing fragmentation, excessive conservatism, and uneven enforcement outcomes.

10.1 Implications for Indian Regulators

For regulators, the DPDP Act presents an opportunity to avoid the "litigation of ambiguity" observed in the EU by shifting emphasis toward ex-ante guidance and supervisory predictability. However, international experience suggests that certainty must be complemented by procedural proportionality. Excessively rigid enforcement may generate chilling effects similar to those documented in GDPR research contexts, where actors default to the most restrictive interpretation to minimize risk (EPRS 2019).

Accordingly, Indian regulators should prioritize:

- Implementation guidance clarifying consent validity, withdrawal mechanics, and purpose compatibility;
- Risk-tiered supervision, focusing enforcement on large-scale, sensitive, or systemic processing rather than low-risk activities;
- Regulatory sandboxes for data-intensive innovation, enabling supervised experimentation without eroding statutory safeguards.

These measures mirror the accountability-oriented approaches seen in Singapore, where regulatory discretion is exercised through guidance and mitigation expectations rather than adversarial litigation (Chik 2022; Lim 2024).

10.2 Implications for Boards and Corporate Governance

At the organizational level, the DPDP Act elevates privacy compliance to a board-level fiduciary concern. Comparative evidence from the EU and California demonstrates that privacy failures increasingly translate into market, reputational, and structural consequences, including constrained data access and forced architectural redesigns (Ghanavi, Hosseini, and Tucker 2025). Indian boards must therefore treat compliance architecture as a form of enterprise risk management, comparable to cybersecurity or financial controls.

Policy guidance for boards should emphasize:

- Clear allocation of accountability between legal, technology, and business leadership;
- Periodic assurance reporting on consent integrity, data flows, and breach readiness;
- Investment decisions that prioritize scalable compliance infrastructure over ad hoc remediation.

Such governance mechanisms align with the broader accountability principle articulated in global data protection scholarship, which links legal compliance to demonstrable organizational controls rather than declaratory policies (Alhadeff, Van Alsenoy, and Dumortier 2012).

10.3 Implications for CTOs and System Architects

For CTOs, the DPDP Act mandates a shift from compliance-as-documentation to compliance-as-code. The absence of a general legitimate interest clause removes discretionary fallback options, making technical enforcement of consent, purpose limitation, and data minimization non-negotiable. As prior sections demonstrate, attempts to automate flexible legal standards tend to reshape those standards themselves, favouring determinism over contextual nuance (Burk 2019; Daly 2024).

Architectural priorities should therefore include:

- Consent orchestration layers decoupled from business logic;
- Purpose-bound data pipelines with enforceable access controls;
- Auditability and observability embedded at the infrastructure level;
- Risk classification modules anticipating future scrutiny of AI and high-impact processing.

Failure to adopt these patterns risks recreating, in technical form, the same ambiguity and enforcement volatility the DPDP Act seeks to avoid.

10.4 Systemic Architecture as Public Policy Infrastructure

At a macro level, the DPDP Act should be understood as part of India's broader digital public infrastructure strategy. Just as payment and identity systems standardized interoperability to reduce transaction friction, privacy compliance infrastructure can standardize lawful data use without continuous legal renegotiation. However, this requires alignment between regulators, industry, and technology providers on reference architectures and compliance benchmarks.

International experience suggests that when such alignment is absent, firms either over-engineer compliance or under-invest until enforcement forces reactive change, both economically inefficient outcomes (Li et al. 2022). The policy imperative, therefore, is to treat privacy architecture as shared infrastructure rather than firm-specific overhead.

XI. CONCLUSION

This paper has examined the concept of “legitimate interest” as a site of persistent legal, regulatory, and architectural ambiguity across major data protection regimes. Comparative analysis of the European Union, Singapore, California (United States), and Brazil demonstrates that legitimate interest, whether explicitly codified or functionally approximated, has consistently failed as a stable compliance anchor for data-intensive economies. Rather than enabling flexible, context-sensitive governance, it has generated litigation, enforcement volatility, and escalating system-level costs.

In the European Union and Brazil, legitimate interest has become a focal point for judicial and regulatory contestation, with courts progressively narrowing its applicability through proportionality, reasonable expectations, and fairness doctrines. In Singapore, ambiguity has been partially contained through an accountability-first administrative model, though at the cost of significant internal governance obligations. In California, the absence of lawful bases has not eliminated uncertainty but displaced it into definitional disputes and technical opt-out enforcement. Across all regimes, ambiguity has migrated from law into system architecture, documentation burdens, and organizational risk management.

