INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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

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

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

ISSN: 2582-6433

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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

ISSN: 2582-6433

BEYOND 'I AGREE': REASSESSING THE CONSENT-CENTRIC FRAMEWORK OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - VIDHI SINGH

In today's digital world, each of us routinely clicks "I Agree" to privacy policies without reading them, often multiple times a day. Whether ordering food online, signing up for a social media account or downloading a mobile application users often provide consent for the collection and handling of their personal data. While the law interprets these clicks as informed and voluntary consent, these actions often reflect acquiescence to standard terms rather than a meaningful exercise of individual choice.

India's Digital Personal Data Protection Act, 2023 (DPDP Act)[1] positions consent as the foundation of its data protection framework. By conditioning the processing of personal data on free, specific, informed, and unambiguous consent, the Act seeks to place individuals, or "Data Principals," at the center of the data protection framework. Prima facie, this approach appears to align with the constitutional recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017)[2], which emphasized informational self-determination and individual autonomy, its effectiveness in practice remains open to question. Despite its central role, the effectiveness of consent in safeguarding privacy remains a matter of significant debate. The assumption that individuals can meaningfully control their personal data through consent is increasingly difficult to sustain, specifically considering today's digital economy which is characterized by information asymmetries, behavioural manipulation, and concentrated platform power. Despite the progressive objective of DPDP Act's, its emphasis on consent as the primary regulatory tool may overburden users and fail to effectively mitigate systemic privacy risks.

This article argues that although consent remains an indispensable component of data protection law, it cannot bear the full weight of privacy governance in contemporary digital markets. Data protection in the 21st century demands stronger institutional accountability

[1] Digital Personal Data Protection Act 2023
[2] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

ISSN: 2582-6433

thereby shifting the responsibility from individual users to institutions that collect, process, and profit from personal data.

The Promise of Consent

The prominence of consent within privacy regulations stems from a compelling principle that individuals must have the authority to determine how their personal information is collected, used and shared. As an expression of autonomy, consent allows individuals to govern the collection and processing of data that may expose deeply personal facets of their lives, preferences, relationships, and identities.

The DPDP Act embodies this principle. Section 6(1) [3] of the Act provides that consent must be free, specific, informed, unconditional, and unambiguous, expressed through a clear affirmative action, and limited to such personal data as is necessary for the specified purpose. Data fiduciaries are expected to give notice explaining the purposes of data processing and the rights available to individuals. The framework aims to enhance individual agency by enabling users to participate actively in decisions concerning their personal information. However, the emphasis on meaningful consent is not a novel feature of privacy regulation. The concept finds its roots in the recommendations of the Committee of Experts on a Data Protection Framework for India, chaired by Justice B. N. Srikrishna, in its 2018 report[4]. Consent as a foundational precondition for the processing of personal data was identified by the committee in its report. The report further suggested that consent must be meaningful and informed rather than just being formal. While considering certain categories of individuals, particularly children, and certain categories of information, such as sensitive personal data, are more vulnerable to misuse, the Committee further recommended enhanced safeguards, including requirements for explicit consent in appropriate circumstances.

The concept of 'Consent Manager' also originated from this committee's report. They are conceived as trusted intermediaries that would provide users with a transparent and accessible interface to manage, review, and withdraw consent for data sharing. Viewed cumulatively, these measures reflect a regulatory commitment to centering individual agency and informational self-determination within India's data protection architecture.

[3] Digital Personal Data Protection Act 2023, s 6
[4] Committee of Experts under the Chairmanship of Justice BN Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Government of India 2018)

ISSN: 2582-6433

Despite its normative appeal, feminist scholars have consistently questioned the expression of individual autonomy. In Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data (2021), Anja Kovacs and Tripti Jain[5] argue that consent cannot be viewed as the outcome of entirely free and equal individuals acting independently of social and structural influences. Relying on the insights of feminist theorists such as Catharine MacKinnon[6], Carole Pateman, and Jennifer Nedelsky, scholars argue that consent is shaped by the social and power dynamics within which individuals make choices. The significance of this critique extends beyond sexual autonomy and into the digital realm. Much like other settings characterized by unequal power relations, the digital economy is structured around significant asymmetries of information, technological expertise, and economic power between individual users and technology companies. Accordingly, the mere presence of consent cannot automatically be equated with meaningful autonomy, particularly where significant power imbalances shape individual decision-making.

