Page 416 - 433 **DOI:** *https://doij.org/10.10000/IJLSI.112633*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 3

2025

From Click to Contract: The Legal Validity of Consent in India's Social Media Data Ecosystem

ABHISHEK SHARMA[1]

ABSTRACT

In today's digital age, social media platforms function not only as communication tools but also as avenues for extensive data collection and behavioural profiling. While consent remains a fundamental principle in contract law and data protection frameworks, it often manifests as a routine checkbox, frequently agreed to without full comprehension or deliberate choice. Many users accept complex terms of service on platforms such as Facebook, Instagram, and Twitter without a clear understanding of how their personal data will be utilised, shared, or monetised. This scenario invites legal and ethical reflection, especially concerning the validity of such consent under Indian law. This paper undertakes a doctrinal analysis of India's data protection and contractual legislation to evaluate whether user consent to social media terms of service meets the criteria of being "free, informed, and specific." It examines three key legislations: the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023. The paper also compares Indian legal provisions with international standards, notably the European Union's General Data Protection Regulation (GDPR), which prioritises affirmative, detailed, and revocable consent. While the GDPR imposes stringent obligations on data controllers, Indian law tends to adopt a more formal approach, often permitting reliance on nominal user consent without verifying genuine understanding or voluntariness. To address these challenges, the paper advocates for legislative amendments, proactive judicial interpretation, and comprehensive user education initiatives. Such measures could help evolve digital consent from a procedural requirement into a substantive, rights-based framework.

Keywords: *Digital Consent, Data Protection, Indian Law, Social Media, GDPR*

I. INTRODUCTION

The omnipresence of social media platforms in daily life has redefined not only communication but also the nature of privacy, autonomy, and consent in the digital age. Platforms such as Facebook, Instagram, WhatsApp, and Twitter offer "free" services that are, in truth, paid for

[1] Author is a Research Scholar at Faculty of Law, Banaras Hindu University, Varanasi, India.

 [ISSN 2581-9453]

through user data—an exchange seldom understood by the average user. This personal data, once obtained, is not only stored but also processed, shared, profiled, and monetized. The legal basis upon which such sweeping data collection rests is almost universally a form of user "consent," typically given by clicking an "I Agree" button appended to a dense, jargon-filled document that few ever read.[2] The contemporary model of consent in digital environments has raised significant discussions among legal scholars, privacy advocates, and judicial bodies. Critics argue that this model often lacks the hallmarks of free, informed, and meaningful consent. Unlike the traditional contractual framework where consent is characterised by active, voluntary, and well-informed agreement between parties of relatively equal bargaining power, digital contracts present a different scenario. Users frequently encounter non-negotiable, standard-form contracts, or adhesion contracts, with little choice but to agree to access essential services. This inherent imbalance in power and knowledge between platforms and users presents legal and ethical concerns. This paper employs a doctrinal methodology to critically evaluate whether consent obtained through digital click-wrap agreements satisfies the criteria for valid consent under Indian law. It references core doctrines of contract and privacy law, legislative materials, and judicial decisions to assess the protection afforded to users within India's social media ecosystem. Additionally, the paper conducts a comparative analysis with international benchmarks, such as the General Data Protection Regulation (GDPR), recognised globally for its robust user-centric data protection standards.

II. UNDERSTANDING CONSENT IN THE DIGITAL CONTEXT

Within the Indian legal framework, consent plays a pivotal role in establishing the validity of contracts and the processing of personal data. It is generally required that consent be free, informed, and unambiguous. However, the evolution of digital transactions, especially on social media platforms, presents distinct challenges to these traditional expectations. In the digital environment, consent is often obtained through standard-form contracts, such as "click-wrap" or "browse-wrap" agreements, where users are presented with predetermined terms that they must either accept in full to use the service or decline, thereby opting out of the service. This binary model of acceptance fails to reflect the elements of negotiation and mutual understanding traditionally expected in contract formation. Studies have shown that users rarely read, let alone comprehend, the terms they accept when using digital services.[3] This practice becomes particularly problematic when these terms include provisions about data harvesting, profiling, or sharing with third parties, all under the broad umbrella of consent. Thus, while technically legal, such practices raise significant doctrinal concerns about the

[2] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
[3] Florencia Marotta-Wurgler, "Does Contract Disclosure Matter?" (2012) 63 Journal of Institutional and Theoretical Economics 41.

authenticity of user consent.

The notion of informed consent becomes even more tenuous when examined through the lens of user experience design and behavioural psychology. Digital interfaces are often designed to "nudge" users toward consenting quickly, using interface strategies such as default settings, pre-ticked boxes, and opaque language.[4] These techniques exploit cognitive limitations and time constraints, turning what should be an act of voluntary agreement into a perfunctory ritual. As a result, the legal formality of consent is maintained, but its substantive meaning is undermined. Additionally, social media users in India may be particularly vulnerable to these practices due to limited digital literacy, language barriers, and a lack of awareness of privacy rights. This disparity between the legal standard and the practical reality further calls into question the efficacy of consent as a mechanism for regulating data usage. As Nissenbaum[5] argues, true consent must involve both comprehension and voluntariness. When these are absent, consent becomes a legal fiction—technically valid but normatively deficient.