India’s Digital Personal Data Protection Act (DPDP Act) represents a deliberate and consequential response to these global failure patterns. By rejecting a general legitimate interest clause and replacing it with a closed list of “certain legitimate uses,” the DPDP Act prioritizes legal certainty, administrative predictability, and infrastructural scalability. This design choice reduces litigation risk and interpretive discretion but imposes a clear trade-off: diminished flexibility for private-sector data reuse and innovation. The Indian approach thus reframes privacy compliance as a deterministic engineering challenge rather than a balancing exercise in legal judgment.

The central contribution of this paper lies in demonstrating that legitimate interest ambiguity is not a doctrinal accident but a structural feature of modern privacy governance. Where laws rely on open-ended balancing, ambiguity manifests as litigation and enforcement risk; where laws eliminate balancing, ambiguity reappears as technical rigidity and compliance engineering cost. The DPDP Act does not escape this dynamic - it relocates it. Understanding this relocation is essential for policymakers, regulators, and firms seeking sustainable compliance strategies.

10.1 Policy Recommendations

Regulators to Prioritize Predictable Supervision over Formalism

Regulators implementing the DPDP Act should resist the temptation to replicate the EU’s enforcement-heavy model through post hoc interpretation. International experience demonstrates that excessive reliance on adjudication exacerbates uncertainty rather than resolving it. Instead, regulators should issue granular implementation guidance on consent validity, withdrawal mechanics, and purpose limitation, enabling firms to design compliant systems ex ante rather than litigate compliance ex post (Krajewski 2014).

A risk-tiered supervisory approach is recommended, focusing enforcement resources on high-impact processing (large-scale analytics, sensitive data, and AI-driven decision systems), while allowing proportional flexibility for low-risk uses. Regulatory sandboxes and supervised experimentation frameworks would further mitigate chilling effects and align privacy protection with India’s innovation and Digital Public Infrastructure objectives (EPRS 2019).

Legislators to Treat Compliance Architecture as Public Infrastructure

The DPDP Act's effectiveness will depend on the availability of interoperable compliance tooling across sectors. Legislators should recognize privacy compliance systems (consent management, audit logging, and purpose enforcement) as shared governance infrastructure, analogous to payments or identity systems. Encouraging open standards and reference architectures can reduce duplicative compliance costs and prevent market concentration among large incumbents with proprietary compliance platforms (Li et al. 2022).

Future amendments or rules should also preserve limited adaptive capacity, particularly for emerging technologies, to avoid regulatory ossification. While the rejection of legitimate interest reduces ambiguity, complete rigidity risks long-term inefficiency.

Boards to reframe Privacy as Enterprise Risk Governance

Boards of Indian firms must internalize privacy compliance as a fiduciary governance issue, not merely a legal checkbox. Comparative evidence from the EU and California shows that privacy failures increasingly produce structural consequences, forced architectural redesigns, data access constraints, and reputational harm (Ghanavi, Hosseini, and Tucker 2025). Boards should mandate periodic assurance reporting on consent integrity, data flows, and breach preparedness, integrating privacy risk into enterprise risk management frameworks.

CTOs to Embed Law into System Design

For technology leaders, the DPDP Act necessitates a shift to compliance-by-design. Consent orchestration, purpose-bound data pipelines, and auditability must be embedded directly into system architecture. Attempts to retrofit compliance after deployment replicate the same ambiguity and enforcement volatility observed under legitimate interest regimes (Burk 2019; Daly 2024). Modular, policy-driven architectures offer the best balance between determinism and future adaptability.

Closing Observation

India's DPDP Act represents one of the most explicit global attempts to resolve the legitimate interest problem through legislative design rather than judicial evolution. Its success will depend not on the elimination of ambiguity, but on whether ambiguity is managed consciously, transparently, and systemically. The broader lesson for global privacy governance is clear: the future of data protection lies not in choosing between flexibility and certainty, but in engineering institutions and systems capable of governing the trade-off between them.

XII. *ACKNOWLEDGMENT*

We have used the Rezorce~Check Global Forensic Platform to extract judgements that is used in this paper

XIII. *REFERENCES*

[1] Alexander, Christopher Bret. 2019. "The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations." *Loyola Consumer Law Review* 32: 199–232.

[2] Alhadeff, Joseph, Brendan Van Alsenoy, and Jos Dumortier. 2012. "The Accountability Principle in Data Protection Regulation." *In Managing Privacy through Accountability*, 49–82. London: Palgrave Macmillan.

[3] Balboni, Paolo, Daniel Cooper, Rosario Imperiali, and Milda Macenaite. 2013. "Legitimate Interest of the Data Controller: New Data Protection Paradigm—Legitimacy Grounded on Appropriate Protection." *International Data Privacy Law* 3 (4): 244–261. https://doi.org/10.1093/idpl/ipt019

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

[5] Basarudin, Noor Ashikin, and Ridwan Adetunji Raji. 2022. "Implication of Personalized Advertising on Personal Data." *Environment-Behaviour Proceedings Journal* 7 (22): 109–118.

