CONSTITUTIONAL IMPLICATIONS OF CONSENT FATIGUE IN DATA PROTECTION: RETHINKING MEANINGFUL CONSENT IN THE INDIAN CONTEXT

Soham Kulkarni & Swaraj Abhyankar, DES Shri Navalmal Firodia Law College Pune

ABSTRACT

The pervasive challenge of consent fatigue in the digital age, where individuals are overwhelmed by incessant requests for data processing consent, leads to automatic acceptance and a diminished sense of control over personal information. This phenomenon profoundly undermines the very premise of "meaningful consent" within data protection frameworks globally. In the Indian context, this issue gains particular salience due to the constitutional recognition of the right to privacy under Article 21, as affirmed in *K.S. Puttaswamy v. Union of India*.[1] Consent fatigue poses a significant constitutional dilemma, as it erodes the principles of informational self-determination and decisional autonomy central to privacy jurisprudence. The Digital Personal Data Protection Act, 2023 (DPDPA), despite its robust definition of consent, faces unique implementation challenges in India due to factors like low digital literacy and the digital divide.[3] This paper undertakes a critical analysis of these constitutional implications, exploring alternative consent models and regulatory interventions. It advocates for a holistic approach that reconciles individual rights with the demands of the digital economy, ensuring privacy is protected as a fundamental and constitutive value.

Keywords: Consent Fatigue, Meaningful Consent, Right to Privacy, Digital Personal Data Protection Act 2023, Informational Self-Determination.

I. INTRODUCTION

Setting the Stage: The Digital Age, Data Proliferation, and the Imperative of Privacy

The contemporary digital landscape is characterized by an exponential increase in data generation, collection, and processing. This pervasive datafication has transformed societal structures and economic models, making robust data protection frameworks indispensable for safeguarding individual rights and societal well-being. Privacy, in this context, has transcended its traditional confines to emerge as a fundamental human right in the digital era. The sheer volume of personal data now routinely collected, stored, and analyzed by both state and private entities necessitates a critical examination of the mechanisms designed to protect individual autonomy in this data-rich environment.

Defining Consent Fatigue and its Emergence in the Global Digital Landscape

Consent fatigue is a widely recognized phenomenon referring to the psychological exhaustion and indifference experienced by individuals due to the incessant and often complex demands for consent for data collection and processing.[4] This is particularly evident in the ubiquitous presence of cookie banners and lengthy privacy notices across digital platforms. Originating as a significant challenge in jurisdictions with stringent privacy regulations, such as the European Union, consent fatigue leads users to routinely grant consent without genuine comprehension or critical evaluation of the implications, thereby reducing consent to a perfunctory act rather than a substantive expression of authorization.[4] The average user encounters approximately 100 websites monthly, leading to an overwhelming exposure to consent requests and the resultant "banner blindness".[4]

The very mechanisms initially conceived to empower users and enhance privacy have, paradoxically, become primary contributors to privacy erosion due to their flawed design and sheer volume. This indicates a systemic failure inherent in the current consent-centric models rather than merely an issue of individual user apathy. The observation that the cookie consent mechanism, intended to enhance user privacy, actually decreases it due to over-exposition, highlights a critical design flaw.[4] The problem stems not from the concept of consent banners themselves, but from their implementation, which often involves poor privacy user experience practices such as dark patterns and complex legal jargon.[4] This design flaw directly fosters consent fatigue, leading to "banner blindness" and automatic acceptance, where users consent

without understanding the implications. This creates a contradiction: the intended outcome of enhanced privacy through informed consent is inverted, resulting in diminished privacy. This suggests that legal frameworks heavily reliant on the current "notice-and-choice" model are inherently vulnerable to practical failure, creating an illusion of control rather than genuine empowerment.[5]

The Indian Context: Unique Challenges and the Constitutional Mandate for Privacy

India, characterized by its immense population, rapid digital transformation, and significant disparities in digital literacy, presents a uniquely challenging environment for implementing effective data protection. The constitutional recognition of privacy as a fundamental right, established by the Supreme Court, sets a high benchmark for data protection, rendering the implications of consent fatigue particularly critical within the Indian legal and social fabric.[1] The prevailing low digital literacy and the pervasive digital divide in India mean that the attainment of truly informed consent is "tremendously challenging and nearly impossible".[3]

II. THE CONSTITUTIONAL FOUNDATION OF PRIVACY IN INDIA: THE PUTTASWAMY LEGACY

Tracing the Evolution of the Right to Privacy in Indian Jurisprudence

The judicial journey towards establishing privacy as a fundamental right in India commenced with early pronouncements, notably in *Gobind v. State of M.P.* (1975). In this case, the Supreme Court, drawing inspiration from American "penumbral" reasoning, recognized privacy as intrinsically woven into the Indian constitutional fabric, despite the absence of the term "privacy" in the Constitution itself.[2] Over the ensuing decades, the Court progressively expanded the ambit of this right across diverse contexts, including issues related to phone tapping, narco-analysis, brain mapping, prisoner's rights, and computer networks.[2] This incremental development laid the groundwork for a more definitive pronouncement on the fundamental nature of privacy.