The concept of digital consent carries significant practical implications for user autonomy and data security. When individuals consent to practices such as location tracking, access to contact lists, or biometric profiling, it may inadvertently limit their control over personal data. Additionally, such consent can lead to secondary data usage, where personal data is used beyond the originally disclosed purposes, potentially undermining the principle of informed agreement. This situation highlights the challenge in upholding the principle of purpose limitation, a fundamental aspect of privacy law, which may be compromised under the broad umbrella of user consent.

In the Indian context, judicial interpretations of consent within digital contracts are still maturing. While courts often emphasise the formal validity of contracts, this focus may sometimes miss the nuanced issues related to user comprehension and voluntary agreement. As India progresses towards a data-centric economy with increasing reliance on algorithmic decision-making, it becomes crucial to address these complexities to foster a more robust legal framework. Furthermore, digital consent frequently encompasses multiple permissions granted simultaneously. For example, a single click might authorise personal data usage for service delivery, targeted advertising, third-party sharing, and data analytics. This bundled consent model can obscure the clarity needed for genuine user autonomy and may not fully align with the standards set by international frameworks such as the GDPR. While Indian users may legally consent to their data being utilised by social media platforms, such consent may not always embody the core attributes of meaningful legal agreement. This disparity between legal

[4] Solon Barocas & Helen Nissenbaum, "Big Data's End Run Around Procedural Privacy Protections" (2014) 57 Communications of the ACM 31.
[5] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).

formalities and ethical considerations calls for a thoughtful re-examination of how consent is defined and applied within India's evolving digital legal environment.

III. THE INDIAN CONTRACT ACT, 1872 AND STANDARD FORM CONTRACTS

The Indian Contract Act, 1872 (ICA), serves as the cornerstone for governing contractual relationships in India. It outlines the essential elements required for a valid contract, such as offer, acceptance, lawful consideration, capacity to contract, and crucially, free consent. According to Section 10 of the ICA, agreements enforceable by law must be formed with the free consent of the involved parties. Section 13 defines consent as an agreement between two or more persons on the same thing in the same sense, while Section 14 further clarifies that free consent should not be influenced by coercion, undue influence, fraud, misrepresentation, or mistake. Despite being enacted in the 19th century, the fundamental principles of the ICA continue to hold significance today. Nevertheless, these principles were originally formulated without anticipating the complexities associated with digital transactions and online platforms. In contemporary settings, especially on social media platforms, consent is often acquired through standard-form contracts, commonly referred to as adhesion contracts. These contracts are typically drafted by service providers and presented to users on a non-negotiable, take-it-or-leave-it basis. While they offer efficiency, they often lack flexibility, being dense, technical, and challenging for the average user to fully comprehend.[6]

In traditional legal doctrine, contracts are founded on both assent and understanding. Standard-form digital contracts, however, pose challenges to the concept of mutual assent. When users click "I Agree" to access platforms such as social media, they often do so without fully grasping the implications of their consent. This raises concerns about whether such consent is substantive or merely formal. Indian courts have acknowledged that certain standard-form contracts may be voidable if deemed unconscionable or unfairly imposed. For instance, in *LIC of India v. Consumer Education and Research Centre*[7], the Supreme Court ruled that contracts with unconscionable terms imposed by a dominant party on a weaker party could be invalidated for being contrary to public policy.

Despite this, the application of these legal principles to digital contracts is still evolving. Courts have not extensively examined the nuances of legal capacity and informed consent within the realm of online service agreements. The prevailing assumption tends to be that clicking "I Agree" signifies voluntary consent. However, this formalist perspective may not fully account for the power imbalance between service providers and users, as well as the psychological and linguistic hurdles that may impede users from thoroughly reading or understanding the contract

[6] Randy E. Barnett, "The Sound of Silence: Default Rules and Contractual Consent," (2002) 78 Virginia Law Review 821.
[7] AIR 1995 SC 1811

terms.[8] An analysis of this situation suggests that the current interpretation of consent in Indian contract law may not fully reflect the complexities of digital transactions. The routine acceptance of standard-form contracts, often without a thorough review of their content, raises questions about the authenticity of consent. While users technically agree to the terms, factors such as limited meaningful choice and the intricate language used can make it challenging to ensure that consent is genuinely informed and voluntary.[9]

Indian law currently does not have specific statutory protections addressing unfair terms in standard-form contracts. Comparatively, jurisdictions such as the United Kingdom have established clear statutes like the Unfair Contract Terms Act 1977, enabling courts to invalidate unfair provisions in consumer contracts. The lack of a similar law in India results in limited oversight over the fairness and transparency of terms of service offered by platform providers, potentially affecting the level of protection available to users. Considering these circumstances, it may be beneficial to revisit the doctrinal understanding of consent within the framework of standard-form digital contracts. Such a revision could focus on enhancing the user's ability to comprehend, negotiate, and willingly agree to the terms. Without this critical re-evaluation, there is a risk that the Indian Contract Act may not keep pace with rapid technological advancements, which could impact its effectiveness in upholding contractual fairness.