In theory, such models promote transparency, accountability, and individual empowerment. If users are well equipped with information then their choices can be aligned with their preferences and privacy expectations. Individuals though must possess the time, knowledge, and bargaining power necessary to make informed decisions to maximise the effectiveness of this framework. Available evidence, however, suggests that these conditions are rarely met in practice.

The Myth of Informed Consent

One of the most significant challenges facing consent - based regulation is the problem of consent fatigue[7] whereby users are bombarded with countless requests for consent which ultimately forces them to click on the 'I Agree' or 'Accept' without reading the accompanying terms or pop-up notices. This results in consent that is neither truly informed nor genuinely voluntary.

Compounding this problem is the issue of information asymmetry.Digital platforms possess extensive knowledge about their technologies, data practices, and business models, creating a significant informational imbalance between companies and users. Comparing it to the other

[5] Anja Kovacs and Tripti Jain, Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data (Internet Democracy Project 2021)
[6] Catharine A MacKinnon, Toward a Feminist Theory of the State (Harvard University Press 1989)
[7] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev 1880

ISSN: 2582-6433

side, users often have limited understanding of how their data is used, collected and even monetized. The sheer length and technical complexity of privacy policies often render them inaccessible to the average user, undermining the possibility of genuinely informed consent.

In a landmark 2008 study, researchers Aleecia McDonald and Lorrie Cranor[8] found that reading privacy policies takes an average of 10 minutes per policy. They further estimated that if individuals were to read every privacy policy they encountered, they would need to devote hundreds of hours each year to the task. Supporting this conclusion with empirical data, the researchers noted that the average American encounters roughly 1,462 websites per year; which would require about 244 hours annually to read every policy encountered. Even though privacy policies have changed over time, the central concern endures: individuals cannot be expected to make informed decisions when information is overly complex and difficult to understand.

Given these complexities, consent often becomes a legal fiction. The existence of consent in circumstances where users agree to data practices, but majority do so without understanding their implications, may satisfy formal legal requirements while failing to achieve substantive privacy protection.

These concerns are particularly relevant in India, where rapid digitalization has introduced millions of first time users into the digital ecosystem Given disparities in digital literacy, language accessibility, and awareness of privacy risks, reliance on consent alone as a privacy safeguard appears increasingly unrealistic.

The challenge is further exacerbated by persistent digital inequalities. Despite having more than 90 crore internet users, India continues to experience significant gender and demographic disparities in digital access and participation. According to recent studies, including the JETIR Digital Literacy Report[9], only 29% of women in India are digitally literate compared to 59% of men. Against this backdrop, the assumption that users can meaningfully evaluate privacy notices and make informed choices concerning data processing becomes increasingly difficult to sustain.

[8] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543
[9] M V L Narasimham and P Keshalu, 'Digital Literacy and the Role of Employment in India' (2025) 12(3) Journal of Emerging Technologies and Innovative Research (JETIR) 352

ISSN: 2582-6433

Whatsapp''s 2021 Privacy Policy controversy[10] illustrates these concerns. The policy faced backlash from regulators and courts on the ground that users were effectively presented with a take-it-or-leave-it choice regarding the sharing of personal data within the Meta ecosystem. The Competition Commission of India (CCI) concluded that WhatsApp had abused its dominant market position and consequently imposed penalties. The dispute brought into sharp focus a broader concern: where digital platforms possess significant market power and users lack meaningful alternatives, consent may become largely formal rather than genuinely voluntary. The scrutiny directed at WhatsApp's privacy policy by courts and regulators demonstrates the shortcomings of consent-based privacy regulation. Formal agreement by users to data sharing arrangements doesn't reflect a genuine understanding of the terms or a meaningful opportunity to refuse them. As a result, consent alone is not sufficient evidence of autonomy, choice, or effective privacy protection.

