INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ANATOMY OF A PRIVACY POLICY: COMPARATIVE DISCLOSURE OBLIGATIONS UNDER GDPR, DPDP ACT 2023, AND CCPA/CPRA

AUTHORED BY - SAMUDRANIL CHAKRABARTI
Fifth Year Student, B.A., LL.B. (Hons.)
Amity University Kolkata

ABSTRACT

Privacy policies constitute the primary legal and operational interface through which data-processing organizations communicate information-handling practices to data subjects. Yet, despite their central placement within modern data protection frameworks, empirical evidence shows that traditional privacy notices remain lengthy, opaque, and fundamentally ineffective in facilitating genuine, informed consent. This paper undertakes a comparative doctrinal and empirical-design analysis of the disclosure and notice obligations imposed under the European Union's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act, 2023 (DPDP Act), and the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA). The study comprehensively evaluates the substantive content, temporal requirements, accessibility and localization standards, consent architectures, and enforcement mechanics governing privacy disclosures across these three prominent regulatory regimes.

The paper argues that while all three frameworks seek to enhance transparency and individual control over personal data, they are built upon fundamentally divergent regulatory philosophies. The GDPR advances an expansive, rights-based model grounded in lawful processing, accountability, and active informational self-determination. The DPDP Act implements a heavily consent-centric, paternalistic framework that positions detailed notice as a strict statutory prerequisite to valid data processing. Meanwhile, the CCPA/CPRA employs a market-oriented consumer-protection model focused on transactional disclosure, downstream data control, and dynamic opt-out rights. Through a systematic evaluation of statutory provisions, regulatory guidelines, enforcement trends, and judicial precedents, this study identifies key operational frictions relating to sensitive data classifications, downstream vendor management, private rights of action, and user interface-based compliance requirements.

ISSN: 2582-6433

Finally, the study demonstrates that conventional monolithic privacy policies fail to achieve meaningful user comprehension, thereby inducing cognitive overload and "notice fatigue." To resolve these systemic inefficiencies, this paper proposes a modular, multi-layered privacy notice architecture designed to simultaneously satisfy the heterogeneous disclosure obligations of the GDPR, DPDP Act, and CCPA/CPRA. By positioning privacy notices at the intersection of data governance, statutory compliance, and user-centered design, this study contributes a scalable and sustainable compliance framework for organizations navigating an increasingly fragmented global digital economy.

Keywords: Privacy Notice, GDPR, DPDP Act 2023, CCPA/CPRA, Layered Disclosure, Privacy-by-Design, Cross-Border Compliance.

I. INTRODUCTION

The modern digital economy operates on the systematic collection, continuous analysis, and commercial monetization of personal data. Across social media platforms, cloud-based architectures, e-commerce ecosystems, financial technology applications, and complex artificial intelligence systems, personal information has shifted from a mere secondary operational byproduct to a principal economic asset and a key driver of corporate valuation.[1] As data processing operations grow increasingly sophisticated, automated, and opaque, the legal and technical mechanisms governing transparency and individual control over personal information have acquired heightened significance. Within this regulatory landscape, the privacy policy occupies a unique and shifting position. Once regarded as a boilerplate contractual disclaimer drafted primarily to mitigate corporate liability, the privacy policy has evolved into a vital instrument of corporate data governance, statutory transparency, and individual informational autonomy.[2]

Modern data protection regimes rely extensively on notice-based transparency. Under this "notice and choice" paradigm, privacy notices are legally expected to inform individuals about the categories, purposes, lawful bases, retention periods, and transfer destinations of data processing activities, theoretically empowering them to make rational, self-interested decisions regarding their personal information.[3] This regulatory approach reflects constitutional and human-rights principles that identify informational privacy as an essential facet of human dignity, personal liberty, and individual self-determination.[4] In theory, robust disclosure requirements reduce the profound information asymmetries

ISSN: 2582-6433

existing between data subjects and sophisticated data-processing entities, thereby enabling individuals to exercise meaningful control over their digital identities.

In practice, however, the real-world utility of privacy notices remains deeply contested. Cognitive and behavioral science studies consistently demonstrate that consumers rarely read privacy policies in their entirety, and often lack the temporal resources, cognitive capacity, or specialized expertise required to comprehend complex, legalese-heavy disclosure documents.[5] This systemic barrier, widely conceptualized as "notice fatigue," has led to extensive academic criticism of the traditional "notice and choice" framework. Lengthy disclosures, dense legal prose, and repetitive consent banners frequently degrade the user experience and create an "illusion of consent," wherein formal regulatory compliance is achieved without promoting actual user understanding.[6] Consequently, a deep chasm has emerged between technical legal compliance and genuine user comprehension.

This systemic friction is amplified for multinational organizations that operate across multiple jurisdictions. The European Union's General Data Protection Regulation (GDPR) adopts a universal, rights-based approach rooted in fundamental human rights, requiring strict accountability and a multiplicity of lawful bases for processing.[7] India's Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a highly centralized, consent-oriented framework that enforces notice as an absolute statutory precondition to lawful digital processing.[8] In contrast, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), relies on a consumer-protection model designed to guarantee market transparency, transactional equity, and unilateral consumer opt-out rights.[9]

Reconciling these divergent legal requirements within a single, coherent compliance strategy presents a formidable challenge. While existing literature has explored cross-border data transfers and general enforcement trends, comparative legal scholarship addressing the specific architectural requirements of privacy policies remains limited. This paper addresses this gap by conducting a comparative doctrinal analysis of the disclosure and notice obligations established under the GDPR, the DPDP Act, and the CCPA/CPRA. The paper argues that the operational frictions generated by these divergent frameworks make a monolithic, "one-size-fits-all" privacy policy legally non-compliant and behaviorally counterproductive. Instead, it proposes a modular, multi-layered privacy notice framework that leverages human-computer interaction (HCI) principles and privacy-by-design methodologies.

