Page: 939-959 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 4

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.409

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)
To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript Click here

THE PRIVACY PARADOX IN THE DIGITAL AGE: PRIVACY RIGHTS VS USER BEHAVIOR

Pranjal Aggarwal*, Albab Sarosh, Pratiksha Savita*****

I. ABSTRACT

The contemporary world shows increasing digital platform use to the point that it creates a basic contradiction between what people say about their privacy concerns and what they do online. Users frequently express apprehension about personal data collection while they routinely accept extensive privacy policies which grant broad application permissions and require them to disclose personal information for the sake of convenience. The privacy paradox phenomenon creates major challenges because it shows how consent-based data protection systems fail to provide effective protection against personal information misuse. The present article examines this contradiction within the Indian legal framework, with particular emphasis on the Digital Personal Data Protection Act, 2023 (DPDP Act), its notice and consent architecture, and the regulatory response to manipulative interface designs or dark patterns. The study uses only doctrinal methods to examine constitutional principles which emerge from K.S. Puttaswamy v. Union of India and relevant statutory provisions and judicial developments and the European Union's General Data Protection Regulation. The DPDP Act establishes vital protections through its consent requirements and data fiduciary duties, but its implementation faces obstacles because people do not understand their rights and how to make choices. The article proposes a shift from consent as the principal mechanism of protection towards accountability as a regulatory default, emphasising data minimisation, privacy by design, transparent notices and stronger restrictions on manipulative consent mechanisms. The study demonstrates that effective privacy protection needs to account for real human behaviour instead of depending on an unrealistic model of users who have complete knowledge of digital technology.

* 1st Semester LLM Student at Amity Law School, Amity University, Noida, Email ID – pranjalaggarwal900@gmail.com

** 1st Semester LLM Student at Amity Law School, Amity University, Noida, Email ID – khanalbab803@gmail.com

*** Pratiksha Savita, 1st Semester LLM Student at Amity Law School, Amity University, Noida, Email ID – pratikshasavita2017@gmail.com

II. KEYWORDS

Privacy Paradox; Informed Consent; Digital Personal Data Protection Act, 2023; Right to Privacy; Dark Patterns; Data Fiduciary.

III. INTRODUCTION

Digital services enable people to use their personal information as a common form of currency throughout their daily activities. People share their location data, contact information, personal photos, internet browsing records and payment details in order to use communication services, navigation applications, entertainment platforms and financial services. People show discomfort because they want to control their personal data while they need data to assess their security through surveillance and profiling. People tend to read privacy policies, but they accept them without reading and they give permission for data collection that goes beyond what their needs require while they trade their personal data for ease of use.

The "privacy paradox" describes the pattern where people disclose information against their declared privacy wishes.[1] The statement shows that someone who uses online platforms has reached their maximum capacity to make personal decisions. The statement shows that someone who uses online platforms has reached their maximum capacity to make personal decisions.

The legal importance of the paradox arises from data protection systems which permit personal data processing through their notice and consent requirements. The Digital Personal Data Protection Act of 2023 (DPDP Act) in India establishes notice obligations while defining consent requirements as free and specific and informed and unconditional and unambiguous consent which must be demonstrated through definite positive actions.[2] Its core processing provisions are scheduled to commence on 13 May 2027.[3] The effectiveness of their work depends on how well people

[1] P.A. Norberg, D.R. Horne and D.A. Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors' (2007) 41(1) *Journal of Consumer Affairs* 100–126.
[2] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 5 and 6.
[3] Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), dated 13 November 2025, *The Gazette of India*, Extraordinary, Part II, sec. 3(i).

comprehend the presented information and how they evaluate outcomes and process information when faced with excessive difficulties. The process of obtaining consent through extended or complicated interfaces achieves click-based requirements yet does not provide authentic approval. The interface design which compels users to reveal information creates a more serious problem.