IV. THE INFORMATION TECHNOLOGY ACT, 2000 AND ITS LIMITATIONS

The Information Technology Act, 2000 (IT Act) marked India's initial step towards regulating the digital landscape, offering legal recognition to electronic records, digital signatures, and addressing cyber offenses. Originally designed to support the growth of e-commerce and digital transactions, later amendments and associated rules have broadened its scope to encompass critical aspects such as privacy, data protection, and intermediary liability. Section 43A of the Information Technology (IT) Act holds significant importance concerning digital consent and data privacy. Introduced by the Information Technology (Amendment) Act, 2008, this provision mandates that a body corporate managing sensitive personal data or information (SPDI) is liable to pay compensation if it fails to implement reasonable security practices. Complementing this, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, provide a clearer definition of SPDI and outline procedural requirements for its lawful processing, including the necessity of obtaining user consent.[10]

[8] Nancy S. Kim, Wrap Contracts: Foundations and Ramifications (Oxford University Press 2013).
[9] Margaret Jane Radin, Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law (Princeton University Press 2012).
[10] Kovacs, A., "Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork", in *CyberBRICS*, ed. Belli, L., Springer, Cham, 2021, pp. 133–181, available at https://doi.org/10.1007/978-3-030-56405-6_4 (last visited Nov. 14, 2024).

While Section 43A establishes a framework for accountability among data processors, a doctrinal analysis highlights both its strengths and areas for improvement. The rules define "consent" in a specific, procedural manner. For instance, Rule 5(1) stipulates that consent must be obtained in writing—via letter, fax, or email—yet it does not extensively address qualitative dimensions such as whether the consent is free, informed, specific, or revocable. This indicates a solid foundational approach to data privacy, albeit with room for refinement to enhance the robustness of consent mechanisms. This stands in contrast to international norms, such as the GDPR, which provide comprehensive definitions and thresholds for valid consent. Secondly, while the rules outline certain obligations, they do not explicitly require platforms to provide data principals with comprehensive information regarding the purposes of data collection, the third parties with whom data may be shared, or the duration for which data will be retained.[11] This gap may contribute to an information imbalance between social media platforms and users. As a result, although users technically provide consent, it may not always be based on fully informed choices. Addressing this aspect could strengthen the principles of data protection and promote responsible handling of personal information.[12] Thirdly, the enforcement of Section 43A and the SPDI Rules faces certain challenges. Although the provision allows users to seek compensation for negligent data handling through adjudicating officers, this mechanism primarily operates reactively, depending on users to identify and report instances of data misuse. The absence of proactive monitoring or a dedicated sanctioning authority under the IT Act may limit the effectiveness of compliance measures. Enhancing institutional oversight could potentially improve the practical impact of Section 43A as a regulatory safeguard.[13]

The IT Act, while foundational to Indian cyberlaw, does not comprehensively address certain emerging issues in contemporary data governance. Key areas such as algorithmic profiling, predictive analytics, and cross-border data transfers are not explicitly covered. Furthermore, the Act does not provide statutory rights related to data portability, rectification, or erasure—elements that are increasingly viewed as essential to protecting informational autonomy. Although the Act mandates user consent, its effectiveness is limited as it may not always be context-sensitive or enforceable in practical scenarios. Moreover, the Act currently lacks explicit provisions for addressing unfair terms in privacy policies and terms of service. Service providers are not bound by statutory obligations to ensure that their consent mechanisms are

[11] Deven R. Desai & Joshua A. Kroll, "Trust but Verify: A Guide to Algorithms and the Law," (2017) 31 Harvard Journal of Law & Technology 1.
[12] Sabine Trepte, "The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances", *Communication Theory*, Vol. 31, No. 4, November 2021, pp. 549–570, available at https://doi.org/10.1093/ct/qtz035 (last visited Nov. 18, 2024).
[13] Anupam Chander and Haochen Sun (eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, Oxford, 2023.

accessible or considerate of the diverse linguistic and educational backgrounds of Indian users. This gap can create a disconnect between the legal formalities of consent and its substantive validity.

In conclusion, while the IT Act and its associated rules represent significant progress in establishing a cyberlaw framework in India, there is room for enhancement to fully address the complexities of digital consent and data protection in today's data-driven environment. Strengthening the statute to include comprehensive user rights and more robust enforcement mechanisms could improve its efficacy in safeguarding against exploitative data practices.

V. DIGITAL PERSONAL DATA PROTECTION ACT, 2023 – PROGRESS AND PITFALLS

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), marks a pivotal development in India's data protection framework. As the first Indian legislation solely focused on the regulation of personal data collection, storage, processing, and transfer across both public and private sectors, it aims to provide a more structured legal approach. The DPDP Act replaces the previous fragmented system under the Information Technology Act, 2000, introducing a comprehensive framework designed to enhance data protection. A notable feature of the DPDP Act is its clear emphasis on user consent as the cornerstone for lawful data processing. According to Section 6, consent must be "free, informed, specific, and unambiguous," and should be provided through a definite affirmative action. Additionally, it mandates that prior notices be communicated in clear and straightforward language, addressing long-standing concerns regarding the clarity and transparency of consent mechanisms. This provision aligns with international standards, such as Article 7 of the General Data Protection Regulation (GDPR), which also underscores the importance of affirmative, informed consent. While the DPDP Act introduces several progressive measures, it is not without its limitations. Certain doctrinal gaps may affect its effectiveness in fully safeguarding meaningful consent and ensuring robust informational autonomy. Nonetheless, the Act represents a significant stride towards strengthening data protection in India, with room for ongoing evaluation and improvement.[14]