K.S. Puttaswamy v. Union of India: A Landmark Verdict and its Implications for Data Protection

The watershed judgment by a nine-judge bench in *K.S. Puttaswamy (Retd.) v. Union of India* (2017) definitively affirmed the right to privacy as a fundamental right enshrined under Article

21 of the Indian Constitution.[1] This ruling marked a monumental achievement, elevating data privacy to the same constitutional stature as the rights to life and personal liberty, and unequivocally emphasizing the individual's right to control their personal data.[1] The genesis of this judgment lay in the constitutional challenges mounted against the Aadhaar scheme, which mandated the collection of extensive biometric and demographic data, raising profound questions about informational autonomy.[2]

The *Puttaswamy* judgment, by rooting privacy in human dignity and autonomy, fundamentally transforms data protection from a mere regulatory compliance issue into a matter of constitutional human rights. This implies that any mechanism of data processing, including consent, that undermines genuine individual choice or understanding is not merely a statutory violation but a potential infringement of a constitutionally guaranteed right. The Court recognized data privacy as a fundamental right under Article 21, emphasizing autonomy, dignity, and the individual's right to control their personal data.[1] If consent fatigue leads to individuals losing effective control over their data and making choices that are not truly autonomous, as described by the phenomenon of "murky consent" [4], then this directly challenges the constitutional principles of informational self-determination and decisional autonomy that

Puttaswamy established. The "moral magic" of consent, which legitimizes data processing, is lost when consent is "murky".[5] Consequently, the means by which consent is obtained or presumed must themselves be constitutionally sound, not just legally compliant, to uphold the fundamental right to privacy. This constitutional grounding imposes a higher standard of scrutiny on data processing practices than purely statutory compliance, indicating that the state has a positive obligation to ensure that the operationalization of consent genuinely respects and enables these core constitutional values.

Article 21 and the Triple Test: Legality, Legitimate Aim, and Proportionality as Constitutional Safeguards

In *Puttaswamy*, the Supreme Court articulated a rigorous three-pronged proportionality test that any state action infringing upon the right to privacy must satisfy: (i) it must be backed by a valid law (legality); (ii) it must pursue a legitimate state aim; and (iii) the means employed must be proportionate to the aim, encompassing suitability, necessity, and fair balance (*proportionality stricto sensu*).[6] This test serves as a critical constitutional safeguard, ensuring

that restrictions on privacy are not arbitrary but are justified and proportionate to a compelling public interest.

The triple test serves as the crucial constitutional lens through which the efficacy and legitimacy of consent mechanisms, particularly in the context of pervasive consent fatigue, must be rigorously evaluated. If consent is not truly informed, free, and unambiguous, the means of data collection and processing may fail the proportionality test, even if a legitimate state aim is present. The observation that the triple test is the standard for assessing privacy infringements, including necessity (least intrusive means) and fair balance, is critical.[6] Consent fatigue results in "murky consent," which Professor Solove describes as "mostly fictional" and lacking legitimacy.[5] If data processing relies on such "murky consent," then the means of obtaining this consent (e.g., overwhelming banners, dark patterns) are not the least intrusive or fairest way to achieve a legitimate aim. This directly challenges the "necessity" and "fair balance" limbs of the proportionality test. A system that effectively coerces or tricks individuals into "consenting" cannot be considered a proportionate means of data collection when less intrusive and more genuinely empowering alternatives exist. This establishes a constitutional imperative for the state to actively ensure that data protection laws and their practical implementation genuinely facilitate meaningful consent, or to explore alternative lawful bases for data processing that do not rely on a flawed consent model. Failure to do so could render data processing unconstitutional under Article 21, even if a statutory basis exists.

III. CONSENT IN INDIAN DATA PROTECTION REGIMES: A CRITICAL EXAMINATION

The Information Technology Act, 2000 and SPDI Rules: Early Frameworks and Limitations of Consent

Prior to the enactment of the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 (IT Act) and its subsidiary Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), constituted the primary regulatory framework for data privacy in India.[10] Under these rules, consent was the foundational principle for processing personal data, especially sensitive personal data.[10] However, the definition of "consent" remained ambiguous, often defaulting to principles derived from contract law, with minimal explicit limitations as long as it was "willingly obtained".[10] While the SPDI Rules did impose certain restrictions on data

collection (e.g., lawful purpose, necessity, awareness of collection, retention limits, purpose limitation) and disclosure (requiring prior permission for third-party sharing, with specific exemptions for government agencies), the overarching vagueness of consent itself posed a significant challenge.[11]

The imprecise definition of "willingly obtained" consent under the IT Act and SPDI Rules inadvertently created a conducive environment for the emergence and proliferation of consent fatigue. This historical context illuminates how a lack of stringent legal clarity can contribute to problematic industry practices, thereby laying the groundwork for the current challenges in achieving meaningful consent. The absence of explicit requirements for specificity, informed choice, or clear affirmative action in the IT Act's consent framework allowed data fiduciaries to adopt broad, undifferentiated consent mechanisms, such as blanket "I agree" buttons.[10] This permissive environment, stemming from vague legal guidance, directly contributed to the conditions that foster consent fatigue, such as overwhelming users with non-granular requests and lacking transparency. The "willingly obtained" standard was easily satisfied by a mere click, without ensuring genuine understanding or choice. This historical analysis underscores the necessity of the DPDPA's more stringent and detailed consent requirements, implicitly acknowledging that the older standards were insufficient to protect privacy in a rapidly evolving digital landscape. It highlights a legislative learning curve in recognizing the practical inadequacies of a loosely defined consent.

