CONSENT IS NOT CONTROL: RETHINKING INDIVIDUAL CHOICE UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION FRAMEWORK

by

Pratham Bhardwaj[1]

ABSTRACT

The growing use of digital platforms has made the collection and processing of personal data a part of everyday life. While consent is often treated as the primary means of protecting individual privacy, the reality is more complicated. Lengthy privacy policies, limited alternatives and unequal bargaining power can make it difficult for individuals to understand what they are agreeing to or to exercise genuine control over their personal information. This article examines the consent framework under India's Digital Personal Data Protection Act, 2023, in light of the constitutional recognition of privacy by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India. It argues that consent remains important but cannot, on its own, provide adequate protection in a digital environment where individuals may lack the information or practical freedom needed to make informed choices. The article therefore emphasises the need for clear privacy notices, responsible data processing, accessible grievance redressal and stronger institutional accountability. It concludes that meaningful data protection requires more than obtaining an individual's agreement; it requires a framework in which organisations are held responsible for how personal data is collected, used and protected.

IJLJ
ISSN: 2583-2794

Keywords: Digital Privacy; Data Protection; Consent; Informational Privacy; Individual Autonomy; Accountability.

[1] 2nd Year BA LLB (Hons.), Student at NMIMS Indore.

Indian Journal of Law and Jurisprudence | Licensed under Creative Commons — https://creativecommons.org/licenses/by/4.0/ | DOI: 10.5281/zenodo.23536973 | Title: Consent Is Not Control: Rethinking Individual Choice under India's Digital Personal Data Protection Framework

INTRODUCTION

Personal data has become an essential part of everyday life. Online shopping, digital payments, social networking, educational platforms and government services routinely involve the collection of information about individuals. Such information may include names, contact details, financial records and other details that reveals aspects of a person's life.

Consent is often presented as the principal means through which individuals retain control over their personal information. The underlying idea appears straightforward : a person should understand how their information will be used and should be able to decide whether to permit that use. In practice, however, this model raises a difficult question which is, does clicking an acceptance button represent a meaningful decision or does it sometime reflect the only practical way to access a service?

India's Digital Personal Data Protection Act, 2023 (DPDP Act), seeks to regulate the processing of digital personal data while recognising both individual protection and the need for lawful processing. The Digital Personal Data Protection Rules, 2025 provides us with further details concerning the implementation of the framework. Their significance must be considered alongside the statutory commencement schedule which phases the operation of the act and rules.[2]

This article examines the limits of consent as a means of protecting informational privacy. It argues that consent remains necessary in appropriate circumstances but cannot by itself ensure meaningful control. Effective protection also requires responsible data – handling practices, clear communication, accessible remedies and institutional accountability. The article examines legislation and constitutional jurisprudence on the limitations of individual privacy management.

CONSTITUTIONAL FOUNDATIONS OF INFORMATIONAL PRIVACY

The constitutional basis of privacy in India was authoritatively recognised by the Supreme Court in Justice K.S. Puttaswamy V. Union of India.[3] The court held that privacy is a constitutionally protected right under the fundamental rights framework. The judgement recognised that privacy concern is not merely secrecy but also individual autonomy, dignity and the ability to make important decisions without unjustified interference.

Informational privacy forms an important part of this understanding. Individuals disclose personal information for particular purposes but disclosure does not necessarily amount to an

[2] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025).
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

unrestricted surrender of control over that information. For example, A person who provides a telephone number to receive a delivery update has not necessarily agreed to receive unrelated marketing communications. Similarly, supplying financial information to complete a transaction does not mean that the individual has abandoned every legitimate expectation concerning its subsequent use.

The constitutional significance of informational privacy lies in the relationship between personal information and individual autonomy. Information, when collected and combined, may reveal patterns of behaviour, personal relationships, financial circumstances and other aspects or private life as well. The consequences of its misuse may therefore extend beyond embarrassment or unwanted communication. They can affect dignity, freedom of choice and a person's ability to participate confidently in social and economic life.

The Puttaswamy judgement also demonstrates that privacy cannot be understood as an absolute prohibition on information processing. Privacy interests must be considered alongside legitimate public purposes and other constitutionally relevant interests. The constitutional inquiry becomes particularly important where state action is involved while private sector processing must be assessed under the applicable statutory and legal framework. The DPDP Act represents a legislative attempt to establish rules governing digital personal data. Its effectiveness should therefore be evaluated against the broader constitutional importance of privacy without assuming that every dispute involving a private company automatically becomes a direct constitutional claim. The central question for this article is whether the legal framework gives individuals a sufficiently meaningful role in decisions concerning their information.

CONSENT UNDER THE DPDP ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), establishes a framework for processing digital personal data through specified legal grounds, including consent and certain recognised legitimate uses. Section 4 provides that personal data may be processed only in accordance with the Act and for a lawful purpose either on the basis of consent given by the individual or for certain legitimate uses recognised under Section 7.[4] This distinction is important because the Act does not make consent the exclusive basis for every instance of lawful processing.