Behavioural Economics and the Reality of User Decision-Making

The insights of behavioural economics suggest that individuals often do not make privacy decisions in the rational manner envisioned by traditional legal frameworks. As a result, access to information alone is insufficient. This idea is well reflected in what privacy scholars describe as the "privacy paradox." As highlighted by Ari Ezra Waldman[11], there exists a significant disconnect between individuals' stated privacy preferences and their actual disclosure behaviour. Even though individuals value privacy, they often share personal information in exchange for minor conveniences or incentives. This demonstrates that privacy decisions are influenced by behavioural biases and contextual factors. Accordingly, providing users with information and opportunities to consent does not, by itself, guarantee effective privacy protection.

Behavioral economics through the concept of present bias further explains this phenomenon. Studies demonstrate that when faced with a choice between a smaller immediate benefit and a larger future benefit, individuals often prefer immediate gratification even when it's contrary to their long term interest. This idea is reflected in Daniel Kahneman and Amos Tversky's Prospect Theory[12], which shows that individuals evaluate gains and losses in subjective rather

[10] In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users, Suo Motu Case No 01 of 2021(Competition Commission of India)
[11] Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age (Cambridge University Press 2018)
[12] Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47

ISSN: 2582-6433

than strictly rational terms. Further this illustrates that privacy decisions are influenced by behavioural biases and contextual factors

Moreover, user behaviour is increasingly influenced by digital interfaces. The use of pre-selected options, visually prominent acceptance buttons, and confusing rejection pathways can force individuals toward choices that favour data collection. Such practices and manipulative interfaces are referred to as 'dark patterns' which exploit behavioural biases and reduce consumers' ability to make informed decision making. The Central Consumer Protection Authority (CCPA) issued the Guidelines for Prevention and Regulation of Dark Patterns, 2023[13], which identify and prohibit a range of manipulative design practices, including Forced Action, Basket Sneaking, and Confirm Shaming. The Guidelines classify such practices as unfair trade practices and seek to protect consumer autonomy in digital environments. Furthermore, CCPA has repeatedly directed digital and e-commerce platforms to conduct self-audits and eliminate these manipulative interfaces accompanied by a declaration confirming that their platforms are free from dark patterns[14].

The capacity of the consent to function as a meaningful safeguard becomes increasingly questionable if it is influenced by cognitive limitations and deliberately engineered interface designs. Dark pattern regulation therefore highlights a broader reality that privacy protection cannot depend solely on individual consent, but must also address the structural and design choices made by digital platforms.

The problem of unequal bargaining power

The notion of consent is premised on the existence of meaningful alternatives and the idea of voluntary choices. Yet in many digital markets, the absence of meaningful alternatives limits users' ability to refuse data practices without sacrificing access to essential services.

Tech giants such as Google, Meta and Amazon have become deeply integrated into everyday

Econometrica 263

[13] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023

[14] Ministry of Consumer Affairs, Food and Public Distribution, 'Central Consumer Protection Authority Issues Advisory to E-Commerce Platforms for Self-Audit Within 3 Months to Detect Dark Patterns and Ensure Its Resolution' (Press Information Bureau, 7 June 2025) https://consumeraffairs.gov.in/public/upload/admin/cmsfiles/pressRelease/Central_Consumer_Protection_Authority_issues_advisory_to_E-Commerce_Platforms_for_self-audit_within_3_months_to_detect_Dark_Patterns_and_ensure_its_resolutionpress_release.pdf

ISSN: 2582-6433

life, influencing communication, commerce, education and employment. Even if users switch to alternative options, data dependent ecosystems and network effects make such alternatives impractical. In the context of the Digital markets Act[15],The European commission recognized that these firms tend to operate as digital gatekeepers and control key services such as search engines, app stores and operating systems. Accordingly, consent is frequently procured in contexts characterized by substantial inequalities in economic and bargaining power, raising questions to its voluntary nature.