The matter at hand involves constitutional matters which extend beyond simple contractual obligations and consumer protection rights. The Supreme Court established privacy rights as fundamental rights through its decision in Justice K.S. Puttaswamy (Retd.) v. Union of India by recognizing privacy rights as part of the guarantees of life and personal liberty and other basic human rights. The judgment treated informational privacy, autonomy and dignity as interconnected constitutional interests, and established that privacy intrusions require three conditions- legality and legitimate aim and proportionality- to demonstrate their validity.[4] The existence of clear consent does not provide sufficient proof to determine if informational autonomy rights have been maintained.

The study evaluates the effectiveness of DPDP Act consent requirements with consumer protection regulations against dark patterns to assess their ability to protect user privacy rights. The research analyzes constitutional principles together with legal requirements and court rulings while using the European Union General Data Protection Regulation as a reference point. The central inquiry is whether Indian law places excessive protective responsibility on users and whether stronger duties on data fiduciaries are required.[5]

A. Statement of Problem

The processing of personal data according to Indian data protection law requires individual consent as its legal foundation. However, actual conditions for obtaining consent from people do not allow them to make informed decisions based on free will. Users constantly face lengthy notifications which use complex terminology and

[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[5] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, F. No. CCPA-1/1/2023-CCPA (Reg), dated 30 November 2023; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

© 2026. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

require them to give permission multiple times while interface designs create situations where users find it easier to accept than to decline. The process of deliberation suffers because consent fatigue and information asymmetry together with the immediate attractiveness of digital convenience.

When users lack both understanding of how their data will be used and the ability to refuse consent their agreement functions as official permission instead of genuine control over their personal information. The resulting difficulty exists at both constitutional and regulatory levels because a framework designed to protect privacy rights forces protection responsibilities onto people who lack the ability to evaluate complicated data handling practices. This article evaluates whether Indian law effectively resolves the fundamental problem and identifies necessary doctrinal and legislative changes.[6]

B. Research Questions

The research is guided by the following questions:

1. What is the legal basis of the right to privacy in India, and how does it relate to the idea of individual autonomy and choice?
2. How does the Digital Personal Data Protection Act, 2023 structure notice and consent, and what assumptions about user behaviour does it make?
3. How do manipulative interface designs, commonly identified as dark patterns, and consent fatigue undermine the validity of consent, and how does Indian law currently respond?
4. What doctrinal or legislative reforms would better align privacy protection with actual user behaviour?

C. Research Objectives

The principal objectives of this research are:

1. To examine the constitutional foundation of informational privacy and the autonomy rationale underlying individual consent.

[6] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347(6221) Science 509–514.

2. To analyse the notice and consent provisions of the Digital Personal Data Protection Act, 2023, and critically examine the behavioural assumptions underlying their operation.
3. To assess the legal responses to manipulated and fatigued consent, particularly through consumer-protection legislation and the Guidelines for Prevention and Regulation of Dark Patterns, 2023.
4. To recommend doctrinal and legislative reforms that reduce excessive dependence on individual consent where behavioural conditions make it an unreliable mechanism of privacy protection.

D. Research Methodology

The research uses only doctrinal methods for its investigation.

The primary sources of the study include Article 21 of the Constitution and the Digital Personal Data Protection Act of 2023 and the Digital Personal Data Protection Rules of 2025 and the Consumer Protection Act of 2019 and the Dark Patterns Guidelines of 2023 and the Information Technology Act of 2000 together with its related subordinate legislation and court rulings.[7]

The secondary materials used for this study include the Justice B.N. Srikrishna Committee Report (2018) and academic commentary and behavioural-economics literature which investigators utilized to explain the privacy paradox without producing empirical results. The researchers examined statutory provisions through textual analysis and contextual examination while using the GDPR as a partial comparison. The researchers chose not to conduct any surveys or interviews or experiments or independent empirical research.

[7] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023); the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated November 13, 2025; the Consumer Protection Act, 2019 (Act 35 of 2019); the Information Technology Act, 2000 (Act 21 of 2000); the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 5; the Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. CCPA-1/1/2023-CCPA (Reg), dated November 30, 2023; Regulation (EU) 2016/679 (General Data Protection Regulation).

E. Research Hypothesis

The main hypothesis which this study investigates asserts that the Digital Personal Data Protection Act 2023 the consent-based design system requires to function needs users who make informed decisions about their digital activities yet this requirement conflicts with established research findings about human behavioral patterns which include bounded rationality and consent fatigue and information asymmetry and the ability to be manipulated by interface design elements.