While Section 6 outlines consent requirements, its practical application is influenced by exceptions detailed in Section 7. This provision permits data processing without explicit consent for specific "legitimate uses," such as when the data principal voluntarily provides data for a defined purpose without indicating refusal. Although this facilitates operational efficiency by allowing inferred or implicit consent, it may reduce the strictness associated with affirmative consent, raising concerns about user autonomy and the potential for retrospective justifications. The DPDP Act establishes certain rights for data principals under Sections 12 to 14, including

[14] Graham Greenleaf, "Global Tables of Data Privacy Laws and Bills 2023", available at SSRN https://ssrn.com/abstract=4405514 (last visited Nov. 22, 2024).

the right to access information about data processing, the right to correct and erase personal data, and the right to nominate a legal heir. These measures are noteworthy for promoting a user-focused data protection framework. Nonetheless, their limited scope excludes comprehensive rights like data portability and the right to object to automated decision-making, features that are integral to international standards such as the GDPR.[15]

A notable aspect of the DPDP Act is the exemption provided to the state under Section 17. This clause permits the Central Government to exempt any of its agencies from the Act's application for reasons including national security, public order, or sovereignty. While these exemptions aim to address critical national interests, concerns have been raised about their broad scope and the absence of detailed procedural safeguards or judicial oversight. This has led to discussions about the potential implications for citizens' privacy and the need to balance security considerations with accountability within a rights-based data protection framework.[16] The institutional framework of the Act presents areas that warrant careful consideration. The Data Protection Board of India, tasked with adjudicating complaints and ensuring compliance, operates under the oversight of the executive. While this structure facilitates streamlined governance, it also raises questions about the Board's independence when compared to regulatory authorities in other sectors. Ensuring a balanced enforcement mechanism will be crucial to upholding user rights effectively.

Additionally, the Act could benefit from more comprehensive provisions addressing algorithmic profiling and automated decision-making, particularly concerning social media platforms. These platforms extensively utilise artificial intelligence to analyse user behaviour for targeted advertising and content curation. Introducing statutory safeguards in this area could help mitigate potential risks related to algorithmic bias and the formation of filter bubbles, while supporting innovation and user engagement.[17]Thus, the DPDP Act represents a shift from a purely procedural to a rights-based framework. However, it faces challenges due to legislative ambiguities, enforcement weaknesses, and policy compromises. The Act's provisions for consent, while improved in clarity, need to further empower users to understand and control their digital identities. Thus, while the DPDP Act is a significant advancement, it still has room for improvement in securing data rights in the age of digital surveillance.

[15] Sushruti Verma, *A Global Review of Digital Rights: Lessons for India's Personal Data Protection Act* (June 5, 2024), available at SSRN: https://ssrn.com/abstract=4855530 (last visited Nov. 23, 2024).
[16] Kiren Nishat, "Human Rights Protections in Digital Surveillance: Balancing Security Needs and Privacy Rights", *Mayo Communication Journal*, Vol. 1, No. 1, 2024, pp. 83–92.
[17] Bart Custers *et al*., "The Role of Consent in an Algorithmic Society – Its Evolution, Scope, Failings and Re-conceptualization", in Kostas, E., Leenes, R., & Kamara, I. (eds.), *Research Handbook on EU Data Protection*, Edward Elgar Publishing, 2022, pp. 455–473, available at https://doi.org/10.4337/9781800371682.00027 and SSRN: https://ssrn.com/abstract=4331737 (last visited Nov. 24, 2024).

VI. COMPARATIVE FRAMEWORK – GDPR AND THE LEGAL BENCHMARK

An essential aspect of assessing the effectiveness of India's digital consent framework involves comparing it with international standards, particularly the European Union's General Data Protection Regulation (GDPR). The GDPR has established itself as a global benchmark for data protection laws. Its comprehensive, rights-centric approach offers an insightful contrast to India's current regulatory framework, which tends to be more formalistic and varied. The GDPR defines consent with clarity and precision. According to Article 4(11), consent must be "freely given, specific, informed, and unambiguous." Additionally, Article 7 stipulates that consent should be demonstrated through a clear affirmative action, like an explicit opt-in mechanism, and does not allow pre-ticked boxes or implied consent. This focus on active and deliberate consent helps ensure that individuals have a clear understanding and control over how their personal data is used.[18]

India's approach, as outlined in the Digital Personal Data Protection Act, 2023 (DPDP Act), has evolved with improved language but does not entirely mirror the GDPR's stringent standards. Section 6 of the DPDP Act specifies that consent must be "free, informed, specific, and unambiguous." However, provisions such as inferred consent in Section 7 may reduce the overall rigour of these requirements. Moreover, while the GDPR grants a wide range of complementary rights, including data portability, the right to erasure (commonly known as the "right to be forgotten"), and strong protections concerning automated decision-making, Indian law currently offers a more limited set of rights with notable gaps, especially in areas like algorithmic profiling and user control over automated systems.[19]