ISSN: 2582-6433

II. RESEARCH OBJECTIVES

This study investigates the evolving legal architecture of privacy notices and comparative disclosure obligations across three influential data protection regimes. To address the compliance challenges of multi-jurisdictional data processing, this research pursues the following objectives:

First, to analyze and contrast the statutory disclosure requirements prescribed under Articles 12, 13, and 14 of the GDPR, Section 5 of the DPDP Act 2023, and the "Notice at Collection" provisions of the CCPA/CPRA, highlighting key differences in their substantive content, overall presentation, and legal scope.

Second, to evaluate the temporal dimensions of privacy disclosures across these regimes, focusing specifically on the legal and user-interface implications of the DPDP Act's mandate that detailed notice must precede or accompany consent.

Third, to investigate the legal treatment of specialized data classifications, comparing the GDPR's "special categories of personal data," the CCPA/CPRA's "sensitive personal information" framework, and the DPDP Act's uniform, single-tier approach to personal data.

Fourth, to assess the interface-based and operational compliance requirements imposed by each framework, including the mandatory placement of consumer rights linkages, opt-out mechanisms, and localized language options.

Fifth, to identify and map the principal compliance frictions and regulatory risks encountered by multinational enterprises attempting to maintain a single, global privacy disclosure document.

Sixth, to design and propose a modular, three-tiered privacy notice architecture that harmonizes the technical requirements of the GDPR, DPDP Act, and CCPA/CPRA, thereby reducing notice fatigue and improving user comprehension.

ISSN: 2582-6433

III. RESEARCH QUESTIONS

To fulfill these objectives, this study addresses the following research questions:

1. How do the foundational definitions of personal data and jurisdictional thresholds under the GDPR, DPDP Act, and CCPA/CPRA shape the mandatory scope of an organization's privacy disclosures?
2. How do the temporal requirements and trigger events for delivering privacy notices differ among the three regimes, and what are their corresponding impacts on digital business workflows?
3. To what extent does Section 5 of the Indian DPDP Act 2023 — requiring notice to accompany or precede consent — alter conventional user interface (UI) architectures and consent collection mechanisms?
4. How do specialized regulatory mandates, such as the CCPA/CPRA's homepage links ("Do Not Sell or Share My Personal Information") and the DPDP Act's multilingual accessibility requirements, alter platform design and user experience?
5. What are the specific legal risks and operational bottlenecks that occur when a multinational corporation uses a single, consolidated global privacy policy?
6. Can a modular, multi-layered privacy notice architecture successfully reconcile the structural tensions between the GDPR, DPDP Act, and CCPA/CPRA while mitigating cognitive overload and notice fatigue?

IV. RESEARCH HYPOTHESES

To guide this comparative analysis, the following hypotheses are formulated and tested:

Hypothesis 1 (H1): The adoption of a single, uniform global privacy policy presents severe legal and operational risks for multinational organizations due to irreconcilable conflicts in the statutory definitions, legal bases, and consent triggers across the GDPR, DPDP Act, and CCPA/CPRA.

Hypothesis 2 (H2): A modular, multi-layered privacy notice architecture satisfies the diverse regulatory requirements of all three jurisdictions more effectively than a traditional static policy, while significantly reducing user notice fatigue and enhancing data comprehension.

Hypothesis 3 (H3): Highly prescriptive, context-specific disclosure regimes require the

ISSN: 2582-6433

systematic integration of legal compliance with front-end user interface (UI) design, transforming privacy notices from passive legal disclaimers into active, programmatic compliance mechanisms.

Hypothesis 4 (H4): Divergences in how the GDPR, DPDP Act, and CCPA/CPRA classify sensitive personal data and manage downstream third-party transfers create structural compliance frictions that cannot be resolved through a single, static disclosure model.

V. RESEARCH METHODOLOGY

This study employs a qualitative doctrinal and comparative legal research methodology to analyze the disclosure and notice obligations of the GDPR, DPDP Act, and CCPA/CPRA. This primary analysis is integrated with a user-centered interface compliance evaluation to assess how theoretical legal requirements translate into digital product design.

The doctrinal and comparative legal analysis involves a detailed, line-by-line examination of the relevant statutory provisions: Articles 12, 13, and 14 of the GDPR[10]; Section 5 and related consent requirements of the DPDP Act 2023[11]; and California Civil Code §§ 1798.100 and 1798.130[12]. The comparative analysis is enriched by evaluating authoritative regulatory guidelines, including the European Data Protection Board's (EDPB) Guidelines on Transparency[13], opinions of the California Privacy Protection Agency (CPPA), and judicial precedents from the Court of Justice of the European Union (CJEU) and the Supreme Court of India.

The interface compliance and user-centered evaluation draws upon principles of human-computer interaction (HCI), behavioral economics, and privacy-by-design. It analyzes contemporary digital disclosure patterns, including contextual just-in-time notices, privacy nutrition labels, consent dashboards, and global opt-out signals (e.g., Global Privacy Control). These designs are evaluated against statutory mandates to determine if they successfully satisfy legal disclosure duties while preserving user usability.

VI. LITERATURE REVIEW

A. Theoretical Foundations of Privacy Disclosure

The statutory obligation to disclose data-handling practices is grounded in fundamental philosophical, ethical, and constitutional theories of individual autonomy, dignity, and

ISSN: 2582-6433

informational self-determination. Under Kantian ethics, individuals are recognized as autonomous agents who must never be treated merely as a means to an end, but always as ends in themselves.[14] Translated to data protection, this philosophy dictates that organizations must provide comprehensive transparency regarding data processing, ensuring that individuals can make free, self-directed decisions about their personal digital sphere.