The Act requires data fiduciaries to meet accountability standards which the consumer protection rules against dark patterns operate as a partial solution to existing deficiencies because those requirements create a need for customers to provide their consent under all circumstances. The current system which uses consent as its primary protective mechanism results in organizations meeting basic legal requirements while failing to provide proper protection of citizens' constitutional rights to control their personal information.

F. Literature Review

The privacy paradox emerges when people declare their concern about privacy yet proceed to share personal information. Norberg, Horne and Horne identify the difference between intended and observed disclosure, while Acquisti, Brandimarte and Loewenstein explain that privacy decisions are shaped by uncertainty, context, malleable preferences and cognitive limitations.[8]

The accounts show that disclosure does not always function as a stable preference which people fully understand. Users who experience consent fatigue and immediate-benefit bias together with bounded rationality will select service access over understanding data processing long-term impacts. The problem escalates because platforms possess better knowledge of their data handling methods than users do.[9]

[8] P.A. Norberg, D.R. Horne and D.A. Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors' (2007) 41(1) Journal of Consumer Affairs 100–126; Alessandro Acquisti, Laura Brandimarte and George Loewenstein, supra note 6.

[9] Masooda Bashir, Carol Hayes, April D. Lambert and Jay P. Kesan, 'Online Privacy and Informed Consent: The Dilemma of Information Asymmetry' (2016) 52(1) Proceedings of the Association for

The primary legal framework for regulation which depends on notice and consent has been found to be insufficient according to legal scholars. The lengthy and intricate notices create significant expenses for users who need to read and understand them because they must read through multiple requests which lead to automatic acceptance.

The Justice B.N. Srikrishna Committee recognized that consent cannot be the sole basis for all legitimate processing and recommended additional grounds which should be used together with a system that designates data processors as fiduciaries who must use information responsibly and for specific purposes.[10] The required protection needs to establish binding responsibilities which do not depend on a person's ability to negotiate all data handling procedures.

The constitutional scholarship following the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* establishes informational privacy as a fundamental right which protects human dignity and individual freedom and personal decision-making rights.[11] User privacy extends beyond their current agreement since it includes both their decision-making process and their capacity to manage their private data.

The study of dark patterns demonstrates that interface design allows users to be manipulated through techniques such as forced action, confirm-shaming, and interface interference. The Central Consumer Protection Authority's 2023 Guidelines transform specific consumer protection concerns into official standards, yet their implementation differs from the requirements of a data protection assessment which determines valid consent.[12]

The existing literature thus provides two behaviour-based explanations and two critiques of consent-based regulation and three separate studies of constitutional

Information Science and Technology 1–10; Daniel J. Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880–1903.

[10] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018).

[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[12] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. CCPA-1/1/2023-CCPA (Reg), dated November 30, 2023.

privacy rights. This article addresses the intersection: it tests India's statutory consent architecture, fiduciary duties and dark-pattern responses against the behavioural conditions under which digital consent is actually obtained. The analysis asks whether statutory duties can correct these weaknesses without eliminating meaningful individual choice.

IV. LEGAL AND JUDICIAL ANALYSIS

The privacy paradox creates a basic problem which challenges the legal belief that people can effectively safeguard their private data through personal decision-making. The data protection framework requires informed consent, but its actual value depends on the situations in which people give their consent. The analysis of this conflict in India requires examination of constitutional privacy rights through the Digital Personal Data Protection Act 2023 DPDP Act and consumer protection laws and developing legal standards for digital platforms.

A. Constitutional Foundation of the Right to Privacy (RQ1)

The constitutional foundation of informational privacy lies principally in Article 21 of the Constitution of India, which guarantees the right to life and personal liberty. The nine-judge Constitution Bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India* declared privacy as a fundamental right after rejecting the argument that privacy only existed as an implied interest lacking constitutional protection.[13] The judgment established that privacy rights exist through the protection of dignity and individual autonomy and personal liberty which enables people to control their fundamental life elements.