The Digital Personal Data Protection Act, 2023: A Paradigm Shift?

The Digital Personal Data Protection Act, 2023 (DPDPA), enacted in August 2023, signifies India's inaugural comprehensive personal data protection legislation.[12] Its core objective is to meticulously balance the individual's right to privacy and personal data with the legitimate processing needs of data fiduciaries.[12] The Act unequivocally establishes consent as the foundational principle for the processing of personal information.[13]

Defining "Valid Consent": Free, Specific, Informed, Unconditional, Unambiguous, and Clear Affirmative Action

Section 6(1) of the DPDPA rigorously stipulates that consent provided by a Data Principal must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action".[3] This comprehensive definition marks a significant advancement, aiming to mitigate the use of

deceptive "dark patterns" and default opt-in mechanisms.[13] However, the subjective interpretation of terms such as "free," "specific," and "informed" is anticipated to necessitate judicial clarification for consistent and effective implementation.[13]

Notice Requirements and the Role of Consent Managers

The DPDPA mandates that any request for consent must be accompanied or preceded by a notice.[12] This notice is crucial for informing the Data Principal about the specific personal data being collected, the purpose of its processing, and the procedures for exercising their rights, including the right to withdraw consent and lodge grievances.[12] The Act further stipulates that this notice must be presented in clear, plain language, with an option to access it in English or any language specified in the Eighth Schedule to the Constitution.[13]

A noteworthy innovation introduced by the DPDPA is the concept of a "Consent Manager".[12] These are entities, registered with the Data Protection Board of India, designed to provide Data Principals with a centralized platform to grant, manage, review, and withdraw their consent provided to various data fiduciaries.[12] This mechanism aims to streamline and empower individual consent management.

"Certain Legitimate Uses": Exceptions to the Consent Principle and their Scope

While emphasizing consent, the DPDPA also delineates "certain legitimate uses" for which personal data may be processed without explicit consent.[13] These exceptions include instances where data is voluntarily provided for a specific purpose (e.g., a phone number for a payment receipt), processing by the State for benefits or services, medical emergencies, and employment-related matters.[15] This provision replaced the earlier, more contentious concept of "deemed consent".[16]

The inclusion of "certain legitimate uses" within the DPDPA creates an inherent tension with the Act's otherwise strong emphasis on explicit consent. While pragmatically intended to facilitate essential governance and service delivery, a broad interpretation of these exceptions could inadvertently dilute individual autonomy and the constitutional right to privacy, especially if they become a *de facto* bypass for the challenges of obtaining meaningful consent in practice. The DPDPA requires stringent "free, specific, informed, unconditional, unambiguous" consent [13], yet simultaneously permits "certain legitimate uses" where consent

is not required.[13] If data fiduciaries find it increasingly difficult to obtain "meaningful consent" due to consent fatigue and India's digital literacy challenges [3], there is a strong incentive for them to increasingly rely on the "legitimate uses" provisions. This could lead to a *de facto* shift away from consent as the primary basis for data processing, potentially eroding the very individual control and informational self-determination that *Puttaswamy* sought to protect.[6] The courts will play a critical role in narrowly interpreting these "legitimate uses" to prevent them from becoming a loophole that undermines the constitutional protection afforded to personal data. This highlights a potential legislative trade-off between administrative efficiency and the full realization of individual privacy rights. It necessitates careful judicial oversight to ensure that such exceptions do not inadvertently diminish the constitutional protection afforded to personal data.

The Right to Withdraw Consent and its Practicalities

The DPDPA significantly strengthens the Data Principal's right to withdraw consent, explicitly mandating that the ease of withdrawing consent must be comparable to the ease with which it was initially granted.[13] This crucial provision is designed to counteract "dark patterns" that intentionally complicate the withdrawal process, thereby empowering individuals to genuinely control their data permissions.