A notable distinction exists in the enforcement frameworks. Under the GDPR, strong supervisory authorities in each member state are authorised to perform proactive audits and levy substantial penalties (up to 4% of global turnover or €20 million, whichever is higher) for non-compliance. This robust enforcement structure encourages data controllers to maintain exemplary data protection standards. In contrast, India's enforcement mechanisms are still maturing. The Data Protection Board, established under the DPDP Act, may face challenges in demonstrating full independence, which could affect its effectiveness in applying stringent measures. The current regulatory setup in India suggests a comparatively lenient enforcement environment, potentially impacting the consistent application of consent requirements.[20]The disparity in user empowerment and transparency measures highlights the nuanced differences

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council, General Data Protection Regulation (EU GDPR), 2016 O.J. (L 119) 1.
[19] Graham Greenleaf, "Global Tables of Data Privacy Laws and Bills 2023", available at SSRN https://ssrn.com/abstract=4405514 (last visited Nov. 22, 2024).
[20] Sushruti Verma, *A Global Review of Digital Rights: Lessons for India's Personal Data Protection Act* (June 5, 2024), available at SSRN: https://ssrn.com/abstract=4855530 or http://dx.doi.org/10.2139/ssrn.4855530 (last visited Nov. 23, 2024).

between the two regulatory frameworks. The GDPR demonstrates a strong dedication to authentic user control through its emphasis on clear, accessible privacy notices and the stipulation that withdrawing consent should be as straightforward as granting it. In contrast, Indian platforms, guided by current contractual and statutory provisions, often consolidate multiple consent requests, thereby reducing the specificity of choices available to users. This practice can inadvertently restrict users from opting out of particular data uses without affecting their access to the entire service, which diverges from the level of detailed control advocated by the GDPR.[21]

In conclusion, the Indian legal framework has advanced in acknowledging digital consent as an essential aspect of data protection. However, its foundational principles are not as robust as those outlined in the GDPR. A comparative overview indicates that India's present system, marked by formal consent procedures and constrained enforcement capabilities, does not yet offer the extensive safeguards provided under the GDPR. To enhance this framework, India could benefit from incorporating clearer definitions, bolstering user rights, and establishing an independent enforcement body to ensure digital consent is both significant and effectively upheld.

VII. JUDICIAL APPROACH IN INDIA: CONSTITUTIONAL AND JURISPRUDENTIAL FOUNDATIONS

The right to privacy in India has undergone significant transformation over the past decade, largely due to the judiciary's expanding interpretation of fundamental rights under the Constitution. This evolution reached its zenith in the landmark Supreme Court decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[22], wherein a nine-judge bench unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution, encompassing dignity, autonomy, and informational self-determination.[23] The ruling marked a constitutional shift, establishing privacy as a necessary condition for the free exercise of individual liberty in a digital age.

The Puttaswamy judgment conceptualized privacy in three dimensions: bodily, spatial, and informational. The court emphasized that informational privacy involves control over personal data, particularly the right to make informed choices about data collection and use. The judgment explicitly acknowledged that digital consent, to be valid, must not only be formally obtained but also grounded in user autonomy and comprehension. As Justice Kaul observed, the individual must be able to meaningfully decide when, how, and to what extent data is shared

[21] Wayne R. Barnes, "Shifting Towards Boilerplate Regulation", *University of Miami Law Review*, Vol. 79, 2024, p. 1.
[22] (2017) 10 SCC 1
[23] *Justice K.S. Puttaswamy (Retd.) v. Union of India,* (2017) 10 SCC 1, *per* Justice D.Y. Chandrachud

with others.[24]

While Puttaswamy laid a strong constitutional foundation for a rights-based framework on data privacy and consent, subsequent judicial interpretations and policy implementations have yet to fully embody these principles. Courts have largely deferred to legislative processes and refrained from engaging deeply with the enforceability of consent in digital contracts. Even where data misuse or overreach by platforms is alleged, Indian jurisprudence has seldom addressed the matter through the lens of Article 21 rights, particularly the right to informational autonomy.[25] This reticence contrasts sharply with judicial approaches in other jurisdictions. For instance, European courts, particularly the Court of Justice of the European Union (CJEU), have played an active role in defining and enforcing the contours of data rights. In *Planet49 GmbH v. Bundesverband der Verbraucherzentralen*,[26] the CJEU ruled that consent obtained through pre-checked boxes is invalid, as it does not meet the threshold of active, informed participation by the user. Indian courts, however, have not yet developed comparable jurisprudence assessing whether digital contracts—especially standard-form agreements used by social media platforms—violate constitutional principles of privacy and fairness.

The current judicial landscape reveals a notable gap that diminishes the practical enforcement of constitutional principles within the realm of daily digital interactions. Although the doctrine of proportionality, endorsed in the Puttaswamy judgment as a standard for assessing privacy infringements, serves as a critical evaluative tool, its application to the data processing activities of private entities remains inconsistent. This oversight potentially exposes users to consent mechanisms that may not fully respect the balance between contractual obligations and fundamental rights. Furthermore, Indian courts have yet to thoroughly explore the compatibility of digital contracts, which often require broad, all-encompassing consent for diverse data uses, with the core values enshrined in the Constitution. The prevalent reliance on standard-form contracts in the digital ecosystem highlights the need for judicial scrutiny that transcends a purely formal approach to consent. A more nuanced evaluation should consider whether users genuinely comprehend and agree to the stipulated terms, thereby enriching the discourse on digital rights.