The Court recognized informational privacy as a separate element of the right. The collection and use of personal information constitutes constitutional matter because such data reveals a person's identity together with their preferences and relationships and their typical patterns of behavior. The protection of privacy rights now includes the right to defend oneself against physical intrusions together with the right to

[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

control how others use and share their personal data.[14] The judgment also articulated a three-fold proportionality requirement for State interference because it required three elements which included the legal basis for State actions and the legitimate purpose of State actions and the need to balance operational methods against the intended goals. The State must additionally ensure adequate procedural safeguards against abuse.[15]

The relevance of this constitutional understanding becomes apparent when consent is examined in digital environments. A user's acceptance of contractual terms cannot automatically establish that informational autonomy has been meaningfully exercised. The visible choice which people make under circumstances where they cannot refuse and their real freedom to choose are both conditions which exist.

The Delhi High Court evaluated the legal objections against WhatsApp's 2016 privacy policy modifications together with its Facebook data sharing regulations in *Karmanya Singh Sareen v. Union of India.*[16] The Court did not finally adjudicate the existence or scope of the fundamental right to privacy. The Court evaluated the private service terms challenge because Puttaswamy case reference was still pending at that time. The Court ordered that user information must remain confidential when users delete their accounts before the specified date and Facebook must not receive any user information that exists before 25 September 2016.[17] The decision shows how hard it is to protect privacy rights because three elements contract terms platform requirements and actual options for customers to choose from work together to create this challenge.

B. Consent Architecture under the DPDP Act (RQ2)

The DPDP Act establishes consent as the main requirement for data processing activities. The first section of the law requires organizations to provide dual information which explains the data they collect and the specific purposes they intend to use the data. The first section of the section 6 requirements mandates that all parties

[14] Ibid.
[15] Ibid. See also *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.
[16] *Karmanya Singh Sareen v. Union of India*, MANU/DE/2607/2016 (Delhi High Court, September 23, 2016).
[17] Ibid., W.P. (C) No. 7663 of 2016, judgment dated September 23, 2016.

must receive information in their native language while the section prohibits any form of consent that lacks clear affirmative approval. The section 6 requirements mandate organizations to provide content through plain language which users can access in either English or an approved Eighth Schedule language. The sections from 6(4) to 6(6) establish the right to withdrawal while processing must stop except for permitted legal situations. The section 6(7) regulations enable organizations to administer consent through a Consent Manager while section 6(9) handles registration procedures. The Data Fiduciary must present evidence that both notice and consent procedures occurred according to section 6(10).[18]

The Act establishes consent as its primary foundation but contains multiple additional grounds for its legal operation. Section 7 permits specified legitimate uses without consent, including certain voluntarily provided data and processing connected with State functions or legal obligations. The Section 8 document establishes requirements for processors and security measures and procedures about breach notification and data disposal. Section 9 requires verifiable parental consent for children's data and restricts tracking, behavioural monitoring and targeted advertising directed at children.[19]

The architecture design assumes that users have the ability to comprehend notifications and they will choose to stop processing work. The 2025 Rules require presentation through Rule 3 which mandates a separate notification together with detailed data description and defined purposes and visible methods for withdrawal and redress.[20] The notice and core consent requirements have not yet started their implementation. The G.S.R. 843(E) regulation establishes that sections 3 to 5 and section 6(1) to (8) and (10) together with sections 7 to 17 will start their enforcement eighteen months after 13 November 2025 which results in a start date of 13 May 2027. The start date for Section 6(9) and Rule 4 regarding Consent Manager registration will

[18] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 5 and 6(1), 6(3)–(7), 6(9) and 6(10).
[19] Ibid., ss. 7, 8 and 9.
[20] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Rules, 2025*, G.S.R. 846(E), dated November 13, 2025, r. 3.

begin one year after 13 November 2026.[21] Notification needs to be separated from the time when full operations start.