IV. THE PHENOMENON OF CONSENT FATIGUE: MANIFESTATIONS AND GLOBAL IMPACT

Causes of Consent Fatigue: Over-exposition, Complex Notices, Dark Patterns, and Cookie Walls

The principal driver of consent fatigue is the overwhelming volume of consent requests that users encounter daily across various digital platforms.[4] This burden is compounded by prevalent poor privacy user experience (UX) practices, which include the presentation of excessively complex and legalistic privacy notices, the implementation of "cookie walls" (which restrict access to content unless consent is granted), and the insidious use of "dark patterns" (deceptive design elements that subtly manipulate users into making less privacy-protective choices).[4] The sheer number of websites an average user visits monthly, approximately 100, directly contributes to this over-exposition, making it nearly impossible for individuals to meaningfully engage with each consent request.[4]

Manifestations: Banner Blindness, Automatic Acceptance, Annoyance, and Decreased Trust

Individuals subjected to prolonged consent fatigue often develop "banner blindness," a tendency to automatically dismiss consent requests without engaging with their content.[4] This leads to an unthinking or automatic acceptance of terms and conditions, even when such terms may be detrimental to their privacy interests.[3] The constant interruptions inherent in these consent mechanisms also contribute to user annoyance and a significant erosion of trust in digital services and brands.[4] Users, faced with the choice of engaging with complex notices or simply clicking "accept" to access desired content, often choose the latter, thereby sacrificing informed decision-making for convenience.

Impact on User Autonomy and Privacy: The Illusion of Control

The most profound consequence of consent fatigue is the insidious erosion of user autonomy and effective privacy. When consent is rendered without genuine understanding, free choice, or conscious deliberation, it devolves into "murky consent"—a legal fiction devoid of true legitimacy and incapable of providing the "moral magic" that transforms otherwise intrusive data collection into a lawful activity.[5] This creates a dangerous illusion of control, where individuals perceive themselves as making informed choices about their data, while in reality, their decisions are often coerced, manipulated, or simply uninformed. Professor Solove incisively observes that such "murky consent" is "consent without magic" and "should authorize only a very restricted and weak license to use data".[5]

Consent fatigue fundamentally undermines the philosophical and legal bedrock of consent as a legitimizing force. It transforms consent from an active, autonomous exercise of individual will into a passive, often involuntary, act of procedural compliance, thereby creating a systemic and pervasive privacy deficit. The observation that consent fatigue leads to "banner blindness" and "automatic acceptance" [4], which Solove characterizes as "murky consent" lacking "moral magic" [5], is telling. The systemic design flaws in consent mechanisms that lead to fatigue result in consent becoming a "fictional" or "murky" concept.[5] This directly undermines the core legal and ethical purpose of consent, which is to legitimize data processing by ensuring it is based on informed, free choice. If consent is not genuinely given, the data processing built upon it lacks a legitimate foundation, leading to a "privacy deficit" where privacy is theoretically protected but practically eroded. This implies that the entire edifice of data protection,

particularly in legal systems heavily reliant on consent, is rendered precarious if consent fatigue is not effectively addressed. It necessitates a profound re-evaluation of whether consent, in its current operational form, can truly serve as the primary and constitutionally adequate basis for data processing, especially within frameworks that uphold autonomy and dignity.

Business Implications: Data Quality, Personalization, and Compliance Dilemmas

Consent fatigue extends beyond consumer detriment, posing significant negative implications for businesses. Reduced consent rates directly translate into lost opportunities for collecting valuable first-party data, resulting in diminished behavioral and analytical data, and consequently, inaccurate business insights.[4] This directly impedes effective personalization, targeted advertising, and overall ad performance. Google Analytics 4, a powerful analytics service, relies on precise data, and consent fatigue leads to less precise data and inaccurate insights.[4] Furthermore, businesses face the dilemma of collecting consent from users who do not genuinely consent, making it difficult to establish relevant Key Performance Indicators (KPIs) for measuring brand engagement.[4] Businesses are thus confronted with a critical choice: either accept compromised ad performance and targeting due to data loss and poor analytics, or risk severe penalties for non-compliance with privacy regulations.[4]

V. CONSENT FATIGUE IN THE INDIAN CONTEXT: CHALLENGES TO MEANINGFUL CONSENT

The Digital Divide and Low Digital Literacy: Exacerbating Consent Fatigue

India's profound digital divide and widespread low levels of digital literacy significantly intensify the problem of consent fatigue.[3] A considerable portion of the Indian populace remains largely uninformed about the intricacies of data privacy, rendering it "tremendously challenging and nearly impossible" for data fiduciaries to secure truly "informed" consent, as mandated by the DPDPA.[3] Even with simplified notices, the fundamental cognitive understanding of data implications and the long-term consequences of sharing personal information are frequently absent.

The socio-economic realities prevalent in India elevate consent fatigue from a mere digital inconvenience to a systemic impediment to the effective exercise of fundamental rights for a substantial segment of the population. This indicates that a purely individual-centric consent

model is inherently inequitable and fails to uphold the constitutional guarantee of privacy for all, particularly for vulnerable populations. The widespread low digital literacy and significant digital divide in India are not just practical challenges; they are causal factors that magnify the effects of consent fatigue.[3] When individuals lack basic digital understanding, even simplified privacy policies become incomprehensible, making genuine "informed" consent virtually impossible. This means the DPDPA's reliance on informed consent, despite its strong wording, is rendered ineffective for a substantial segment of the populace.[3] This creates a profound inequality in privacy rights, where socio-economically disadvantaged communities are disproportionately unable to exercise their constitutional right to informational self-determination, contradicting the

Puttaswamy court's assertion that privacy is not "a privilege for the few".[7] This necessitates a shift towards a more protective, potentially paternalistic, or collective approach to data protection in India, where the primary onus and responsibility for safeguarding privacy shifts more heavily onto data fiduciaries and regulatory bodies, rather than solely on the individual.