This theoretical imperative is further mirrored in liberal political philosophy, particularly in John Stuart Mill's "harm principle."[15] In this light, privacy disclosures serve as vital protective instruments. By equipping individuals with knowledge about how their data is gathered, aggregated, and evaluated, disclosures help prevent informational harms — including surveillance, algorithmic discrimination, and predatory profiling — before they occur.

In India, this constitutional theory of informational autonomy was formally recognized by the Supreme Court's landmark nine-judge bench in Justice K.S. Puttaswamy v. Union of India.[16] The Court declared privacy to be an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution. The Court emphasized that "informational privacy is a facet of individual liberty" and that any state or private restriction on this right must satisfy the three-fold test of legality, legitimate state aim, and proportionality. While Puttaswamy addressed state action, its underlying constitutional principles directly shaped the legislative drafting of the DPDP Act 2023, positioning transparency as a cornerstone of data fiduciary accountability.

Furthermore, the legal architecture of privacy notices shares strong conceptual foundations with the doctrine of "informed consent" in bioethics.[17] Just as medical interventions require prior disclosure of risks, alternatives, and procedures, digital processing requires a clear understanding of data actions to validate user consent. In both contexts, consent is legally and ethically void if it is procured through deception, omission, or complex obfuscation.

B. Notice Effectiveness and Compliance Design

Despite these compelling theoretical foundations, extensive empirical research in behavioral economics and HCI reveals that the traditional "notice and choice" framework is broken in practice. In his critique of "privacy self-management," Daniel J. Solove argues that the cognitive demands of reading every privacy policy a user encounters are mathematically and practically impossible to satisfy.[18] Solove points out that individuals suffer from severe cognitive limitations, bounded rationality, and systematic biases that prevent them from assessing the long-term, aggregated risks of data sharing.

This systemic breakdown is worsened by "notice fatigue." Research by Acquisti, Brandimarte, and Loewenstein demonstrates that while individuals claim to value privacy, their actual

ISSN: 2582-6433

behavioral choices are highly context-dependent and easily manipulated by interface design.[19] When confronted with long, complex legal documents, users experience cognitive overload, causing them to click "agree" simply to bypass the friction and access the service. This behavioral pattern turns the privacy policy into a mechanism that often immunizes data controllers from liability while offering data subjects no real protection.

To counter notice fatigue, HCI researchers have advocated for "privacy-by-design" and alternative, user-friendly disclosure structures. Cranor et al. pioneered the development of "privacy nutrition labels" — standardized, tabular summaries designed to let users compare privacy practices at a glance.[20] Other scholars have demonstrated that "just-in-time" notices significantly improve user comprehension and engagement compared to static, all-encompassing policies.[21] Recent scholarship also examines how global privacy laws increasingly mandate specific user interface designs. From the CCPA's opt-out links to the GDPR's strict bans on pre-ticked consent boxes, data protection law is directly shaping product design.

VII. RESEARCH & ANALYSIS

7.1 Definitional Frameworks, Jurisdictional Thresholds, and Scope of Protection

To address the first Research Question (RQ1) and evaluate Hypothesis 1 (H1), this section explores the statutory definitions of personal data, jurisdictional boundaries, and the scope of protection across the GDPR, DPDP Act, and CCPA/CPRA.

Philosophical Divergences Across Regimes

The foundational design of disclosures in each framework is dictated by a core philosophical divide. The European Union's General Data Protection Regulation adopts a rights-based model, positioning data protection as a fundamental human right. It focuses entirely on protecting the rights, freedoms, and dignity of the individual "Data Subject." India's Digital Personal Data Protection Act, 2023, implements a consent-centric model, emphasizing transactional paternalism, and positions comprehensive prior notice as a strict statutory prerequisite to procuring valid consent from the "Data Principal." Conversely, California's framework under the CCPA and CPRA adopts a consumer-protection model utilizing a commercial and market-oriented paradigm, focusing on ensuring market transparency, transaction equity, and post-collection data controls for the "Consumer" and their wider "Household."

ISSN: 2582-6433

The Definition of Protected Information

The threshold question of what constitutes protected data reveals a major regulatory divide. Under Article 4(1) of the GDPR, "personal data" is defined broadly as any information relating to an identified or identifiable natural person.[22] The CJEU has consistently interpreted this definition expansively, holding in Breyer v. Bundesrepublik Deutschland that dynamic IP addresses constitute personal data if a legal pathway exists to link them with identity records held by an internet service provider.[23] Similarly, India's DPDP Act, under Section 2(t), defines "personal data" as "any data about an individual who is identifiable by or in relation to such data."[24] While this definition mirrors the GDPR's scope, Section 3(a) introduces a critical restriction: the Act applies strictly to "digital personal data." Purely analog, paper-based files that are never digitized are entirely exempt, while the GDPR covers both digital processing and structured non-digital filing systems under Article 2(1).[25]

The CCPA/CPRA departs from both models by adopting a transactional, consumer-protection taxonomy. California Civil Code § 1798.140(v)(1) defines "personal information" as information that identifies, relates to, describes, or could reasonably be linked with a particular consumer or household.[26] By explicitly including the "household" construct, California law broadens the scope of mandatory disclosure to cover shared smart home devices, IoT hubs, and family accounts where data is aggregated at the household level. This variation confirms Hypotheses H1 and H4, proving that a single, unified data definition is structurally impossible to maintain globally.

