Page: 304-323 *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 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.14

CRITIQUING THE 'NOTICE AND CONSENT' FRAMEWORK WITHIN INDIA'S DPDP ACT, 2023 AND CONSUMER PROTECTION REGIMES

Nitin Shukla[1]

I. ABSTRACT

The introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark in the digital jurisprudence in India that transformed the country into a unified statutory framework, moving away from a disjointed regulatory framework of Information Technology Act, 2000, to a centralized one, based on the Notice and Consent approach. This research paper critically, in detail, and exhaustively critiques this framework, enshrined in the DPDP Act, Sections 5 and 6, by contrasting it with the parallel remedial framework of the Consumer Protection Act, 2019, in Section 7, the so-called Legitimate Uses exception. This paper is based on the thesis that the standard of a valid consent stated in the DPDP Act including the necessity of a free, specific, informed, unconditional, and unambiguous consent is quite high, but the realities of consent fatigue and limited rationality combined with the broadly defined statutory exemption would tend to diminish those requirements to a mere legal fiction. Moreover, the paper also points to a very important jurisprudential difference, namely, the centralization of the enforcement in Data Protection Board of India (DPBI) with penalties accruing to the State, but the absence of direct compensation to Data Principals in the form of harm definition is also identified. The legislative option unwittingly increases the CPA as the main source of individual remedial compensation on harms of privacy, namely under the category of "Unfair Trade Practices" and "Unfair Contracts." By comparing and contrasting with the GDPR and the PDPA of Singapore, and looking at the new Indian case law such as the Ashwani Chawla v. Flipkart Internet Pvt. Ltd. This study explains the confusing dual-compliance environment in which mobile numbers of collection cases are now being determined as cases of consumer protection following recent rulings on this topic by Chandigarh Commission. This paper concludes that the convergence of these two regimes forms a requisite yet discordant system of checks and balances, in which the failures of the DPDP Act consent

[1] PhD Research Scholar, Faculty of Law University of Lucknow, Lucknow (India). Email: ps9288213@gmail.com

model should be compensated by the application of the consumer law principles of dark patterns and fiduciary responsibility in good faith.

II. KEYWORDS

Digital Personal Data Protection Act 2023, Notice and Consent, Consumer Protection Act 2019, Unfair Trade Practices, Data Fiduciary, Legitimate Uses, Dark Patterns, Privacy Jurisprudence, Consent Fatigue, Data Sovereignty.

III. INTRODUCTION

The digital economy is based on the sale of personal data to the services, which traditionally has been regulated by the model of Notice and Consent. This model assumes that in case a person is given adequate information (Notice) and positively consents to the processing of their data (Consent), their autonomy is not violated, and the following processing of the data is justified[2]. Constitutional sanctioning of this autonomy in India came in the historic case of *Justice K.S. Puttaswamy (Retd.). v. Union of India,* in which the Supreme Court in a bench of nine judges unanimously concluded the right to privacy, as a fundamental right, inherent to life and individual liberty under Article 21 of the Constitution.[3] Clearly the Court associated privacy to both the principle of dignity and informational self-determination, requiring state to implement a well-designed regime of data protection, which would reconcile individual rights and justifiable state interests[4].

After this judicial order and multiple versions of the project legislation, such as the Personal Data Protection Bill, 2019, the Parliament adopted the Digital Personal Data Protection Act, 2023 (DPDP Act). [5]. The Act purportedly puts the Data Principal (the person) at the heart of the data economy, giving them rights to access, correction, and

[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[3] The Consumer Protection Act, No. 35 of 2019 (India).
[4] "Rebooting consent in the digital age: a governance framework for health data exchange," PubMed (article record) (last visited Feb. 4, 2026), https://pubmed.ncbi.nlm.nih.gov/34301754/ (last visited Feb. 4, 2026).
[5] Digital Personal Data Protection Act, No. 22 of 2023 (India) (enacted 2023)

erasure and liabilities to Data Fiduciaries (entities deciding on the purpose and the means of processing). [6]

Nevertheless, the effectiveness of the "Notice and Consent" model has been challenged by the global discussion of the privacy law. According to the scholars, the model is afflicted with the so-called privacy paradox, where users, despite their desire to have privacy, engage in a habit of giving it away due to the lack of information, cognitive bias, and the so-called consent fatigue that occurs when presented with too many privacy notices. In reaction, the DPDP Act proposes such mechanisms as "Just-in-Time" notices and "Consent Managers" in order to simplify the process. [7]. However, at the same time, the Act adds Section 7, which allows processing to be done without consent under the category of "Certain Legitimate Uses", and this begs the question of the undermining of the very privacy the Act is meant to defend.[8]

This is complicated by the Consumer Protection Act, 2019 (CPA). The CPA, as opposed to the DPDP Act, which aims at regulatory compliance and penalties imposed by the state, offers an individual redressal mechanism. Since the CPA has now incorporated the unauthorized release of personal information into the definition of the term Unfair Trade Practices (2019 amendment), it has become a parallel and possibly more readily available forum through which privacy lawsuits can be brought.