C. Manipulated and Fatigued Consent (RQ3)

The Consumer Protection Act, 2019 prohibits unfair trade practices and gives the Central Consumer Protection Authority power to stop consumer harm. The Dark Patterns Guidelines, 2023, issued under section 18, define dark patterns as deceptive interface practices that impair consumer autonomy, decision-making or choice. The regulations prohibit three specific practices which include forced action and confirm-shaming and interface interference.[22] The rules can handle designs which force users to share their information while hiding their options for protecting their privacy. The rules do not establish an entire framework for validating consent through data protection assessment.

Competition law provides another viewpoint. The Competition Commission of India determined WhatsApp engaged in abusive practices when it evaluated the 2021 privacy policy through its order which it issued on 18 November 2024 and imposed a fine of Rs 21314 crore for the take-it-or-leave-it data sharing requirement.[23] The NCLAT decision from 4 November 2025 confirmed the existence of unfair conditions and market denial which led to the imposition of penalties and most remedial measures. The 15 December 2025 clarification order confirmed that all remaining opt-out options and transparency solutions would apply to both advertising and non-advertising data sharing practices.[24] The Supreme Court dismissed the interim-stay

[21] Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), dated November 13, 2025, *The Gazette of India*, Extraordinary, Part II, sec. 3(i); Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Rules, 2025*, G.S.R. 846(E), dated November 13, 2025, r. 1(3)–(4).

[22] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, F. No. CCPA-1/1/2023-CCPA (Reg), dated November 30, 2023, cls. 2, 3 and 4, read with Annexure I; the Consumer Protection Act, 2019 (Act 35 of 2019), ss. 2(47) and 18.

[23] Competition Commission of India, *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users*, Suo Motu Case No. 01 of 2021, along with Case Nos. 05 and 30 of 2021, order dated November 18, 2024.

[24] *WhatsApp LLC v. Competition Commission of India*, Competition Appeal Nos. 1 and 2 of 2025, National Company Law Appellate Tribunal, judgment dated November 4, 2025; *WhatsApp LLC v. Competition Commission of India*, I.A. No. 6817 of 2025 in Competition Appeal (AT) No. 1 of 2025, National Company Law Appellate Tribunal, order dated December 15, 2025.

applications in February 2026 because the appellants had withdrawn their requests while the appeals remained pending.[25] The litigation shows how platform dependence can make consent coercive.

The Information Technology Act, 2000 and the SPDI Rules, 2011 establish an existing framework which governs sensitive personal data by requiring organizations to obtain consent and maintain privacy policies. The DPDP Act will remove Section 43A through its implementation of Section 44(2) which will take effect on 13 May 2027. The earlier regime remains relevant.[26]

D. Comparative Aid: The GDPR (RQ4)

The GDPR presents an effective comparative benchmark. Article 4(11) defines consent as a freely given, specific, informed and unambiguous indication of wishes. The requirements of Article 7 demand that consent must be shown through demonstrable evidence together with requests which must be accessible and withdrawal must be as simple as granting consent. Article 6 recognizes that lawful bases exist beyond consent which include contract and legal obligation and legitimate interests.

The requirements of Article 25 mandate data protection through design and default settings which establish controllers as responsible for preventive measures.[27] The lesson states that system designers and legal boundaries should protect privacy rights because users cannot effectively manage their security when faced with complex system designs. The service becomes essential because users have no practical options to switch to similar services.

V. CRITICAL ANALYSIS AND ORIGINAL CONTRIBUTION

The privacy paradox shows people make different privacy choices because their online behavior does not match their privacy statements. The way people interpret the

[25] *Meta Platforms, Inc. v. Competition Commission of India*, Civil Appeal Nos. 301–302 of 2026 and connected matters, Supreme Court of India, order dated February 23, 2026.
[26] The Information Technology Act, 2000 (Act 21 of 2000), s. 43A; the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rr. 4 and 5; the Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 44(2); Notification G.S.R. 843(E), dated November 13, 2025.
[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (General Data Protection Regulation), arts. 4(11), 6, 7 and 25.

situation shows incomplete understanding of the matter. The approach will lead to an individual failure assessment of a problem that exists at a structural level. Users may value privacy and still disclose personal information because digital services are embedded in education, employment, banking, communication and ordinary social participation. All active platforms create practical costs for users who must either accept platform terms or find alternative ways to access their preferred services. The paradox shows users whose privacy needs remain unfulfilled. The study shows people make privacy choices when they exist in situations where one side knows more than the other and the temporary options available to them are restricted.[28]

The legal consequences are significant. A framework which depends on people to read notices and understand processing operations and make informed choices about their data transfer responsibility to the person who lacks the ability to meet those responsibility requirements. Data fiduciaries control the processing operations because they have superior technical expertise and they manage the interface and they choose which data processing purposes to pursue.