Section 6 sets out the requirements governing consent. Under Section 6(1), consent must be free, specific, informed, unconditional and unambiguous, and must be expressed through a

[4] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4, 7 (India).

clear affirmative action.[5] It must also signify agreement to the processing of personal data for the specified purpose and be limited to the personal data necessary for that purpose. These requirements indicate that consent is not intended to be treated as a mere formality. The nature of the information requested and the purpose for which it will be processed are relevant whether the individual has meaningfully agreed to the proposed processing.

Section 5 addresses notice. It requires the Data Fiduciary to provide the individual with a notice accompanying or preceding a request for consent.[6] The notice must identify the personal data and the purpose of processing and provide the specified information concerning the individual's rights and the means of making a complaint to the Data Protection Board of India. Such requirements are intended to provide individuals with relevant information before they decide whether to consent. However, the practical value of notice depends not only on the information being provided but also on whether it is presented clearly enough to support an informed decision.

Section 6(4) provides that an individual may withdraw consent at any time and that the ease of withdrawal must be comparable to the ease with which consent was given. This provision addresses an important concern in digital environments : an individual maybe able to accept a request immediately but encounter unnecessary difficulties when attempting to withdraw permission. If implemented effectively, the statutory requirement could help prevent withdrawal mechanisms from becoming a practical obstacle to exercising individual choice. Under the commencement notification issued in November 2025, Section 6(4) together with Sections 6(1)-6(8) and 6(10) is scheduled to commence eighteen months after publication on 13 May 2027.[7]

The act also imposes distinct responsibilities on Data Fiduciaries under Section 8. Section 8(1) addresses responsibility for compliance with the Act and its Rules, while Section 8(2) addresses processing undertaken on a Data Fiduciary's behalf by a Data Processor subject to the statutory wording. Section 8(4) concerns appropriate technical and organisational measures for effective observance of obligations. Section 8(5) requires reasonable security safeguards to prevent personal data breaches and Section 8(6) addresses notification of personal data breaches to the Board and affected individuals in accordance with the provision.[8] These obligations demonstrate that the legislative framework extends beyond

[5] Id. § 6(1).
[6] Id. § 5.
[7] Ministry of Electronics and Information Technology, Notification No. G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025).
[8] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1)–(2), (4)–(6) (India).

individual consent. It also places responsibility on organisations for how personal data is processed, protected and managed.

The commencement schedule is essential to understanding the present legal position. Section 5 and the core consent provisions in Sections 6(1)-(8) are scheduled to commence on 13 May 2027. Section 6(9), concerning Consent Managers follows a separate timeline and is schedules to commence on 13 November 2026. The relevant provisions of Section 8 are also subject to the phased commencement specified in the notification. The Act and Rules must therefore be analysed by distinguishing between provisions that have been enacted, those already in force and those scheduled to become operative in the future.

The DPDP Act thus provides a framework that combines consent, recognised grounds for processing and responsibilities imposed on Data Fiduciaries. The central question is not whether consent has a role in data protection but whether the statutory safeguards and institutional responsibilities can translate formal individual choice into meaningful protection. Examining that question requires attention both to the content of the legislation and to the practical difficulties individuals may face when attempting to understand or influence the processing of their personal data.

WHY FORMAL CONSENT MAY NOT PRODUCE MEANINGFUL CHOICE

The first difficulty is the imbalance between the information available to organisations and the information available to individuals. Organisations may understand their data systems, commercial incentives and processing practices in considerable detail. Individuals, by contrast, may encounter only a short notice or a link to a lengthy privacy policy. Even where the information is technically available, the practical usefulness depends on whether it can be understood and assessed before a decision must be made.

This problem is not unique to India. Daniel J. Solove's analysis of privacy self management explains why placing responsibility on individuals to understand and negotiate every data processing decision can be inadequate. The volume and complexity of information make it difficult for people to assess the consequences of each choice meaningfully. The point is not that individuals are incapable of making decisions. Rather, the demands placed on them may be unrealistic in an environment where numerous services seek permission to collect and process information.[9]

A second difficulty concerns the difference between formal agreement and genuine choice. Consider a student who must use an online platform to access course material. The platform

[9] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

presents a lengthy privacy policy and requires acceptance before access is granted. The student may technically be free to refuse but refusal could mean losing access to an essential academic resource. In such circumstances, the existence of a choice does not necessarily establish that the individual has a realistic alternative.

This example does not prove that every compulsory acceptance mechanism is unlawful. Its significance is analytical, i.e., the meaningfulness of consent depends partly on the circumstances in which it is requested. Where services are essential or alternatives are limited, the individual's ability to negotiate may be considerably weaker than thee wording of a consent screen suggests.

Third, consent may fail to address the wider consequences of data processing. An individual might understand the immediate purpose of providing information without being able to anticipate how data will be combined, analysed or used to make later decisions. The privacy implications of a single piece of information may appear limited while the implications of combining several datasets may be substantial. Individual consent cannot reasonably be expected to resolve every concern associated with complex processing systems.