Subsequent to the drafting of this manuscript, the Government of India notified the Digital Personal Data Protection Rules, 2025, on 13–14 November 2025, thereby operationalizing the Digital Personal Data Protection Act, 2023 through a phased implementation framework. The Rules envisage a three-stage rollout: Phase I (November 2025) concerning the establishment and operationalization of the Data Protection Board of India; Phase II (November 2026) governing the registration and

[6] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Ministry of Electronics & Information Technology (MeitY) (pdf) (upload date on file: June 2024) (on file with MeitY)
[7] Digital Personal Data Protection Act § 5 (India) (interpreted discussion), DPDPA Section 5 with interpretation, DPDPA.com, available at https://dpdpa.com/dpdpa2023/chapter-2/section5.html (last visited Feb. 4, 2026)
[8] Digital Personal Data Protection Act § 6 (India) (interpretation), DPDPA.com, https://dpdpa.com/dpdpa2023/chapter-2/section6.html

functioning of Consent Managers; and Phase III (May 2027) bringing into force substantive compliance obligations for Data Fiduciaries.

This development materially contextualizes the present critique. While the Act has now entered its implementation trajectory, the structural concerns identified in this paper particularly regarding consent architecture, legitimate uses, and the remedial deficit remain salient in assessing how the statutory design will function in practice within the evolving regulatory ecosystem.[9]

A. Research Questions

1. Does the Notice and Consent architecture of the DPDP Act, 2023, succeed in enabling Data Principals to have informational self-determination or is this autonomy made illusory by the cognitive constraints of users and the design of digital consent artefacts?
2. What is the extent to which the "Legitimate Uses" (Section 7) of the DPDP Act, especially in terms of the aspect of voluntary data provision, provides a statutory loophole that avoids the requirement of the Unambiguous Consent (under the GDPR)?
3. Does the jurisprudence of Deficiency in Service and Unfair Trade Practice under the Consumer Protection Act, 2019, effectively address the remedial gap in individuals who suffered non-financial privacy injuries in the absence of such provisions being made in the DPDP Act, 2023?

B. Hypothesis

Procedurally sound but substantively weakened by the behavioral fact of consent fatigue and the wide-ranging Legitimate Uses exemptions, the Notice and Consent framework of the DPDP Act, 2023, is a threat to the reduction of user autonomy to a legal fiction. As a result, the Consumer Protection Act, 2019, has become the de facto civil redress to privacy breaches, in which the court should apply the "Unfair Trade

[9] Digital Personal Data Protection Act § 8 (India): Data fiduciary obligations (interpretation), DPDPA.com, https://dpdpa.com/dpdpa2023/chapter-2/section8.html (last visited Feb. 4, 2026)

Practice" provisions to regulate the Dark Patterns and impose the fiduciary duty of care that the regulatory focus of the data protection statute virtually overlooks.

C. Research Objectives

1. To critically assess the effectiveness of the "Notice and Consent" framework that is entrenched in the DPDP Act, 2023, in particular, to examine the adequacy of statutory protection mechanisms such as the so-called Just-in-Time notices to defeat the behavioral effects of the so-called bounded rationality and consent fatigue.
2. To investigate the legal aspects of the "Legitimate Uses" exception (Section 7) and the lack of the definition of the harm in the DPDP Act, it is necessary to find out whether these provisions undermine the fiduciary duty of care and the independence of the Data Principal in comparison with such international regulations as the GDPR and the PDPA in Singapore.
3. To examine the new role of the Consumer Protection Act, 2019, as a parallel remedial action, in particular, to explore the interpretation of the term "Unfair Trade Practices" (Section 2(47)) and the term "Unfair Contracts" (Section 2(46)).

D. Research Methodology

The study uses a doctrinal and comparative research legal methodology to offer a comprehensive examination of the legislation framework.