Users encounter lengthy notices at times when they want to complete a transaction instead of assessing its data effects. The consent obtained under these conditions meets the formal interface requirement but does not show that the user made a true independent choice. The constitutional value of informational privacy can only be protected through methods which prove that every affirmative click represents actual informed decision-making by users.[29]

The DPDP Act, 2023, recognises this difficulty to an extent. Section 6 requires consent to be free, specific, informed, unconditional and unambiguous, while section 8 establishes general compliance security breach notification and data deletion duties for data fiduciaries. The fiduciary needs to demonstrate that they followed the Act by providing evidence of notification and consent acquisition. These provisions are

[28] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, "Privacy and Human Behavior in the Age of Information" (2015) 347(6221) *Science* 509–514; P.A. Norberg, D.R. Horne and D.A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors" (2007) 41(1) *Journal of Consumer Affairs*100–126.

[29] Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126 *Harvard Law Review* 1880–1903; *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

important because they recognise that responsibility cannot rest entirely upon the data principal. The system still maintains consent as a vital element because the current legal requirements do not provide complete data reduction and privacy protection obligations which this paper suggests.[30]

The authors of this study advocate for an organizational change which replaces consent-based protection with accountability as the standard practice. Organizations using the first method will consider their documented consent as the main reason for their processing activities, which requires people to prove their rights violations after they stop working. The second method requires fiduciaries to show that they need to process data and that their processing methods match their designated goals while complying with responsible design standards, regardless of whether they received customer consent. Organizations need to obtain consent, but they must show their institutional obligations through responsible behavior. The approach supports the constitutional framework which establishes privacy as a fundamental element of human dignity and personal freedom instead of a contractual choice.[31]

The requirement for data minimization should become established as a statutory duty which applies to all situations. Fiduciaries should collect only information reasonably necessary for a specified purpose, retain it only for as long as that purpose requires and periodically review whether continued processing remains justified. The system assists in decreasing both data exposure risks and data misuse occurrences because it prevents organizations from collecting unnecessary information which they would otherwise gather through inexpensive technological methods.

The second requirement mandates that organizations establish privacy protection measures through their design process while maintaining these protections as default security settings. Organizations should establish their services with privacy protection measures which include limited visibility and restricted sharing options. The system

[30] Digital Personal Data Protection Act, 2023, ss 6 and 8.
[31] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

should require additional processing to have both an identifiable purpose and a valid legal foundation instead of permitting access through general default settings.[32]

The third requirement for notices demands that they should adhere to a standardized short-form writing system. The first layer of this system needs to present three data collection categories together with their respective collection purposes and legal bases and main data distribution partners and data withdrawal methods and grievance redressal processes. The detailed layer enables users to access both technical materials and additional content. Service providers would achieve better service comparisons through standardization while users face less cognitive effort because they encounter fewer different presentation styles. The DPDP Rules, 2025 already require notices to be independently understandable and to include itemised data and specified purposes. The standardised model will build upon existing frameworks which should remain intact.[33]

The original contribution of this paper is thus a change in the organising principle of privacy regulation. The law should not ask only whether a user clicked, agreed or continued using a service. The law requires examination of three elements which include information collection purpose, necessity of information collection and presentation of choice, together with the organization path to justifying its actions. The privacy paradox is not solved by demanding more attentive users. Institutions need to create systems which maintain protective functions because users operate their systems in normal daily activities.