Jurisdictional Thresholds and Extraterritorial Reach

Under Article 3(2), the GDPR asserts broad extraterritorial jurisdiction via its "effects-based" test, applying to controllers not established in the EU if their processing activities relate to the offering of goods or services to data subjects in the Union, or the monitoring of their behavior within the Union.[27] Section 3 of the DPDP Act similarly asserts extraterritorial application, governing the processing of digital personal data outside India if such processing is in connection with offering goods or services to Data Principals within India.[28] DPDP Act sets any minimum commercial or financial thresholds.

Neither the GDPR nor the The CCPA/CPRA, however, applies strictly to for-profit entities doing business in California that meet one or more specific commercial thresholds: annual gross revenues exceeding twenty-five million dollars; annually buying, selling, or sharing the personal information of 100,000 or more consumers or households; or deriving 50% or more of annual revenues from selling or sharing consumers' personal information.[29] This threshold-

ISSN: 2582-6433

based approach excludes small businesses and non-profits, aligning with its identity as a market-regulation tool rather than a universal rights charter, further validating Hypothesis 1 (H1).

7.2 Consent Mechanics, Notice Timing, and Temporal Bottlenecks

This section addresses the second Research Objective (RO2) and resolves Research Questions 2 and 3 by evaluating when notices must be delivered and how they interact with consent collection.

Notice Trigger Events and Timing

The temporal relationship between presenting a privacy notice and starting data processing represents a key compliance challenge. Under GDPR Articles 13 and 14, when data is collected directly from the data subject, the notice must be provided "at the time when personal data are obtained." When data is obtained from third-party sources, the controller must provide the notice within a reasonable period, but at the latest within one month, or at the first communication with the data subject.[30]

The DPDP Act 2023 establishes a highly front-loaded, strict timing rule. Section 5(1) mandates that every consent request must be preceded or accompanied by a detailed, written notice.[31] Under this framework, data processing based on consent is strictly conditional on this prior disclosure. Furthermore, Section 5(2) introduces a highly demanding transitional rule for legacy data: if a Data Principal gave consent to data processing prior to the commencement of the Act, the Data Fiduciary must, as soon as reasonably practicable, provide a fresh notice describing the processing activities and the Data Principal's rights under the new law.[32] This requires organizations to systematically map and re-notify their entire historical Indian user database.

The CCPA/CPRA approaches timing through its "Notice at Collection" requirement under California Civil Code § 1798.100(a): a business must provide this notice to consumers "at or before the point of collection."[33] If a business later intends to use previously collected information for materially different purposes, it must provide a fresh notice describing those new purposes before any such processing begins.

Reshaping Digital User Interfaces: The Impact of DPDP Act Section 5

The DPDP Act's requirement that notice must precede or accompany consent fundamentally reshapes conventional digital user interfaces. In many Western markets, organizations have

ISSN: 2582-6433

traditionally relied on "implied consent" or passive "browse-wrap" agreements, where a user's continued navigation of a website is treated as acceptance of a privacy policy linked in the footer. The DPDP Act completely prohibits this passive model. Because consent under Section 6(1) must be "free, specific, informed, unconditional, and unambiguous with an associated affirmative action,"[34] organizations must integrate active gating and consent mechanisms directly into their user interfaces. This direct link between the legal mandate of Section 5 and the restructuring of user-facing screens strongly supports Hypothesis 3 (H3), demonstrating that privacy notices are no longer static legal documents but interactive compliance features embedded directly within the code of the user interface.

Language, Accessibility, and Localization Mandates

Under GDPR Article 12(1), notices must be delivered in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[35] The EDPB's Transparency Guidelines actively encourage the use of multi-layered notices and standardized icons.[36] The DPDP Act 2023 introduces a highly complex linguistic requirement: Section 5(3) mandates that the Data Principal must have the option to access the notice and the consent request in English or in any of the 22 regional languages specified in the Eighth Schedule to the Constitution of India.[37] This language localization mandate creates unprecedented operational and translation challenges for digital platforms, further validating Hypothesis 3 (H3). The CCPA/CPRA requires notices to be designed to be easy to read and highly visible, accessible to consumers with disabilities (WCAG 2.1 standards), and available in every language in which the business ordinarily provides contracts or sales materials in California.[38]

7.3 Specialised Classifications and the Sensitive Data Dichotomy

To satisfy the third Research Objective (RO3) and test Hypothesis 4 (H4), this section evaluates how each framework classifies "sensitive" or "special" categories of data.

The GDPR Prohibition-by-Default Model

The GDPR, under Article 9(1), adopts a strict prohibition-by-default model for "special categories of personal data," including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health metrics, or sexual history and orientation.[39] Under Articles 13(1)(c) and 14(1)(c), if an organization processes any special categories of personal data, its privacy notice must explicitly identify the specific lawful basis under Article 6 and the corresponding

ISSN: 2582-6433

statutory exception under Article 9(2) that permits such processing.

The CCPA/CPRA Consumer-Control Model

The CCPA/CPRA establishes a consumer-controlled framework for "Sensitive Personal Information" (SPI) under California Civil Code § 1798.121.[40] SPI is defined broadly to include government-issued identifiers, precise geolocation, racial or ethnic origin, religious beliefs, mail and text contents, genetic data, and biometric information. Rather than prohibiting the processing of SPI, the CCPA/CPRA requires businesses to provide a clear, conspicuous disclosure in their Notice at Collection and include a highly visible link on their homepage titled "Limit the Use of My Sensitive Personal Information," empowering consumers to restrict the business's use of their SPI solely to those services an average consumer would reasonably expect.