The "Privacy Paradox" in India: Discrepancy between Stated Values and Actual Behavior

Even among the minority of Indians who possess an awareness of privacy's significance, a notable "privacy paradox" exists, wherein many individuals readily compromise their data for the sake of convenience.[3] This disjunction between stated privacy values and actual online behavior further underscores the inherent limitations of a framework that places excessive reliance on individual consent as the primary safeguard for privacy. A PwC India survey revealing that only 16% of consumers are aware of the DPDPA further highlights this disconnect.[3]

Clickwrap Agreements and the Enforceability of Consent in a Low-Awareness Environment

The pervasive use of clickwrap agreements, where users routinely click "I agree" without reading the accompanying privacy policies, presents a particularly acute challenge in India.[3] Research indicates that a significant majority of participants accept these agreements without engaging with their content, raising serious questions about the legal enforceability and the genuine nature of such consent, especially given the critical importance of understanding data

processing consequences to mitigate risks.[3] Scholars have even labeled such agreements as "adhesion contracts" where users often accept without genuine consent.[3]

The Inadequacy of Current Consent Mechanisms for a Diverse Populace

Despite its ambitious objectives, India's consent-based data protection law struggles to adequately address the unique and complex challenges inherent in its diverse society, particularly the widespread low digital literacy and the persistent digital divide.[3] This fundamental inadequacy renders the current framework ineffective for a substantial portion of the population, necessitating a profound re-evaluation of its foundational principles and operational mechanisms. The law's over-reliance on informed consent, while well-intentioned, becomes ineffective when a significant segment of the populace remains uninformed regarding data privacy.[3]

VI. CONSTITUTIONAL IMPERATIVES: RECONCILING CONSENT FATIGUE WITH ARTICLE 21

Revisiting the Triple Test: Does Consent Fatigue Render Data Processing Unconstitutional?

The central constitutional challenge presented by consent fatigue is whether data processing predicated on such "murky" or uninformed consent can genuinely satisfy the rigorous *Puttaswamy* triple test. While the legality limb might be met by the existence of the DPDPA, the means by which consent is obtained, if demonstrably undermined by fatigue and lack of understanding, may fail the proportionality requirement, specifically the "necessity" and "fair balance" limbs.[6] If consent is not truly "free" and "informed" as stringently defined by the DPDPA [13], then the underlying processing lacks a legitimate foundation from the perspective of individual autonomy, thereby constituting an "unwarranted invasion" of privacy.

Consent fatigue exposes a profound vulnerability in the legal fiction of consent, transforming it from a robust constitutional safeguard into a mere procedural formality. This indicates that the state bears a positive constitutional obligation under Article 21 to ensure that consent mechanisms are not merely legally defined but are practically effective in upholding individual autonomy and dignity, thereby preventing the erosion of fundamental rights through systemic design flaws. The observation that consent fatigue leads to "murky consent" [5] and undermines

the "informed" and "free" aspects of consent [3] is critical. The

Puttaswamy judgment requires data processing to meet the triple test, including proportionality.[6] If consent is "murky" and not genuinely "free" and "informed," then the means by which personal data is collected and processed are inherently flawed. This directly impacts the "necessity" and "fair balance" components of the proportionality test. If individuals are effectively compelled or tricked into consenting due to overwhelming design or lack of understanding, the state's action (or its failure to adequately regulate such practices) could be interpreted as failing its positive duty to protect the fundamental right to privacy. The illusion of control [5] means the individual's constitutional right to informational self-determination [2] is not truly exercised, thus failing the "fair balance" test. This shifts the burden from individual user vigilance to state responsibility. The state cannot merely legislate a definition of consent; it must ensure that the practical conditions for meaningful consent exist. If they do not, then the state must explore alternative constitutional bases for data processing that do not rely on a flawed consent model, to avoid infringing Article 21. This calls for a fundamental re-evaluation of the current legislative framework's constitutional adequacy in protecting privacy.