Despite its strong advocacy for digital privacy, the Indian judiciary has not fully leveraged its interpretive role to examine digital consent practices rigorously. Embracing a more engaged and forward-looking judicial approach could effectively bridge the divide between constitutional ideals and the realities of digital transactions, particularly concerning social media data management..

---

[24] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[25] Jyoti Bala and Amita Arora, "An Analysis of Surveillance and Data Protection with Reference to the Right to Privacy", Part 2, *Indian Journal of Integrated Research in Law*, Vol. 2, 2022, p. 1.
[26] C-673/17, EU:C:2019:801

VIII. KEY CHALLENGES IN LEGAL DOCTRINE

Despite formal recognition of digital consent in both statutory law and constitutional jurisprudence, its application within the Indian legal system remains fraught with doctrinal inconsistencies. The core challenges arise not from the absence of legal standards but from the tension between the formal requirements of consent and the practical realities of digital interactions. These challenges create a substantial gap between legal theory and user experience, raising fundamental concerns about enforceability, fairness, and the true autonomy of users in the digital sphere.

A. Illusion of Choice

A significant concern lies in the perceived autonomy offered by social media platforms. While it may seem that users have options, the reality often resembles a "take-it-or-leave-it" framework, limiting opportunities for meaningful negotiation or selective refusal. This scenario challenges the essence of voluntariness—a cornerstone of valid consent as outlined in the Indian Contract Act, 1872, and the DPDP Act, 2023. When the use of crucial services necessitates agreeing to extensive data collection policies, the concept of user choice appears influenced more by obligation than genuine independence.[27] In such cases, consent cannot be meaningfully distinguished from submission.

B. Overreach of Purpose

Another doctrinal issue pertains to the expansive and vague articulation of data processing purposes. Privacy policies of major social media platforms frequently cite broad goals such as "enhancing user experience," "service improvement," or "marketing communications" without specifying how user data will be utilized. Such generalizations violate the principle of purpose limitation, which holds that data should be collected only for clearly defined and legitimate purposes. When consent is obtained for open-ended purposes, it not only fails to be specific but also facilitates function creep—the gradual repurposing of data for unintended or unauthorized uses.[28]

C. Bundled and Blanket Consent

In most platform agreements, consent is bundled in a manner that significantly limits user choice, as users are unable to selectively accept or reject different aspects of data collection and usage. A single click authorizes access to a wide array of personal information—ranging from location and contacts to device metadata and behavioural patterns—often without granular options. This consent structure, which is ubiquitous among major platforms, runs

[27] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, (Public Affairs, New York 2019).
[28] Daniel J. Solove and Paul M. Schwartz, "An Overview of Privacy Law in 2022", 2022, available at https://scholarship.law.gwu.edu/faculty_publications/1602/ (last visited Nov. 25, 2024).

counter to the principle of informed consent and falls short of global best practices. Although Indian statutory language recognizes the need for specific consent, the prevailing practices highlight a stark discrepancy between policy and implementation.[29] When consent is structured as a binary—accept all terms or forfeit service—users are deprived of agency, rendering the contractual exchange unequal and potentially unconscionable.

D. Lack of Remedies and Legal Recourse

Even when consent mechanisms are problematic or abusive, users in India face significant legal and procedural barriers to seeking redress. This is because the enforcement bodies under existing law, such as the adjudicating officers under the Information Technology Act and the Data Protection Board under the DPDP Act, are primarily reactive and lack institutional autonomy. Additionally, the absence of collective redress mechanisms and class action provisions further weakens users' ability to challenge systemic issues in digital contracts.[30] This enforcement vacuum limits the efficacy of even well-worded statutory provisions on consent.

E. Absence of Doctrinal Distinction in Contract Law

A related challenge lies in the failure of Indian contract law to distinguish between negotiated contracts and standard-form digital contracts. The Indian Contract Act does not specifically address the imbalance of power or knowledge in adhesion contracts. Unlike jurisdictions with specific consumer protection statutes or unfair contract terms legislation (e.g., the UK's Consumer Rights Act 2015), India lacks a legal framework that allows courts to invalidate unfair terms in online service agreements. As a result, courts often apply the same doctrinal standards to both negotiated and standard-form contracts, failing to appreciate the coercive architecture of digital consent.

F. Neglect of Linguistic and Cultural Diversity

Finally, the uniformity of digital consent forms in English ignores the multilingual reality of Indian society. Many users encounter these terms in a language they cannot comprehend, yet are still deemed to have provided informed consent. This undermines the legitimacy of consent and creates a class of digitally disempowered users who are especially vulnerable to exploitative practices.[31] The doctrine of informed consent, in such a scenario, becomes a hollow standard that fails to protect the very individuals it purports to serve. These challenges

[29] Christopher Kuner *et al*., *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles* (May 4, 2021), available at SSRN: https://ssrn.com/abstract=3839645 or http://dx.doi.org/10.2139/ssrn.3839645 (last visited Nov. 25, 2024).