One of the most common and useful illustrations could be that of messaging applications where even if a user disagrees with certain data practices, the decision to leave a widely adopted service often results in the loss of access to important social, professional or educational networks. Consider messaging applications. A user may object to certain data practices, but abandoning a widely used platform may mean losing access to social, professional, or educational networks. Similar dynamics exist in relation to search engines, online marketplaces, and digital payment systems. Consequently, the voluntariness of the consent is limited due to the imbalance of power between users and platforms. When participation in digital life requires acceptance of extensive data processing practices, consent begins to resemble acquiescence rather than autonomous choice. This has encouraged regulatory authorities around the world to question whether privacy can be adequately protected through individual decision-making alone.

Lessons from Global Data Protection Frameworks

India is not the first jurisdiction to rely on consent as a cornerstone of privacy regulation. The European Union's General Data Protection Regulation (GDPR) [16]on the same line recognizes consent as one of the lawful bases for processing personal data. According to Article 6(1)(a) of the GDPR[17] consent must be freely given, specific, informed, and unambiguous, and is typically demonstrated through a clear affirmative act. Similarly, Section 6 of India's Digital Personal Data Protection Act, 2023 (DPDP Act)[18] requires consent to be free, specific, informed, unconditional, and unambiguous, along with a clear notice inclusive of the details regarding purpose of data collection and processing. Both frameworks therefore place

[15] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)
[16] Regulation (EU) 2016/679 (General Data Protection Regulation)
[17] GDPR, art 6(1)(a)
[18] Digital Personal Data Protection Act 2023, s 6

ISSN: 2582-6433

significant emphasis on individual consent as a mechanism for legitimizing the processing of personal data.

However, the GDPR also reflects an awareness of the limitations of consent-centric governance. Article 5(2) of the GDPR[19] requires data controllers to be responsible for, and actively demonstrate, compliance with all data protection principles which thus reveals the limitations of consent-centric governance. European regulators have increasingly embraced accountability, recognizing the limits of individual responsibility in data protection.

Obligations are placed directly on organizations through principles such as data minimization, purpose limitation, privacy by design, and organizational accountability. Rather than relying predominantly on individual users to protect their privacy, it seeks to ensure that data processing practices are fair, proportionate, and necessary from the outset.

Taken together, developments across jurisdictions increasingly demonstrate that effective privacy protection cannot rest solely on individual choice but requires robust institutional safeguards and accountability mechanisms.

Moving Beyond Consent

The DPDP Act is an important milestone in India's digital governance framework. Though, present evidence suggests in today's competitive and complex digital environment, consent alone is insufficient. A widely cited study by McDonald and Cranor as discussed earlier in this article highlighting the practical limitations of informed consent as a regulatory safeguard.

I. At the outset, emphasis on organisational accountability is necessary. Responsibility for demonstrating that data processing practices must be borne by data fiduciaries as these are necessary, proportionate, and privacy-conscious. This is also aligned with the international regulatory framework. A notable example is the GDPR's accountability principle, which places responsibility directly on organizations to both adhere to and demonstrate compliance with data protection standards.

II. Privacy by design must be promoted by the regulators which will ensure that privacy protections are embedded into technological systems from the beginning instead of burdening users to navigate complex choices. Research shows that users rarely change

[19] GDPR, art 5(2)

ISSN: 2582-6433

default settings, thus making system design an important factor in determining privacy outcomes. Thus privacy protections embedded into products by default can be more effective than repeated consent requests. This view is also supported by a Carnegie Mellon University study[20] which argued that reading every privacy policy encountered would require approximately 76 workdays per year, highlighting the practical limits of informed consent.