Helen Nissenbaum's account of contextual integrity offers an useful way to understand this difficulty. Her approach examines whether information flows are appropriate to the social context in which information is shared rather than treating privacy solely as a matter of individual secrecy or control. Applied cautiously to the Indian framework, this perspective highlights the importance of examining the purpose and circumstances of information use rather than asking only whether a person clicked an acceptance button.[10]

Fourth, formal rights may be weakened by practical barriers to exercising them. A withdrawal mechanism that is difficult to locate, a grievance process that is hard to navigate or an explanation written in inaccessible language may discourage individuals from acting on their rights. The DPDP Act's recognition of withdrawal and grievance redressal is therefore important but the practical value of these safeguards will depend on how effectively the relevant mechanisms function once the applicable provisions are in force.

These concerns should not be overstated. Consent remains useful, and clear notices and meaningful choices can improve individual autonomy. Nor is it realistic to expect every person to read every privacy notice in full. The problem is that a framework relying too heavily on individual attention may leave the least informed and least powerful individuals with the weakest protection.

[10] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).

The more defensible conclusion is that consent should be retained but placed within a broader system of legal accountability. Individuals should not have to become experts in data governance merely to use ordinary digital services.

FROM CONSENT TO ACCOUNTABILITY : A MORE EFFECTIVE APPROACH

A stronger approach should begin with the quality of information provided to individuals. Privacy notices should explain the relevant categories of personal data, the specific purposes of processing and the available means of exercising rights in clear and accessible language. Layered notices can help by presenting essential information first and making further details available without overwhelming the reader. Thee DPDP Rules, 2025 envisage notices that are independently understandable and sufficiently detailed to support informed consent. Effective implementation should preserve this emphasis on clarity rather than treating notice as a document produced merely to demonstrate formal compliance.[11]

Second, withdrawal should be practically accessible. Where consent can be provided through a simple interface, withdrawing it should not require an unnecessarily complicated process. A clearly labelled option, a straightforward account setting or another accessible method may help give effect to the statutory principle that withdrawal should be as easy as giving consent. Organisations should also communicate the consequences of withdrawal accurately including any processing or retention that may continue where permitted or required by law.

Third, responsibility must remain with the organisations that determine the purposes and means of processing. The Act's provisions on Data Fiduciary obligations offer an important basis for this approach. Organisations should assess whether the data they collect is necessary for the stated purpose, establish appropriate security safeguards, restrict unnecessary access and avoid retaining information beyond the period justified by the purpose or applicable legal requirements. These proposals should be implemented consistently with the actual statutory provisions rather than by assuming that every desirable privacy principle is expressly stated in identical terms in the Act.

Fourth, grievance redressal must be accessible in practice. A person who discovers that information has been mishandled should be able to identify the appropriate channel, understand the steps involved and receive a meaningful response. The effectiveness of rights depends not only on their recognition in legislation but also on the availability of remedies when organisations fail to respect them. The statutory arrangements for grievance redressal and the Data Protection Board should therefore be assessed in light of accessibility,

[11] Digital Personal Data Protection Rules, 2025, rr. 1(4), 3.

institutional capacity and the effectiveness of enforcement once the relevant provisions become operative.

Fifth, regulation should recognise that data protection involves competing interests. Excessively burdensome requirements may create difficulties, particularly for smaller organisations, while weak safeguards may expose individuals to avoidable risks. Proportionate implementation can address this tension by focusing attention on the nature of the data, the purpose of processing and the risks associated with misuse. Clear regulatory guidance can also help organisations understand their obligations without reducing compliance to a checklist.

These proposals do not require abandoning consent. They seek to give consent a more realistic role. Consent is strongest when people receive understandable information, have a genuine opportunity to refuse or withdraw where applicable and can rely on organisations to meet independent legal obligations. It is weakest when individuals are expected to bear the consequences of decisions made under conditions of uncertainty and unequal bargaining power.

The distinction between existing statutory requirements and proposed reforms must remain clear. Some measures, including accessible notices and withdrawal mechanisms follow directly from the structure of the Act & Rules. Other measures may require further regulatory guidance, institutional development or legislative change. Their precise legal basis should be established before they are presented as mandatory obligations.

CONCLUSION

Consent is an essential part of data protection but it should not be confused with complete control over personal information. The ability to accept a notice or withdraw permission does not necessarily eliminate information asymmetry, unequal bargaining power or the difficulty of anticipating how data may be used in complex digital systems.

India's Digital Personal Data Protection Act, 2023, provides a framework that recognises consent while also imposing obligations on Data Fiduciaries and establishing individual rights. Its effectiveness will depend on the quality of implementation, the accessibility of remedies and the extent to which organisations take responsibility for their processing practices. The phased commencement of the Act and Rules makes it particularly important to distinguish the framework's enacted provisions from those that are already operative.

The central issue is therefore not whether consent should be discarded, but whether it is being asked to do too much. A person should not have to understand every technical detail of data

processing to receive meaningful protection. Consent must operate alongside clear information, responsible processing, appropriate security, accessible grievance redressal and effective enforcement. Ultimately, a credible data protection framework should be judged not merely by the number of consent requests accepted, but by whether individuals can realistically understand and exercise their rights.

— I J L J —
ISSN: 2583-2794