[30] Daniela Stockmann, "Tech Companies and the Public Interest: The Role of the State in Governing Social Media Platforms", *Information, Communication & Society*, Vol. 26, No. 1, 2022, pp. 1–15, available at https://doi.org/10.1080/1369118X.2022.2032796 (last visited Nov. 25, 2024).

[31] Payal Arora, The Next Billion Users: Digital Life Beyond the West (Harvard University Press 2016).

point to a systemic disconnect between the legal validity of consent and its substantive quality. Without addressing these core issues, Indian law risks sustaining a regime where consent is both omnipresent and meaningless—a paradox that erodes the normative foundation of user autonomy and trust in the digital ecosystem.

IX. RECOMMENDATIONS

The preceding analysis demonstrates that the legal doctrine governing digital consent in India is fragmented, outdated in parts, and inadequate for ensuring meaningful user autonomy in the digital environment. The formal recognition of consent as a prerequisite for lawful data processing has not been matched by the development of robust legal and institutional mechanisms to uphold the quality of that consent. To remedy these deficiencies and bring Indian law in line with constitutional principles and global best practices, several reforms—legislative, judicial, and administrative—are necessary.

A. Codify Clear Standards for Digital Consent

Indian legislation must go beyond formal acknowledgment of consent and define its essential attributes in precise and enforceable terms. Drawing inspiration from Article 7 of the GDPR, Indian law should codify that valid consent must be freely given, specific, informed, unambiguous, and capable of being withdrawn at any time. These principles should be directly incorporated into both the Digital Personal Data Protection Act, 2023, and the Indian Contract Act, 1872, through amendments or interpretive guidelines. Additionally, judicial interpretations must endorse these standards to ensure doctrinal coherence.

B. Introduce Unfair Contract Terms Regulation for Digital Agreements

India must adopt a specific statute or amend existing consumer protection laws to address unfair terms in digital contracts. This could follow the model of the UK's Consumer Rights Act 2015 or the EU's Unfair Contract Terms Directive. Courts should be empowered to strike down contractual clauses that are excessively one-sided, non-transparent, or that compel blanket consent to intrusive data practices. Such a law would allow judicial scrutiny of terms that are hidden in dense privacy policies or imposed without genuine user understanding.

C. Mandate Granular Consent and Real-Time Opt-Out Mechanisms

Consent should not be bundled. Platforms must be required to implement granular consent systems, allowing users to selectively agree to different categories of data processing, such as location access, biometric data, behavioural profiling, and third-party data sharing. Furthermore, users must be able to withdraw consent in real time, without suffering disproportionate consequences or service denial. The ease of withdrawing consent must mirror the ease of granting it. This principle should be enforceable through specific rules issued by the Data Protection Board.

D. Strengthen the Independence and Powers of the Data Protection Board

The current structure of the Data Protection Board under the DPDP Act lacks institutional independence and functional autonomy. It is critical to transform the Board into a quasi-judicial body with powers equivalent to regulators like the Securities and Exchange Board of India (SEBI) or the Competition Commission of India (CCI). The Board must have the authority to conduct audits, issue binding orders, and impose meaningful penalties for non-compliance. Its composition should include legal, technical, and human rights experts to ensure holistic adjudication.

E. Promote Multilingual and Culturally Sensitive Consent Mechanisms

Given India's linguistic diversity, the law must mandate that all consent notices, privacy policies, and platform terms be made available in regional languages. The language must be simple, accessible, and free of legalese. In addition, platforms should be required to adapt their consent processes to local contexts, recognizing differences in digital literacy, socio-economic status, and cultural understanding. This aligns with constitutional principles of equality and inclusiveness and ensures that consent is not only formally valid but substantively meaningful.

F. Launch Public Education Campaigns on Digital Rights

The government, in collaboration with civil society organizations, should launch comprehensive digital literacy programs focusing on consent, data privacy, and user rights. Awareness must extend beyond urban areas and include rural and marginalized communities. Empowering users with knowledge is essential to democratizing the digital space and ensuring that individuals can meaningfully engage with and assert their rights in digital contracts.

These reforms collectively aim to reframe consent not merely as a procedural gateway but as a substantive safeguard that respects user agency and constitutional values. Without such measures, the Indian legal framework will continue to endorse a superficial notion of consent, allowing invasive data practices to persist under the guise of legality.

X. Conclusion

The contemporary digital environment, dominated by data-driven technologies and ubiquitous social media platforms, has brought new urgency to the question of what constitutes valid consent under Indian law. Consent is no longer a private agreement between equal parties; it is a regulatory mechanism central to the governance of digital identity, data ownership, and individual autonomy. This paper has demonstrated that while Indian law has evolved to include consent as a cornerstone of its data protection framework, its interpretation and enforcement remain constrained by outdated doctrinal assumptions, procedural formalism, and limited institutional capacity. Through analysis of the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, it is evident that

the concept of consent in India is treated more as a procedural threshold than a substantive safeguard. Standard-form digital contracts, with their non-negotiable and opaque terms, fundamentally alter the balance of power between platforms and users.[32] These contracts undermine the classical understanding of free and informed consent, replacing it with a formality that serves corporate compliance rather than user empowerment.[33]