VI. FINDINGS, SUGGESTIONS AND CONCLUSION

The first finding which provides an answer to Research Question 1 shows that the privacy paradox fails to show people who display no interest in privacy protection. The element shows how far people go from their declared desire to keep information secret toward their actual digital activities. Users will share their personal data

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts 5(1)(c), 25.
[33] Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025, r 3.

because they face information gaps and find it easy to share data while following social norms and experiencing consent fatigue and lacking choice. People need to assess their privacy decisions by considering both their technological environment and their business context instead of viewing them as separate personal decisions.[34]

The second finding, which answers Research Question 2, demonstrates that Indian constitutional law establishes a fundamental legal basis that protects informational privacy rights. The case of *Justice K.S. Puttaswamy (Retd.) v Union of India* established privacy as a fundamental right which derives from human dignity and personal autonomy and individual liberty. The proportionality framework demands that privacy restrictions must fulfill three conditions which include legal requirements and valid purposes and proportionality requirements with suitable protective measures. The *Karmanya Singh Sareen v Union of India* case study demonstrates that private contracts cannot effectively address the more extensive issues which relate to personal data protection. Digital activities need protection through statutory and institutional safeguards which require constitutional recognition to achieve effectiveness.[35]

The third finding, which addresses Research Question 3, shows that the DPDP Act 2023 establishes a significant new legal framework through its requirement of consent and its fiduciary duties and its personal rights and its system for enforcing rights. The system depends on consent but becomes unstable because users lack the ability to understand processing details and handle their processing agreements. The legitimate-use grounds under section 7 serve necessary purposes but require careful interpretation. The Act establishes security and compliance obligations which fail to create an effective system to stop organizations from accumulating too much information and designing consent processes that mislead users. The DPDP Rules 2025 establish new requirements for notice delivery, but their actual success will depend on how well they are put into action and monitored.[36]

---

[34] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, "Privacy and Human Behavior in the Age of Information" (2015) 347(6221) *Science* 509–514.
[35] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1; *Karmanya Singh Sareen v Union of India*, MANU/DE/2607/2016 (Delhi High Court, 23 September 2016).
[36] Digital Personal Data Protection Act, 2023, ss 5–9; Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025, r 3.

The fourth finding, which answers Research Question 4, shows that better models need to combine personal decision-making with system-based accountability. The processing of data requires consent because the process depends on it, but consent cannot be used to justify practices that are either excessive, or unjust. The three requirements of data minimisation together with privacy by design and protective defaults and intelligible notices and safeguards against dark patterns establish essential elements that companies need to protect users from formal consent which fails to provide them real independence. The findings therefore support the research hypothesis: a predominantly consent-centred framework cannot adequately address the behavioural conditions underlying the privacy paradox without stronger accountability obligations. The conclusion needs to recognize that consent functions as a vital factor which enables people to govern their own decisions.

The initial recommendation requires organizations to strengthen their existing DPDP framework by implementing data minimization requirements and establishing mandatory privacy-by-design and privacy-by-default standards. Fiduciaries should document why each category of personal data is necessary, establish retention limits and periodically review continued processing. Default settings should limit the collection of data through profiling and data sharing. The second suggestion is to introduce a standardised short-form notice model, which will be accompanied by detailed supplementary notices. The notices should use simple language, standard headings and easy-to-understand descriptions of their objectives, data types, recipients, data retention periods, withdrawal procedures and complaint resolution methods. Regulatory guidance should provide model formats and examples that various sectors can use, while allowing them to adjust based on their service requirements.[37]

The DPDP framework needs to specifically define dark patterns which exist within consent and withdrawal interface systems. The law should prohibit interface practices that manipulate the decision to consent, obscure refusal, or make withdrawal

[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts 5(1)(c) and 25; Digital Personal Data Protection Act, 2023, ss 6 and 8.

materially more difficult than acceptance. The prohibition should be technology-neutral and accompanied by practical guidance which helps designers understand which practices are forbidden and which ones they can use. The Data Protection Board of India needs better enforcement collaboration with consumer protection organizations according to requirement number four. The Board's data protection mandate and the Central Consumer Protection Authority's responsibility concerning unfair trade practices are complementary. Information-sharing protocols combined with coordinated investigations and established referral procedures will stop fragmented enforcement which leads to different regulatory bodies assessing the same interface through separate frameworks.[38]

The implementation should maintain its current size. Small businesses should receive model compliance documents, accessible guidance and reasonable transition support. The requirements for intensive examination apply to processing activities which involve higher risks and use large-scale profiling methods and handle vulnerable users. This differentiated approach would preserve the protective purpose of the proposed reforms without imposing unnecessary administrative burdens on low-risk activities. Organizations would develop privacy programs because they want to build responsible services instead of creating documents for legal compliance.