The DPDP Act 2023 Uniform Model

In sharp contrast, India's DPDP Act 2023 entirely omits any sub-classification of "sensitive" or "critical" personal data, instead treating all personal data under a single, uniform classification.[41] From a disclosure perspective, this means the statutory notice obligations for processing a user's food preferences are identical to those for processing their medical records or financial transactions. The only exception is children's data under Section 9, which prohibits tracking, behavioral monitoring, or targeted advertising directed at children, and requires verifiable parental consent disclosed clearly in the notice.[42] This structural divergence represents a core "compliance friction" as posited in Hypothesis 4 (H4), making a one-size-fits-all disclosure model structurally untenable.

7.4 Interface Compliance, Vendor Management, and Downstream Flows

This section addresses the fourth Research Objective (RO4) and Research Question 4 by analyzing how each regime mandates the disclosure of downstream data sharing and algorithmic processing.

Vendor Management and Recipient Disclosures

Under GDPR Article 13(1)(e), controllers must disclose the "recipients or categories of recipients of the personal data."[43] While controllers are not strictly required to name every individual processor in the primary privacy notice, they must provide sufficiently detailed categories so that the data subject can understand the real-world implications of the

ISSN: 2582-6433

transfers. The DPDP Act (Section 5(1)(a)) is significantly more demanding[44] — it requires the notice to disclose the identity of any Data Processor processing personal data on behalf of the Data Fiduciary. This requirement to name specific processing partners introduces immense administrative complexity: any change in vendor relationships necessitates an immediate update to the privacy disclosure and, potentially, the re-solicitation of consent.

The CCPA/CPRA approaches third-party transfers through a distinct commercial taxonomy centred on the concepts of "selling" and "sharing" personal information.[45] Businesses must explicitly disclose the categories of personal information sold or shared, the categories of third parties to whom the information was disclosed, and a clear statement of whether the business has actual knowledge of selling or sharing the personal information of consumers under 16 years of age. Crucially, this disclosure must be accompanied by a clear, conspicuous link on the business's homepages titled "Do Not Sell or Share My Personal Information," enabling consumers to opt out of these transfers instantly.

Automated Decision-Making (ADM) and Profiling

Under GDPR Articles 13(2)(f) and 14(2)(g), a controller must explicitly disclose the existence of automated decision-making, including profiling, and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[46] This requires organizations to translate complex algorithmic models into understandable, plain-language explanations within their public-facing privacy policies. The CCPA/CPRA delegates explicit regulatory authority to the California Privacy Protection Agency (CPPA) to issue regulations governing consumer access and opt-out rights regarding automated decision-making technology and profiling.[47] The DPDP Act 2023 is entirely silent on automated decision-making and profiling, leaving the regulation of algorithmic processing entirely dependent on the general notice requirements of purpose specification and consent under Section 5.[48]

7.5 Rights Architectures and Grievance/Redressal Systems

This section addresses the fourth Research Objective (RO4) and Research Question 4 by analyzing how different rights architectures shape the design and presentation of privacy interfaces.

ISSN: 2582-6433

The Right to Data Portability

This is a key transparency requirement under both GDPR Article 20 and the CCPA/CPRA (§ 1798.100), requiring businesses to disclose how users can obtain their data in a structured, commonly used, machine-readable, and portable format.[49][50] However, the DPDP Act 2023 conspicuously excludes the right to data portability,[51] reflecting a policy choice focused on reducing the technical compliance burden on domestic digital startups.

The Right to Withdraw Consent vs. The Right to Opt-Out

In the European and Indian models, consent is a primary legal basis for processing, and the privacy policy must disclose that the individual has the right to withdraw their consent at any time (GDPR Article 7(3); DPDP Act Section 6(4)).[52][53] The withdrawal process must be "as easy as" the giving of consent. Under the CCPA, however, the default paradigm is opt-out: the privacy policy functions as a disclosure of processing activities that are permitted by default, and the operational focus is on the consumer's right to opt-out of the sale or sharing of their information and the right to limit the use of their sensitive data.[54]

Redress, Grievance Management, and Administrative Contact Disclosures

For transparency to be actionable, individuals must know where to direct inquiries, complaints, and legal challenges. Under the GDPR (Article 13(1)(a)-(b)), the privacy notice must state the identity and contact details of the controller and, where applicable, the Data Protection Officer (DPO), and under Article 13(2)(d) must explicitly inform the data subject of their right to lodge a complaint with a specific Supervisory Authority.[55] The DPDP Act (Section 5(1)(b)) places an intense, localized emphasis on grievance redressal: the notice must disclose the contact details of the designated Grievance Officer and the specific procedure through which a Data Principal can register a grievance. Only after exhausting this internal mechanism can the Data Principal escalate their complaint to the Data Protection Board of India (DPBI) under Section 13.[56] The CCPA/CPRA requires businesses to disclose two or more designated methods for submitting requests to exercise consumer rights, including a toll-free telephone number and a website address or interactive web form, under California Civil Code § 1798.130.[57]

7.6 Enforcement Mechanics, Civil Penalties, and Private Action

This section addresses the first Research Objective (RO1) and resolves Research Question 5 by evaluating the different enforcement mechanisms that incentivize compliance.

ISSN: 2582-6433

Administrative and Civil Fines

The punitive landscape of modern data protection is characterized by historically unprecedented financial exposure. Under GDPR Article 83, supervisory authorities can impose administrative fines of up to twenty million euros (EUR 20,000,000), or up to 4% of total worldwide annual turnover of the preceding financial year, whichever is higher, for violations of basic processing principles including transparency and notice obligations under Articles 12, 13, and 14.[58] Under the DPDP Act, Section 28 read with Schedule I, the Data Protection Board of India can impose penalties of up to two hundred and fifty crore rupees (INR 250 crores, approximately USD 30,000,000) for a failure to take reasonable security safeguards to prevent personal data breaches, and up to two hundred crore rupees (INR 200 crores) for failures relating to children's data.[59] Under the CCPA/CPRA, enforcement is handled by the CPPA or the California Attorney General, with civil penalties of up to $2,500 for each unintentional violation and up to $7,500 for each intentional violation, assessed per consumer, per violation.[60] Consequently, a defective "Notice at Collection" on a website accessed by one hundred thousand California residents can rapidly aggregate into a catastrophic multi-million-dollar liability.