The State's Duty to Protect Privacy Beyond Individual Self-Management

The *Puttaswamy* judgment, by recognizing privacy as an inherent fundamental right, imposes a positive and affirmative duty on the state to ensure that any legislative or executive action limiting privacy rigorously adheres to constitutional standards.[6] This implies that the state cannot exclusively rely on individuals to safeguard their own privacy through a model of "privacy self-management," a concept widely criticized as being beyond the practical capabilities of most individuals in complex digital environments.[18] Consequently, the state is constitutionally obliged to integrate more robust accountability measures and proactive oversight mechanisms to ensure that data fiduciaries consistently uphold elevated standards of data protection.[3] This perspective views information privacy as a "constitutive value" that helps form society and shape individual identities, placing limits on the power of both the state and community.[18]

Balancing Innovation, State Interests, and Fundamental Rights in the Digital Sphere

A critical challenge lies in achieving a delicate equilibrium between fostering technological innovation, fulfilling legitimate state interests (e.g., targeted welfare schemes, national

security), and rigorously safeguarding fundamental rights. The "certain legitimate uses" provisions within the DPDPA [15] exemplify this inherent tension, necessitating meticulous judicial interpretation to prevent their expansive application from inadvertently undermining the core principles of privacy. The state's ability to process data for public services, while beneficial, must be carefully balanced against the individual's right to control their information, ensuring that such processing remains proportionate and necessary.

VII. RETHINKING MEANINGFUL CONSENT: TOWARDS A ROBUST INDIAN DATA PROTECTION FRAMEWORK

Beyond "Notice and Choice": Shifting the Onus of Protection to Data Fiduciaries

The prevailing "notice-and-choice" model for obtaining consent has proven largely ineffective in practice, leading to "murky consent" and an illusion of control.[5] A fundamental paradigm shift is imperative, reallocating the primary onus of data protection from individuals to data collectors and processors (data fiduciaries).[18] This entails moving beyond the mere procedural act of obtaining consent to ensuring that data processing is inherently fair, responsible, and consistently aligned with the genuine interests of the data subject, irrespective of a perfunctory consent click.

Shifting the onus from individuals to data fiduciaries signifies a profound conceptual evolution from a traditional consumer-protection paradigm of privacy (where individuals are expected to protect themselves through market choices) to a human-rights based model. In this model, rights are inherent and demand proactive protection by duty-bearers (the state and data fiduciaries). This aligns seamlessly with the concept of "constitutive privacy," which views privacy not merely as an individual right but as a foundational value for a just society.[18] The widespread failure of "privacy self-management" [18] demonstrates that expecting individuals to effectively navigate and protect their privacy in complex digital ecosystems is both unrealistic and unjust. The proposal to shift the onus to data fiduciaries [20] and to view data protection as a "social good" or "constitutive value" [18] represents a critical conceptual leap. It moves from a reactive model, where the burden is on the individual to assert their rights, to a proactive, systemic responsibility model where privacy is designed into systems and practices by default. This aligns with the constitutional recognition of privacy as inherent to human dignity, rather than a negotiable commodity. This requires a fundamental re-imagining of business models and regulatory enforcement. It necessitates a move beyond mere compliance with statutory

consent forms to a deeper integration of privacy-by-design principles, ethical data stewardship, and a recognition of the inherent power imbalance between data fiduciaries and data principals.

Legitimate Purposes Test and Fiduciary Duties

An alternative approach involves implementing a "legitimate purposes test," where data use is strictly limited to what is compatible, consistent, and genuinely beneficial to consumers, and crucially, cannot be overridden by individual consent.[20] This test would permit data use for essential operational functions (e.g., servicing accounts, fulfilling orders) but would necessitate robust de-identification for broader, more innovative applications.[20] Complementing this, a "fiduciary duty" requirement would legally obligate data fiduciaries to perpetually act in the best interests of, and not detrimentally to, data subjects. This would explicitly prohibit using data for self-serving purposes that disadvantage customers or sharing data with third parties that do not prioritize customer interests.[20] This approach recognizes that individuals, particularly those in vulnerable positions, should not be required to relinquish their data protection rights to access digital services.[20]

Granular Consent and Just-in-Time Privacy Notices

To operationalize the DPDPA's requirement for "specific" and "informed" consent, the adoption of granular consent is paramount. This involves requesting separate and distinct consent for each specific category of data processing, thereby affording users greater control and transparency.[21] This approach directly combats the "too much information" aspect of consent fatigue by breaking down complex requests into manageable components. Furthermore, "Just-in-Time Privacy Notices" (JITPN) offer a practical solution by presenting privacy information precisely at the moment it is most relevant to the user, utilizing clear, concise, and jargon-free language to enhance comprehension.[23] While JITPNs face challenges, including the risk of notice fatigue [23], their design principles are critical for improving user experience and fostering more genuinely informed consent.[4] The aim is to provide privacy information at the point of data collection, before the user shares their data, enabling informed decisions.[23]

Role of Independent Third Parties and Privacy Representatives

To counteract power imbalances and prevent manipulative consent practices, the involvement

of independent third parties could be instrumental in establishing fair terms of consent.[19] Alternatively, a balanced process involving representatives of both consumers and businesses could collaboratively define acceptable consent methodologies.[19] The DPDPA's introduction of "Consent Managers" [12] represents a positive step in this direction, offering a neutral platform for individuals to manage their consent preferences. Moreover, the concept of "Privacy Representatives"—whether human or algorithmic—could be introduced to independently assess data processing models, particularly those involving artificial intelligence, for fairness, bias, and potential exclusion.[20] This is particularly relevant as AI systems often require vast amounts of data, challenging principles like data minimization, and their automated decision-making processes necessitate transparency regarding the logic involved and potential consequences for data subjects.[3]