III. Research by behavioral economists including Alessandro Acquisti [21]suggests that interface design can significantly shape user decisions. This perspective is reflected in MIT research[22] showcasing that individuals spend an average of only seven seconds on cookie banners, a period insufficient for making an informed choice. As a result, users often select the easiest option, such as clicking "Accept All." Thus, stronger restrictions on dark patterns and manipulative interface design are essential.

IV. Finally, India should adopt a more risk-based approach to data governance. High-risk processing activities like large-scale profiling, behavioural advertising, facial recognition, and AI driven decision making should be subject to enhanced regulatory scrutiny regardless of formal consent. International frameworks are increasingly moving in this direction. For instance, Article 35 of the GDPR[23] mandates Data Protection Impact Assessments (DPIAs) for high-risk processing, EU's AI Act [24]imposes heightened compliance safeguards for high-risk artificial intelligence systems. In a similar vein, the UK's Information Commissioner's Office (ICO)[25]treats large-scale behavioural profiling and systemic monitoring as high-risk activities warranting enhanced oversight. These trends highlight an emerging consensus that some data processing activities present risks beyond the scope of consent-based protection and require enhanced institutional safeguards.

Together these measures would reduce the burden placed on individuals and instead place greater responsibility on organizations best equipped to identify, assess, and mitigate data-

[20] Daniel Tkacik, 'Website Sheds Light on Shortcomings of Privacy Policies' (Carnegie Mellon University, 11March 2016)
[21] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behaviour in the Age of Information' (2015) 347 Science 509
[22] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger and Lalana Kagal, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence' (CHI Conference on Human Factors in Computing Systems, Honolulu, Hawaii, 25–30 April 2020)
[23] GDPR, art 35
[24] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)
[25] Information Commissioner's Office, Data Protection Impact Assessments (ICO Guidance)

ISSN: 2582-6433

related risks. In a digital landscape defined by informational asymmetries, manipulative design practices, and concentrated platform power, the protection of privacy requires accountable institutions alongside informed users.

Conclusion

The Digital Personal Data Protection Act, 2023 marks a significant step in India's journey towards a comprehensive data protection framework. By positioning consent as the foundation of its framework, the Act seeks to empower individuals and give effect to the constitutional right to privacy. Yet, as this article demonstrates, meaningful privacy protection cannot be founded exclusively on the assumption that individuals possess the capacity to understand and negotiate intricate data processing arrangements.

The disconnect between theory and practice is evident. While studies suggest that meaningful engagement with privacy policies would require hundreds of hours each year, behavioural research consistently shows that users spend only seconds reviewing consent notices before providing their consent.

Digital literacy gaps, information asymmetries, dark patterns, and platform dominance weaken the assumption that consent is always informed and voluntary. As a result, clicking “I Agree” often reflects convenience or necessity rather than genuine choice.

Regulatory frameworks across jurisdictions increasingly recognise these challenges. The GDPR’s accountability regime[26], privacy-by-design obligations, and risk-based regulatory mechanisms for high-risk processing activities collectively signal that effective privacy protection cannot be achieved through individual choice alone. Rather, it requires institutions that collect, process, and profit from personal data to proactively identify and mitigate risks.
As India’s digital participation expands, the stakes of data governance will only become more significant. Excessive reliance on individual consent may place the burden of privacy protection on individuals who are often ill-equipped to manage the associated risks.

Accordingly, effective privacy regulation requires not the abandonment of consent, but a

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 5(2)

ISSN: 2582-6433

realistic appreciation of its limitations as a regulatory tool. Consent should remain an important safeguard, but it must be supported by stronger accountability, privacy-by-design requirements, restrictions on dark patterns, and risk-based oversight. Meaningful privacy protection depends not merely on obtaining consent, but on ensuring that individuals remain protected even after they have given it.