Private Rights of Action and Statutory Damages

GDPR Article 82 provides a robust private right of action, granting any person who has suffered material or non-material damage as a result of an infringement of the Regulation the right to receive compensation from the controller or processor.[61] This includes "non-material" damages such as distress, anxiety, or loss of control over personal data, which has led to a surge in class-action privacy litigation across the European Union. Under CCPA Section 1798.150, consumers cannot sue a business privately for standard disclosure failures; these are the exclusive domain of CPPA administrative enforcement.[62] However, California consumers can bring a private or class-action lawsuit for unauthorized access, exfiltration, theft, or disclosure of their unencrypted personal information resulting from a violation of the duty to implement reasonable security procedures, recovering statutory damages from $100 to $750 per consumer, per incident, or actual damages, whichever is greater. The DPDP Act 2023 entirely excludes a private right of action for damages,[63] positioning the Indian framework as highly paternalistic and relying exclusively on administrative oversight rather than private litigation to enforce transparency and compliance.

ISSN: 2582-6433

7.7 Synthesis and Hypothesis Testing

This section synthesizes the comparative doctrinal findings to resolve Research Questions 5 and 6 and evaluate the research hypotheses.

Verification of Hypotheses H1 and H4

The comparative doctrinal analysis conducted across sections 7.1 through 7.6 provides definitive verification for Hypothesis 1 (H1) and Hypothesis 4 (H4). The evidence demonstrates that the adoption of a single, uniform privacy policy for global operations is not merely operationally difficult but legally high-risk. The structural compliance frictions are systemic: an organization attempting to construct a unified policy faces irreconcilable conflicts between the GDPR's rights-based multi-basis processing, the CCPA/CPRA's consumer opt-out and sale-and-share paradigm, and the DPDP Act's strict notice-before-consent mandate. If a multinational organization drafts a policy that includes all details required under all three regimes, the document becomes an excessively dense, lengthy legal disclosure that exacerbates "notice fatigue" and reduces readability. A single, static disclosure model therefore cannot reconcile these competing legal architectures, validating H1 and H4.

Verification of Hypothesis H3

The analysis of notice timing under the DPDP Act Section 5, language localization mandates, and the CCPA's "Notice at Collection" confirms Hypothesis 3 (H3). Privacy disclosures are no longer passive legal documents. Because the DPDP Act requires active, multi-lingual notice to accompany or precede consent, and because the CPRA requires dynamic homepage links that communicate with backend data storage systems in real-time, compliance must be engineered directly into the user interface, demonstrating that regulatory frameworks with detailed, context-specific disclosure obligations require deep integration between legal compliance and user-interface design.

Validation of Hypothesis H2 and the Path Forward

This doctrinal analysis validates Hypothesis 2 (H2): a layered or modular privacy notice architecture is the only effective mechanism for achieving multi-jurisdictional compliance while preserving user comprehension. By separating disclosures into distinct, functional tiers — an essential notice layer (Tier 1), just-in-time contextual disclosures (Tier 2), and a comprehensive privacy governance center (Tier 3) — organizations can distribute information across multiple levels of engagement. This layered architecture satisfies the specific timing and

ISSN: 2582-6433

consent triggers of the GDPR and DPDP Act, hosts the mandatory links and opt-outs required by the CCPA/ CPRA, and presents clear information to the user at the exact moment of decision-making. The transition from a monolithic, document-centric compliance model to a modular, privacy-by-design compliance architecture represents the necessary evolution of privacy regulation in the global digital economy.

VIII. SUGGESTIONS AND RECOMMENDATIONS

The comparative analysis undertaken in this study demonstrates that the principal challenge facing multinational organizations is not merely compliance with individual privacy statutes, but the reconciliation of competing regulatory philosophies within a single operational environment. The GDPR prioritizes transparency and accountability through detailed disclosure obligations and multiple lawful bases for processing.[64] The DPDP Act 2023 places notice and consent at the center of lawful processing, requiring that disclosures precede or accompany requests for consent.[65]

The CCPA/CPRA emphasizes consumer agency through opt-out rights, notice-at-collection requirements, and interface-based transparency mechanisms.[66] Attempting to satisfy these divergent obligations through a single, static privacy policy frequently results in excessively lengthy disclosures that undermine user comprehension while simultaneously increasing regulatory risk. The findings of this research therefore support the adoption of a dynamic, modular, and privacy-by-design compliance architecture.

Architectural Layout of the Proposed Three-Tiered Framework

To reconcile competing international obligations while minimizing notice fatigue, organizations should transition to a highly modular transparency architecture structured into three distinct structural levels. The first level is the Essential Notice Layer (Tier 1), whose primary operational goal is direct engagement and core clarity, served immediately during onboarding or initial interface interaction, containing concise summaries of primary data types, key processing purposes, essential user rights, and central contact points. The second level is Just-In-Time Contextual Disclosures (Tier 2), whose operational goal is context-specific transparency at the point of decision-making, delivered via interactive notification overlays rendered immediately prior to triggering advanced technical collection, including specific purpose and duration notices served alongside active opt-in toggles. The third level is the Comprehensive Privacy Governance Center (Tier 3), whose operational goal is unabridged

ISSN: 2582-6433

statutory compliance and dynamic user control, delivered via a permanently accessible, searchable portal containing full legal texts, granular jurisdiction selection toggles, explicit third-party processor databases, retention schedules, and structured grievance forms.