[6] Becker, Regina, et al. 2019. "DAISY: A Data Information System for Accountability under the GDPR." *GigaScience* 8 (12): giz140.

[7] Bioni, Bruno. 2020. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Thomson Reuters.

[8] Bukaty, Preston. 2021. *The California Privacy Rights Act* (CPRA): An Implementation and Compliance Guide

[9] Buresh, Donald L. 2022. "Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute?" *Santa Clara High Technology Law Journal* 38: 39–78.

[10] Burk, Dan L. 2019. "Algorithmic Fair Use." *University of Chicago Law Review* 86 (2): 283–306.

[11] Chen, Rex, Fei Fang, Thomas Norton, Aleecia M. McDonald, and Norman Sadeh. 2021. "Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA." *In Proceedings of the Workshop on Privacy in the Electronic Society*, 73–102.

[12] Chik, Warren B. 2022. "The Reasonableness Standard of Compliance in the Singapore Personal Data Protection Act." *Singapore Academy of Law Journal* 34: 352–382.

[13] Choi, W. Jason, and Kinshuk Jerath. 2022. "Privacy and Consumer Empowerment in Online Advertising." *Foundations and Trends in Marketing* 15 (3): 153–212

[14] Citibank NA. 2024. "Dynamically Validating AI Applications for Compliance." *U.S. Patent* 12,111,754 B1.

[15] Crepax, Tommaso. (2024). Global Privacy Control and Portability of Privacy Preferences Through Browser Settings: A Comparative Study of Techno-Legal Challenges Under the Ccpa/Cpra and the Gdpr. 10.2139/ssrn.4710372.

[16] "Daly, Gemma. 2024. "Algorithmic Fairness: Challenges to Building an Effective Regulatory Regime." *Frontiers in Artificial Intelligence* 7. https://doi.org/10.3389/frai.2024.12426052

[17] Determann, Lothar, and Jonathan Tam. 2020. "The California Privacy Rights Act of 2020." *Journal of Data Protection & Privacy* 4 (1): 7–21.

[18] Dharod, Vaibhav, and Kevin Tauro. 2023. "Assessing India's Digital Personal Data Protection Act, 2023." *Indian Journal of Law and Legal Research* 5 (1): 4580–4595

[19] Doneda, Danilo, and Laura Schertel Mendes. 2013. "Data Protection in Brazil: New Developments and Current Challenges." *In Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, 3–20. Dordrecht: Springer

[20] Dresch, Rafael de Freitas Valle, and José Luiz de Moura Faleiros Júnior. 2024. "Special Strict Civil Liability in Brazil's General Data Protection Law." *Brazilian Journal of Law, Technology and Innovation* 2 (2): 98–128.

[21] European Data Protection Board. 2022. *Guidelines on Lawful Basis for Processing*. Brussels.

[22] European Parliamentary Research Service (EPRS). 2019. How the GDPR Changes the Rules for Scientific Research. Brussels: *European Parliament*.

[23] Ferretti, Federico. 2014. "Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?" *Common Market Law Review* 51 (3): 843–868.

[24] Forward, What Way. 2024. "The Mismatch Between GDPR and Behavioural Advertising." *In Privacy, Data Protection and Data-driven Technologies*, 63–89.

[25] Galli, Federico, and Galileo Sartor. 2024. "The Mismatch Between GDPR and Behavioural Advertising: What Way Forward?" *In Privacy, Data Protection and Data-driven Technologies*, 287–327. Routledge

[26] Garacis, Rainier. 2025. "Identification and Assessment of Eligibility Criteria for Preparing the Personal Data Protection Impact Assessment (RIPD)." *Brazilian Journal of Law, Technology and Innovation* 3 (1): 100–116.

[27] Ghanavi, Rozhina, Sepideh Hosseini, and Catherine E. Tucker. 2025. "Privacy Regulation and Ad-Tech Consolidation." *SSRN*.

[28] Gomes, Sofia Mira Pereira Jesus. 2024. EU Personal Data Protection Standards Beyond Its Borders: An Analysis of the European External Governance through GDPR on Data Protection Laws in the ASEAN Region. Master's thesis, *ISCTE-Instituto Universitário de Lisboa*.

[29] Hosseini, Sepideh. 2025. Essays on Economics of Privacy. PhD diss., *University of Toronto*.