Strengthening Regulatory Oversight and Enforcement Mechanisms

The effective functioning of India's data protection regime hinges on the establishment of a truly independent Data Protection Authority (DPA), as envisioned by *Puttaswamy* [1] and provided for in the DPDPA.[15] This DPA must possess robust powers to investigate data breaches, levy appropriate penalties, and issue comprehensive guidelines, operating free from undue political or commercial influence.[1] Furthermore, proactive regulatory supervision and the imposition of more stringent compliance obligations on data fiduciaries are essential to safeguard individuals who may lack the capacity to navigate complex data privacy issues independently.[3] The current Indian DPDP framework is observed to be plagued by challenges due to its over-reliance on consent, lax compliances for significant data fiduciaries, and lack of provisions for regulatory intervention, underscoring the need for stronger enforcement.[3]

The Imperative of Digital Literacy and Privacy Education Initiatives

While legislative and regulatory reforms are undeniably critical, their efficacy will be significantly enhanced by parallel, widespread initiatives in digital literacy and privacy education. Educating the populace about the intrinsic value of their personal data, the potential implications of data sharing, and their rights under the DPDPA is a long-term but indispensable endeavor. Such efforts are crucial for cultivating a genuinely privacy-conscious culture across India, thereby empowering individuals to make more informed decisions and rendering the concept of meaningful consent a practical reality rather than a theoretical ideal.[3] This

comprehensive approach acknowledges that legal frameworks alone cannot fully address the challenges posed by low digital literacy and a nascent privacy culture.

VIII. CONCLUSION AND RECOMMENDATIONS

Summarizing the Constitutional Challenges Posed by Consent Fatigue

The analysis demonstrates that pervasive consent fatigue, significantly exacerbated by India's unique socio-digital landscape, critically undermines the fundamental right to privacy. The erosion of meaningful consent directly challenges the principles of informational self-determination and decisional autonomy, which are central to the *Puttaswamy* legacy. Data processing predicated on "murky consent" fails to satisfy the constitutional proportionality test, thereby rendering such practices constitutionally suspect. The current reliance on individual consent, despite the DPDPA's stringent definition, proves insufficient in a context marked by low digital literacy and the "privacy paradox," where individuals often compromise their data for convenience without full comprehension. This creates a systemic privacy deficit, transforming constitutional rights into mere procedural formalities.

Proposing Policy and Legal Reforms for a Future-Ready Data Protection Regime in India

To address these profound challenges and build a future-ready data protection regime in India, a multi-faceted and integrated approach is imperative:

i. **Legislative Refinements:** There is a pressing need for precise judicial interpretation or targeted legislative amendments to narrowly define "legitimate uses" within the DPDPA. This is crucial to prevent their overreach and potential erosion of individual autonomy, ensuring they do not become a *de facto* bypass for meaningful consent. Furthermore, the development of clear, actionable guidelines within the DPDPA rules for operationalizing "free, specific, informed, unconditional, and unambiguous" consent is essential. This could include mandatory granular consent mechanisms, requiring separate consent for distinct data processing activities, and the widespread adoption of context-sensitive just-in-time notices that provide relevant information at the point of data collection.

ii. **Regulatory Empowerment:** The effective functioning of the Data Protection Board of India hinges on its genuine independence and robust enforcement powers. It is

recommended that the Board implement proactive regulatory audits and stringent accountability measures for data fiduciaries, shifting from a reactive, breach-response model to a preventative, compliance-driven framework. This proactive oversight is vital to ensure that data fiduciaries adhere to elevated standards of data protection, especially when dealing with individuals who may not fully comprehend complex privacy implications.

iii. **Technological and Design Solutions:** Advocating for the widespread adoption of privacy-by-design principles in all digital services is fundamental. This involves embedding privacy safeguards into the very architecture of systems and processes from the outset. Fostering the development of user-friendly interfaces that simplify consent mechanisms and promote transparency is also critical. Additionally, the effective implementation and public awareness of Consent Managers, as a centralized tool for individual data control, should be prioritized to empower users to manage their consent preferences efficiently.

iv. **Socio-Cultural Interventions:** Legislative and regulatory measures must be complemented by substantial, sustained investment in national digital literacy and privacy education programs. These initiatives should target all demographic segments, aiming to cultivate a genuinely privacy-aware populace. Such efforts are crucial for empowering individuals to understand the intrinsic value of their personal data, the potential implications of data sharing, and their rights under the DPDPA, thereby rendering the concept of meaningful consent a practical reality rather than a theoretical ideal.

Emphasizing a Holistic Approach to Safeguarding Digital Rights

Achieving a truly meaningful consent framework in India demands a holistic approach. This approach must acknowledge the inherent limitations of individual privacy self-management, systematically shift greater responsibility and accountability onto data fiduciaries, and be firmly anchored in strong constitutional principles and proactive, independent regulatory oversight. Ultimately, this ensures that privacy is protected not merely as a legal right, but as a fundamental and constitutive value essential for upholding human dignity and fostering a just digital society. The future of data protection in India hinges on this integrated strategy, moving

beyond superficial compliance to cultivate a robust and constitutionally sound digital ecosystem.