The limitations of this regime are not merely theoretical. They manifest in the widespread and often irreversible exploitation of personal data, behavioural profiling, and the erosion of privacy. Judicial decisions, especially the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017), have articulated a rights-based vision of informational autonomy. However, courts have yet to apply this vision to digital contracts and platform practices in a sustained and transformative manner[34] By contrasting India's approach with that of the European Union's General Data Protection Regulation (GDPR), this paper underscores the doctrinal and institutional gaps that prevent Indian users from exercising meaningful control over their data. The GDPR's insistence on affirmative, specific, and revocable consent, backed by robust enforcement, provides a valuable model for reforming India's legal landscape. To address these concerns, the paper has proposed a range of legal and institutional reforms, including codifying granular consent standards, regulating unfair terms in digital contracts, strengthening the Data Protection Board's autonomy, and enhancing public awareness through education. These measures are not merely technical adjustments; they are essential to ensuring that consent in the digital age retains its foundational legal and ethical significance.

In conclusion, the current Indian legal framework renders consent simultaneously omnipresent and ineffectual—a contradiction that weakens user rights and constitutional protections. Without doctrinal clarity, robust enforcement, and user-centric reforms, digital consent in India will remain a legal fiction. It is therefore imperative for lawmakers, courts, and civil society to rethink and reconstruct the concept of consent so that it truly reflects the values of dignity, autonomy, and justice in the digital era.

*****

[32] Margaret Jane Radin, Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law (Princeton University Press 2012).
[33] Nancy S. Kim, Wrap Contracts: Foundations and Ramifications (Oxford University Press 2013).
[34] Kiren Nishat, "Human Rights Protections in Digital Surveillance: Balancing Security Needs and Privacy Rights", *Mayo Communication Journal*, Vol. 1, No. 1, 2024, pp. 83–92.

XI. REFERENCES

1. Anupam Chander and Haochen Sun (eds.), Data Sovereignty: From the Digital Silk Road to the Return of the State, Oxford University Press, Oxford, 2023.
2. Bart Custers et al., "The Role of Consent in an Algorithmic Society – Its Evolution, Scope, Failings and Re-conceptualization", in Kostas, E., Leenes, R., & Kamara, I. (eds.), Research Handbook on EU Data Protection, Edward Elgar Publishing, 2022, pp. 455–473, available at https://doi.org/10.4337/9781800371682.00027 and SSRN: https://ssrn.com/abstract=4331737.
3. Christopher Kuner et al., The EU General Data Protection Regulation: A Commentary/Update of Selected Articles (May 4, 2021), available at SSRN: https://ssrn.com/abstract=3839645 or http://dx.doi.org/10.2139/ssrn.3839645
4. Daniel J. Solove and Paul M. Schwartz, "An Overview of Privacy Law in 2022", 2022, available at https://scholarship.law.gwu.edu/faculty_publications/1602/
5. Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).
6. Daniela Stockmann, "Tech Companies and the Public Interest: The Role of the State in Governing Social Media Platforms", Information, Communication & Society, Vol. 26, No. 1, 2022, pp. 1–15, available at https://doi.org/10.1080/1369118X.2022.2032796
7. Deven R. Desai & Joshua A. Kroll, "Trust but Verify: A Guide to Algorithms and the Law," (2017) 31 Harvard Journal of Law & Technology 1.
8. Florencia Marotta-Wurgler, "Does Contract Disclosure Matter?" (2012) 63 Journal of Institutional and Theoretical Economics 41.
9. Graham Greenleaf, "Global Tables of Data Privacy Laws and Bills 2023", available at SSRN https://ssrn.com/abstract=4405514
10. Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).
11. Jyoti Bala and Amita Arora, "An Analysis of Surveillance and Data Protection with Reference to the Right to Privacy", Part 2, Indian Journal of Integrated Research in Law, Vol. 2, 2022, p. 1

12. Kiren Nishat, "Human Rights Protections in Digital Surveillance: Balancing Security Needs and Privacy Rights", Mayo Communication Journal, Vol. 1, No. 1, 2024, pp. 83–92

13. Kovacs, A., "Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork", in CyberBRICS, ed. Belli, L., Springer, Cham, 2021, pp. 133–181, available at https://doi.org/10.1007/978-3-030-56405-6_4

14. Margaret Jane Radin, Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law (Princeton University Press 2012).

15. Nancy S. Kim, Wrap Contracts: Foundations and Ramifications (Oxford University Press 2013).

16. Payal Arora, The Next Billion Users: Digital Life Beyond the West (Harvard University Press 2016).

17. Randy E. Barnett, "The Sound of Silence: Default Rules and Contractual Consent," (2002) 78 Virginia Law Review 821.

18. Sabine Trepte, "The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances", Communication Theory, Vol. 31, No. 4, November 2021, pp. 549–570, available at https://doi.org/10.1093/ct/qtz035

19. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, (Public Affairs, New York 2019).

20. Solon Barocas & Helen Nissenbaum, "Big Data's End Run Around Procedural Privacy Protections" (2014) 57 Communications of the ACM 31.

21. Sushruti Verma, A Global Review of Digital Rights: Lessons for India's Personal Data Protection Act, available at SSRN: https://ssrn.com/abstract=4855530

22. Wayne R. Barnes, "Shifting Towards Boilerplate Regulation", University of Miami Law Review, Vol. 79, 2024, p. 1

*****