[30] "ICLG. Data Protection Laws and Regulations Report 2025: India. London: Global Legal Group, 21 July 2025. Accessed December 2025. https://iclg.com/practice-areas/data-protection-laws-and-regulations/india

[31] Kamara, Irene, and Paul De Hert. 2018. "Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground." *Brussels Privacy Hub* Working Paper 4 (12).

[32] Kant, Tanya. 2021. "Identity, Advertising, and Algorithmic Targeting." *MIT Social & Ethical Responsibilities of Computing*.

[33] Krajewski, Markus. 2014. "Balancing Legal Certainty with Regulatory Flexibility." In WTO Domestic Regulation and Services Trade, edited by Aik Hoe Lim and Bart De Meester, 79–94. *Cambridge: Cambridge University Press*.

[34] Li, Enqi, et al. 2022. "Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond." *NBER Working Paper* No. 30705.

[35] Lim, Fang-Zhou. 2024. "Data Protection from a Regulatory Theory Perspective." *Singapore Law Review* 41: 162–196.

[36] Lukić, Karlo, Klaus M. Miller, and Bernd Skiera. 2024. "The Impact of the GDPR on Online Tracking." *SSRN Working Paper* 4399388.

[37] Magrani, Eduardo, and Paulo Rodrigo de Miranda. 2025. "The Right to Reasonable Inferences in Automated Decision Systems." *International Review of Law, Computers & Technology* 39 (1): 75–94

[38] Mihăilă, Carmen Oana, and Mircea Mihăilă. 2020. "The Legal Interest, Legal Basis for the Processing of Personal Data and the Right to Private Life." *Fiat Iustitia* 1.

[39] Netto, Dorgival, Carla Silva, João Araújo, and Mayara Santos. 2024. "How Do IT Companies Address Ambiguity Resolution in Legal Requirements Specification?" *SSRN* 4714597.

[40] Niedermeier, Robert, and Mario Egbe Mpame. 2019. "Processing Personal Data under Article 6(f) of the GDPR: The Concept of Legitimate Interest." *International Journal of Data Protection Officer, Privacy Officer & Privacy Counsel* 3: 18–26.

[41] Nwodo, Fochi. 2025. "Clarifying High-Risk Data Processing in AI Governance." *Business Law Review* 46 (5).

[42] O'Connor, Sean, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. 2021. "(Un)Clear and (In)Conspicuous." *In Proceedings of the Workshop on Privacy in the Electronic Society*, 59–72.

[43] Ong, Ee-Ing. 2019. "Singapore Report: Data Protection in the Internet." *In Data Protection in the Internet*, 309–347. Cham: Springer International Publishing.

[44] Perrone, Christian, and Sabrina Strassburger. 2018. "Privacy and Data Protection—From Europe to Brazil." *Panorama of Brazilian Law* 6 (9–10): 82–100.

[45] Petrašević, Tunjica, and Romana Ćosić. 2023. "Legitimate Interest." In GDPR Requirements for Biobanking Activities across Europe, 275–280. *Cham*: Springer

[46] Puthenveeti, Pameela George. 2024. "DPDPA 2023 vs. GDPR: A Comparative Analysis." *DCU Law & Tech Research Cluster*.

[47] PwC India. Digital Personal Data Protection Rules (2025). PwC Knowledge Portal, 2025. Accessed December 2025. https://www.pwc.in/assets/pdfs/digital-personal-data-protection-rules-2025.pdf

[48] Singh, Arshpreet & Thakur, Shailja. (2025). Data Protection and Ai Under the Digital Personal Data Protection Act, 2023: An Indian Perspectives. *INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS*. 2320-2882.

[49] Solove, Daniel J., and Paul M. Schwartz. 2023. *Information Privacy Law*. 7th ed. New York: Wolters Kluwer.

[50] Sombra, Thiago Luís. 2020. "The General Data Protection Law in Brazil: What Comes Next?" *Global Privacy Law Review* 1 (2).

[51] Souza, Marcelo Silveira de. 2021. O papel do Ministério Público no enforcement da Lei Geral de Proteção de Dados.

[52] Tan, David, and Thomas Chee Seng Lee. 2021. "Copyright in Copyright Law: Fair Use, Computational Data Analysis and the Personal Data Protection Act." *Singapore Academy of Law Journal* 33 (2): 1032–1082

[53] Tran, Van Hong, et al. 2025. "Dark Patterns in the Opt-Out Process and Compliance with the CCPA." *In Proceedings of the CHI Conference on Human Factors in Computing Systems*.

[54] Voigt, Paul, and Axel von dem Bussche. 2017. The EU General Data Protection Regulation (GDPR): A Practical Guide. *Cham*: Springer

[55] Xian, Lu, et al. 2025. "Layered, Overlapping, and Inconsistent." In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 3177–3191.