ENDNOTES *[BLUEBOOK 20TH EDITION]* :

1. *Supreme Court Ruling on Data Privacy: A Landmark Judgment, Intelegal, https://www.intelegal.in/supreme-court-ruling-on-data-privacy*

2. *The Right to Privacy in the Supreme Court of India, Penn Law Sch., https://www.law.upenn.edu/live/news/7450-the-right-to-privacy-in-the-supreme-court-of-india*

3. *Beyond Consent: Enhancing India's Digital Personal Data Protection Framework, Indian J.L. & Tech., https://www.ijlt.in/post/beyond-consent-enhancing-india-s-digital-personal-data-protection-framework-data-protect-blog-seri*

4. *Consent Fatigue is Real: Strategies to Improve User Experience & Boost Opt-in Rates, Cookie Script, https://cookie-script.com/news/consent-fatigue-strategies-to-improve-user-experience-and-boost-opt-in-rates*

5. *Daniel J. Solove, ARTICLE, B.U. L. Rev., https://www.bu.edu/bulawreview/files/2024/04/SOLOVE.pdf*

6. *Judicial Interpretation and Data Rights in India: From Puttaswamy to the DPDP Act, 2023, Indian J. Integrated Res. L., https://ijirl.com/wp-content/uploads/2025/04/JUDICIAL-INTERPRETATION-AND-DATA-RIGHTS-IN-INDIA-FROM-PUTTASWAMY-TO-THE-DPDP-ACT-2023.pdf*

7. *Justice K.S. Puttaswamy v. Union of India, S. Asian Translaw Database, https://translaw.clpr.org.in/case-law/justice-k-s-puttaswamy-anr-vs-union-of-india-ors-privacy/*

8. *Repeal Recent Amendments to the RTI Act, 2005: Justice A.P. Shah in an Open Letter, Sabrang India, https://sabrangindia.in/repeal-recent-amendments-to-the-rti-act-2005-justice-a-p-shah-in-an-open-letter/*

9. *Evolution of the Doctrine of Proportionality: Assessing its Scope and Ambit in Relation to the Right to Privacy in India, ResearchGate, https://www.researchgate.net/publication/380296952_Evolution_of_the_Doctrine_of_Proportionality_Assessing_its_Scope_and_Ambit_in_Relation_to_the_Right_to_Privacy_in_India*

10. *India Privacy Law, Off. of Ethics, Risk & Compliance Servs., https://oercs.berkeley.edu/privacy/international-privacy-laws/india-privacy-law*

11. *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, DataGuidance, https://www.dataguidance.com/sites/default/files/in098en.pdf*

12. *Legal Update and Technology Law Analysis, Nishith Desai Assocs., https://www.nishithdesai.com/fileadmin/user_upload/Html/Hotline/Technology_Law_Analysis_Jan0625-M.html*

13. *Consent Rules Under India's Data Protection Laws 2023–25, Ahlawat & Assocs., https://www.ahlawatassociates.com/blog/consent-requirements-under-the-digital-personal-data-protection-act-2023-and-digital-personal-data-protection-rules-2025*

14. *Understanding "Consent" Under the Digital Personal Data Protection Act, 2023 (DPDPA), CISO Platform, https://www.cisoplatform.com/profiles/blogs/understanding-consent-under-the-digital-personal-data-protection-*

15. *The Digital Personal Data Protection Bill, 2023, PRS Legis. Res., https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023*

16. *India's Digital Data Protection Bill: Implications of Deemed Consent, EY, https://www.ey.com/en_in/insights/cybersecurity/india-s-digital-data-protection-bill-implications-of-deemed-consent.*

17. *What are 'Certain Legitimate Uses' Under the DPDP Act, 2023 and the Draft DPDP Rules, 2025?, Tsaaro Consulting, https://tsaaro.com/blogs/what-are-certain-legitimate-uses-under-the-dpdp-act-2023-and-the-draft-dpdp-rules-2025/ .*

18. *Contours of Data Protection in India: The Consent Dilemma, ResearchGate, https://www.researchgate.net/publication/381743009_Contours_of_data_protection_in_India_the_consent_dilemma*

19. *Is There a Role for Consent in Privacy?, Int'l Ass'n of Privacy Profs. (IAPP), https://iapp.org/news/a/is-there-a-role-for-consent-in-privacy*

20. *New Approaches to Data Protection and Privacy, CGAP, https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf*

21. *What is Granular Consent?, CookieServe, https://www.cookieserve.com/knowledge-base/cookie-consent-and-compliance/what-is-granular-consent/*

22. *Granular Consent, Enzai, https://www.enz.ai/learn/glossary/granular-consent*

23. What are Just-in-Time Privacy Notices?, PrivacyEngine, https://www.privacyengine.io/resources/glossary/just-in-time-privacy-notice/.