1. **Statutory Interpretation:** The fundamental analysis is based on a textual interpretation (granular) of the Digital Personal Data Protection Act, 2023, namely the Sections 2 (Definitions), 5 (Notice), 6 (Consent), 7 (Legitimate Uses), and 38 (Relationship with other laws). This is supplemented by the analysis of the Consumer Protection Act, 2019, in relation to Section 2(47) (Unfair Trade Practices) and Section 2(46) (Unfair Contracts).
2. **Comparative Jurisprudence:** The paper compares the Indian DPDP Act to the GDPR of the EU and the PDPA of Singapore to draw out normative

differences. Particularly, it contrasts between a legitimate use (India) and a degraded consent (Singapore) and legitimate interests (EU).

3. **Case Law Analysis:** The study loos into Supreme Court of India case law (e.g. Puttaswamy) and National Consumer Disputes Redressal Commission (NCDRC) (e.g. Ashwani Chawla, Chandigarh Commission Orders).
4. **Interdisciplinary Synthesis:** The legal study is enriched by the ideas of behavioral economics, namely, the notions of the limited rationality and the dark patterns.

E. Literature Review

The scholarly and legal debate on the topic of data protection in India has been shifting towards an emphasis on the lack of legislation to an objection to the particular mechanisms embraced in the DPDP Act. This review divides the literature available into three main areas namely: the critique of the consent model, the fiduciary accountability model, and the area of convergence between consumer and data protection laws.

1. **Crisis of Notice and Consent:** The paradigm of the Notice and Consent has been the prevailing paradigm in the law of privacy around the world. But failure in it has been widely reported by legal experts. The theory of consent fatigue claims that the number of consent requests itself makes the process worthless and turns informed consent into a machine of clicking I Agree. According to the studies conducted by Degeling et al. and others, the users experience the problem of the limited rationality and cannot estimate the risks of sharing such data in the long run, which results in the so-called privacy paradox. The application of this model to the DPDP Act in the Indian situation has been criticized as a means of enhancing these problems. Although Section 5 presents the concept of Just-in-Time notices to lessen the workload of

cognition, opponents claim that the power imbalance still exists unless there are substantive measures against the content of these notices. [10]

2. **The Fiduciary Accountability Model:** Indian law Indian law, especially inspired by the Srikrishna Committee Report and the writings of Rahul Matthan have proposed that the burden should be shouldered not on an individual but on the entity handling the data. [11]. This "Accountability Model" assumes that data controllers are to be treated as Data Fiduciaries with a duty of loyalty and care to the Data Principal that creates a doctor-patient relationship. [12]Nevertheless, the latest legal interpretation states that the ultimate version of the Act watered down this idea, deleting the definition of the notion of "Harm" that existed in the 2019 Bill.[13]

3. **The Intersection of Consumer Law:** An emerging literature on the intersection of consumer protection and data privacy. The fact that the personal data protection is incorporated into the definition of the Unfair Trade Practices in the CPA, 2019, is regarded as a very important development. [14]. Researchers observe that even though the DPDP Act establishes a specialized regulatory authority, the emphasis on state penalties creates a remedial vacuum to people who want to receive compensation. [15]

---

[10] "The Right to (Pry)-vacy: Understanding India's Dystopian Data Protection Legislation," N.Y.U. Journal of Intellectual Property & Entertainment Law (online) (last visited Feb. 4, 2026), https://nyujilp.org/the-right-to-pry-vacy-understanding-indias-dystopian-data-protection-legislation/ (last visited Feb. 4, 2026).

[11] "Consent Fatigue and Data Protection Laws: Is 'Informed Consent' a Legal Fiction," Lawvs (blog post) (last visited Feb. 4, 2026), https://lawvs.com/articles/consent-fatigue-and-data-protection-laws-is-informed-consent-a-legal-fiction (last visited Feb. 4, 2026).

[12] "Puttaswamy v. Union of India (I)," Columbia Global Freedom of Expression (case summary) (last visited Feb. 4, 2026), https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/ (last visited Feb. 4, 2026).

[13] "Challenges and recommendations for enhancing digital data protection in Indian Medical Research and Healthcare Sector," PMC (PubMed Central), https://pmc.ncbi.nlm.nih.gov/articles/PMC11754748/ (last visited Feb. 4, 2026).