8.1 Adoption of a Three-Tiered Layered Notice Architecture

A central recommendation of this study is the replacement of traditional monolithic privacy policies with a layered disclosure model comprising three interconnected tiers of transparency. The first layer, presented at account creation or initial website access, should communicate the core elements of processing in concise and accessible language, identifying the categories of personal data collected, the principal purposes of processing, the rights available to users, and the mechanisms through which consent may be granted or withdrawn. Particular attention should be given to accessibility requirements and linguistic inclusivity, including compatibility with assistive technologies and availability in languages reasonably expected to be understood by the intended user population.

The second layer should consist of contextual disclosures delivered immediately before specific categories of data are collected or processed. Requests for access to location data, biometric information, camera functionality, contact lists, or behavioral tracking technologies should be accompanied by targeted notices explaining the purpose, scope, and consequences of the proposed processing activity. Such contextual notices are particularly significant within consent-centric frameworks because they ensure that users receive relevant information at the moment of decision-making, and they strengthen evidence that consent was informed, specific, and directly connected to the processing activity in question.

The final layer should consist of a permanently accessible privacy governance center containing the full legal disclosure framework of the organization, including detailed information regarding data retention schedules, international transfers, categories of recipients, automated decision-making systems, security practices, grievance mechanisms, and regulatory contact information. It should also support regional customization, enabling organizations to present jurisdiction-specific rights and disclosures where required. The layered architecture therefore reconciles the competing demands of legal completeness and user comprehension by distributing information across multiple levels of engagement rather than concentrating all disclosures within a single document.

8.2 Automated Consent Management and Jurisdiction-Specific Compliance

The effectiveness of a modular disclosure framework depends upon the deployment of

ISSN: 2582-6433

intelligent consent-management systems capable of responding dynamically to regulatory requirements. Modern organizations should implement consent management platforms that identify the applicable legal framework based upon relevant jurisdictional indicators such as IP geo-location, user registration data, or chosen language parameters, and automatically present the disclosures, consent mechanisms, and rights interfaces required by local law. Such systems should be capable of maintaining auditable records of consent transactions, processing withdrawals of consent, and ensuring that user preferences are respected across interconnected systems.

From a comparative perspective, automated compliance mechanisms are particularly important because the GDPR, DPDP Act, and CCPA/CPRA impose materially different obligations regarding consent, transparency, and user choice, rendering a static, uniform interface incapable of simultaneously satisfying all applicable legal requirements. Additionally, organizations should ensure that browser-based privacy preference signals such as Global Privacy Control (GPC) and user-controlled privacy settings are integrated into consent-management processes wherever legally required.

8.3 Transition from Document-Centric Compliance to Privacy-by-Design Architecture

The analysis conducted in this paper demonstrates that effective privacy compliance cannot be achieved through disclosure mechanisms alone. Privacy notices must be supported by technical and organizational measures that ensure actual processing activities remain consistent with representations made to users. Accordingly, organizations should transition from a document-centric compliance model to a privacy-by-design governance architecture embedded throughout the data lifecycle.

A key component of this approach is the implementation of fine-grained access controls that restrict personal data usage to purposes expressly disclosed to users. Data access decisions should be governed through centralized authorization frameworks capable of enforcing purpose limitation and accountability requirements across multiple systems. Similarly, organizations should adopt robust data minimization techniques within testing, analytics, and development environments, protecting personal information used outside production systems through pseudonymization, tokenization, masking, or comparable technical safeguards designed to reduce re-identification risks.

8.4 The Case for Modular Compliance

The evidence examined throughout this study suggests that the future of privacy governance

ISSN: 2582-6433

lies not in increasingly lengthy privacy policies but in adaptive compliance architectures capable of delivering relevant information at the appropriate time, in the appropriate format, and to the appropriate audience. A modular privacy framework represents the most effective means of reconciling the divergent requirements of the GDPR, the DPDP Act, and the CCPA/CPRA. Such an approach preserves transparency, strengthens user autonomy, reduces notice fatigue, and enables organizations to satisfy multi-jurisdictional obligations without sacrificing usability. Consequently, privacy notices should no longer be viewed as isolated legal documents but as integral components of a broader governance ecosystem designed to operationalize transparency, accountability, and user control within the digital economy.

IX. CONCLUSION

The comparative analysis undertaken in this study demonstrates that privacy notices have evolved far beyond their historical function as contractual disclaimers or corporate risk-management documents. Under contemporary data protection regimes, privacy policies operate as legally mandated transparency mechanisms that mediate the relationship between individuals and organizations engaged in the collection, processing, and monetization of personal data. As a result, the design, timing, and content of privacy disclosures have become central components of modern privacy governance.

The analysis reveals that although the General Data Protection Regulation (GDPR), the Digital Personal Data Protection Act, 2023 (DPDP Act), and the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), pursue the shared objective of enhancing transparency and individual control over personal information, they do so through fundamentally different regulatory approaches. The GDPR adopts a rights-based framework built around multiple lawful bases for processing and extensive disclosure obligations.[67] The CCPA/ CPRA emphasizes consumer choice through notice-at-collection requirements, opt-out rights, and interface-based transparency mechanisms.[68] The DPDP Act, by contrast, places consent and prior notice at the center of lawful processing, thereby creating a particularly stringent temporal relationship between disclosure and data collection.[69]

The findings support the first research hypothesis that a uniform, static, and globally applicable privacy policy faces significant structural limitations in satisfying the disclosure requirements of these divergent legal frameworks. The varying approaches to consent, lawful processing, user rights, disclosure content, and interface obligations create operational tensions that cannot

ISSN: 2582-6433

be effectively addressed through a single monolithic document. Efforts to consolidate all jurisdiction-specific requirements into one disclosure often result in excessive complexity, reduced readability, and diminished user comprehension, thereby undermining the very transparency objectives that privacy legislation seeks to achieve.