The privacy paradox demonstrates that people willfully disclose information only when they can make informed choices about their online activities. Users must share their personal data because digital systems require information that users cannot control or comprehend. The law needs to establish boundaries which protect personal data security while providing people the ability to make their own data decisions. The system needs to protect user decision making from unauthorized viewing and from collecting unnecessary information and through deceptive user interface techniques. The constitutional right to privacy becomes meaningful only when the institutions processing personal data bear responsibility for protecting it.

[38] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. CCPA-1/1/2023-CCPA (Reg), 30 November 2023; Digital Personal Data Protection Act, 2023, ss 18–26.

The future of Indian data protection requires evaluation through two specific factors which include the number of displayed notices and recorded consents but require organizations to demonstrate their processing activities through their data handling methods which remain protected throughout the entire data lifecycle. Users who want to use ordinary digital services should not have to learn about data protection because this framework will use actual human behavior to design its system. The service provider must assume responsibility for all situations which include users who work quickly their focus is interrupted or they cannot handle the situation. The shift from using consent as a protection shield toward establishing accountability as the standard practice does not take away from individual rights. It is the institutional condition necessary to make that autonomy real.

VII. REFERENCES

A. Books, Journal Articles and Other Academic Literature

1. Acquisti, Alessandro, Laura Brandimarte and George Loewenstein, "Privacy and Human Behavior in the Age of Information" (2015) 347(6221) *Science* 509–514.

2. Bashir, Masooda, Carol Hayes, April D. Lambert and Jay P. Kesan, "Online Privacy and Informed Consent: The Dilemma of Information Asymmetry" (2016) 52(1) *Proceedings of the Association for Information Science and Technology* 1–10.

3. Norberg, P.A., D.R. Horne and D.A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors" (2007) 41(1) *Journal of Consumer Affairs* 100–126.

4. Solove, Daniel J., "Privacy Self-Management and the Consent Dilemma" (2013) 126 *Harvard Law Review* 1880–1903.

B. Reports and Committee Materials

1. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering*

Indians (Ministry of Electronics and Information Technology, Government of India, 2018).

C. Legislation And Rules

1. Indian Legislation

- The Constitution of India, 1950.
- The Information Technology Act, 2000.
- The Consumer Protection Act, 2019.
- The Digital Personal Data Protection Act, 2023.

2. Indian Rules and Regulations

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Ministry of Electronics and Information Technology, Government of India, 13 November 2025.
- Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. CCPA-1/1/2023-CCPA (Reg), 30 November 2023.
- Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), 13 November 2025, Gazette of India, Extraordinary, Part II, Section 3(i).

D. Judicial Decisions

1. Supreme Court of India

- *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
- *Modern Dental College and Research Centre v State of Madhya Pradesh* (2016) 7 SCC 353.
- *Meta Platforms, Inc. v Competition Commission of India*, Civil Appeal Nos. 301–302 of 2026 and connected matters, order dated 23 February 2026.

2. High Courts

- *Karmanya Singh Sareen v Union of India*, MANU/DE/2607/2016 (Delhi High Court, 23 September 2016).

3. Competition Appellate Decisions

- *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users*, Suo Motu Case No. 01 of 2021, along with Case Nos. 05 and 30 of 2021, Competition Commission of India, order dated 18 November 2024.
- *WhatsApp LLC v Competition Commission of India*, Competition Appeal Nos. 1 and 2 of 2025, National Company Law Appellate Tribunal, judgment dated 4 November 2025.
- *WhatsApp LLC v Competition Commission of India*, I.A. No. 6817 of 2025 in Competition Appeal (AT) No. 1 of 2025, National Company Law Appellate Tribunal, order dated 15 December 2025.

E. International Instruments

1. 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).