The study further supports the second hypothesis that a modular and layered disclosure architecture offers a more effective compliance solution than traditional static privacy policies. By distributing information across multiple levels of engagement — including essential onboarding notices, contextual just-in-time disclosures, and comprehensive privacy governance centers — organizations can better reconcile legal completeness with user comprehension. Such an approach not only accommodates jurisdiction-specific requirements but also mitigates the behavioral challenges associated with notice fatigue and information overload.

More broadly, the research demonstrates that privacy compliance can no longer be understood solely as a drafting exercise undertaken by legal departments. Effective compliance increasingly requires the integration of legal requirements into technological infrastructure, user-interface design, consent-management systems, and organizational governance processes. Privacy notices have become components of a broader privacy-by-design architecture in which transparency, accountability, accessibility, and user control must be operationalized through both legal and technical mechanisms.

As privacy regulation continues to expand across jurisdictions and regulatory fragmentation intensifies, organizations will face increasing pressure to develop disclosure systems that are simultaneously compliant, comprehensible, and adaptable. The modular compliance framework proposed in this paper offers one possible pathway for achieving this balance. By reconceptualizing privacy notices as dynamic governance tools rather than static legal documents, the framework contributes to ongoing debates concerning the future of transparency, informed consent, and effective privacy regulation in the digital age. Ultimately, the future of privacy governance will depend not merely on the quantity of information disclosed to individuals, but on the ability of regulatory frameworks and technological systems to ensure that such information is delivered in a manner that genuinely enables informed choice, meaningful participation, and the protection of individual informational autonomy.

ISSN: 2582-6433

REFERENCES

1. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019).
2. Fred H. Cate, The Limits of Privacy Protection: Information and Consumer Choice, 81 Ind. L.J. 121 (2006).
3. Robert Gellman, Privacy, the Consumer, and the Information Economy, 26 N.C. J. Int'l L. & Com. Reg. 421 (2001).
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
5. Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y Info. Soc'y 543 (2008).
6. Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. Pa. L. Rev. 647 (2011).
7. Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
8. The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
9. California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100–1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA).
10. European Data Protection Board, Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01) (2018).
11. Immanuel Kant, Groundwork of the Metaphysics of Morals (Mary Gregor trans., Cambridge Univ. Press 1998) (1785).
12. John Stuart Mill, On Liberty (J.W. Parker and Son 1859).
13. Ruth R. Faden & Tom L. Beauchamp, A History and Theory of Informed Consent (Oxford Univ. Press 1986).
14. Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).
15. Alessandro Acquisti, Laura Brandimarte & George Loewenstein, Privacy and Human Behavior in the Age of Information, 347 Science 509 (2015).
16. Patrick G. Kelley et al., A "Nutrition Label" for Privacy, Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), ACM (2009).
17. Andrew S. Patrick & Steve Kenny, From Web Privacy Policies to User Interfaces, Proceedings of the Third Annual Workshop on Privacy Enhancing Technologies (PET) (2003).

ISSN: 2582-6433

18. Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779 (Oct. 19, 2016).
19. California Privacy Protection Agency, California Consumer Privacy Act Regulations, Title 11, Division 6, Chapter 1 (2023).

[1]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019).
[2]Fred H. Cate, The Limits of Privacy Protection: Information and Consumer Choice, 81 Ind. L.J. 121 (2006).
[3]Robert Gellman, Privacy, the Consumer, and the Information Economy, 26 N.C. J. Int'l L. & Com. Reg. 421 (2001). [4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[5]Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y Info. Soc'y 543 (2008).
[6]Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. Pa. L. Rev. 647 (2011).
[7]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[8]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[9]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[10]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[11]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[12]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[13]European Data Protection Board, Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01) (2018).
[14]Immanuel Kant, Groundwork of the Metaphysics of Morals (Mary Gregor trans., Cambridge Univ. Press 1998) (1785).
[15]John Stuart Mill, On Liberty (J.W. Parker and Son 1859).
[16]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[17]Ruth R. Faden & Tom L. Beauchamp, A History and Theory of Informed Consent (Oxford Univ. Press 1986).
[18]Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).
[19]Alessandro Acquisti, Laura Brandimarte & George Loewenstein, Privacy and Human Behavior in the Age of Information, 347 Science 509 (2015).
[20]Patrick G. Kelley et al., A Nutrition Label for Privacy, Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), ACM (2009).
[21]Andrew S. Patrick & Steve Kenny, From Web Privacy Policies to User Interfaces, Proceedings of the Third Annual Workshop on Privacy Enhancing Technologies (PET) (2003).
[22]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[23]Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779 (Oct. 19, 2016).
[24]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[25]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[26]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[27]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[28]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[29]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[30]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[31]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP

ISSN: 2582-6433

Act].
[32]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[33]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[34]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[35]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[36]European Data Protection Board, Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01) (2018).
[37]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[38]California Privacy Protection Agency, California Consumer Privacy Act Regulations, Title 11, Division 6, Chapter 1 (2023).
[39]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[40]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[41]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[42]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[43]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[44]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[45]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[46]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[47]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[48]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[49]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[50]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[51]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[52]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[53]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[54]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[55]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[56]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[57]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[58]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[59]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[60]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[61]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[62]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[63]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[64]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[65]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].
[66]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by

ISSN: 2582-6433

the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[67]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[68]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100-1798.199.100, as amended by the California Privacy Rights Act of 2020 (CPRA) [hereinafter CCPA/CPRA].
[69]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDP Act].