[14] "Fiduciary Duties in the Digital Age: A Critical Examination of the Digital Personal Data Protection Act 2023," Indian Journal of Integrated Research in Law (IJIRL) (Volume V Issue III) (pdf) (June 2025), https://ijirl.com/wp-content/uploads/2025/06/FIDUCIARY-DUTIES-IN-THE-DIGITAL-AGE-A-CRITICAL-EXAMINATION-OF-THE-DIGITAL-PERSONAL-DATA-PROTECTION-ACT-2023.pdf (last visited Feb. 4, 2026).

[15] "An Analysis of Differences and Advancements Made by the Data Protection Bill 2023 Compared to Previous Relevant Data Protection Laws," IJIRL (Aug. 2024) (pdf), https://ijirl.com/wp-content/uploads/2024/08/AN-ANALYSIS-OF-DIFFERENCES-AND-ADVANCEMENTS-MADE-

IV. THE STATUTORY ARCHITECTURE OF CONSENT: A BEHAVIOURAL AND DOCTRINAL CRITIQUE

The Digital Personal Data Protection Act, 2023, is seemingly designed along the principles of the consent of the Data Principal as the major lawful foundation of processing personal data. The statutory foundation of the Act is set under the section 6(1) that requires the consent to be free, specific, informed, unconditional, and unambiguous with an explicit affirmative action. Although this language is a reflection of the strict requirements of the GDPR of the European Union (Article 4(11)), a more thorough analysis shows that it contains quite a few structural and behavioural weaknesses once introduced to the Indian digital ecosystem.

A. The Illusion of "Free and Informed" Consent in the Age of Bounded Rationality

The statutory textual condition of consent being informed (Section 6(1)) is enforced by Section 5 which provides that all requests of consent must be underpinned by a notice[16]. The Act is a pioneering Act as it brings in the introduction of the Just-in-time (JIT) notices through the proviso to Section 5 of the Act whereby a summary notice can have a link to the text. Although evidence-based design indicates that JIT notices are less cognitive load, this process cannot explain the phenomenon of Bounded Rationality. According to behavioral economics, users have scarce cognitive resources and time that they utilize in Rational Ignorance, that is, they rationally decide to disregard privacy warnings, since the cost of reading privacy warnings (time) exceeds the perceived immediate payoff (access to the app).

The "Notice" is thus turned into a legal fiction. It is not a user empowerment tool but rather an indemnity clause to the Data Fiduciary. When the user clicks on the I Agree button, he makes a procedural consent that meets the statute but does not have

BY-THE-DATA-PROTECTION-BILL-2023-COMPARE-TO-PREVIOUS-RELEVANT-DATA-PROTECTION-LAWS.pdf (last visited Feb. 4, 2026).

[16] Mark Taylor & Jeannie Paterson, Protecting Privacy in India: The Role of Consent and Fairness in Data Protection, The University of Melbourne (pdf) (last visited Feb. 4, 2026), https://www.unimelb.edu.au/__data/assets/pdf_file/0007/3824485/Taylor,-Mark,-and-Paterson,-Jeannie,-Protecting-Privacy-in-India-The-Role-of-Consent-and-Fairness-in-Data-Protection.pdf (last visited Feb. 4, 2026).

substantive understanding. This is what causes Consent Fatigue, users have become so inundated with constant consent requests that they have learned to reflexively click Accept without reading. The power imbalance of the digital market is disregarded in the DPDP Act because it is based on this model. In contrast to a contract between equals, the terms are dictated by the data fiduciary and the only freedom that the user has is the binary option of either using the digital service or not.

B. The "Unconditional" Mandate and the Bundling Problem

Another important addition to the Indian statute is that the consent must be unconditional.[17] This provision has a clear prohibition against the conditionality of the provision of a service based on the consent to the processing of personal data not necessary to the service. It is a direct legislative reaction to the bundling practice where an application (e.g. a flashlight application) requires access to unrelated information (e.g. contact books) in order to use it. The effectiveness of this provision however depends on how necessary is interpreted. As a platform economy where network effects prevail, Data Fiduciaries frequently claim that a large amount of data is required to serve the purpose of service improvement, personalization, or fraud detection.

In case the Data Protection Board of India (DPBI) takes a liberal approach to the meaning of necessity, the unconditional protection will be rendered ineffective. An example of this would be a social media site claiming that they needed to access the entire address book of a user in order to connect them to friends and thus avoid the conditional consent ban. This represents a regulatory game of tug-of-war in which the onus of establishing non-necessity can be practically passed on to the under-resourced Data Principal.

C. Consent Managers: Centralization of Control or Failure?

Section 6(7) proposes the introduction of "Consent Managers"- parties registered by the Board to provide a single point of contact through which Data Principals can

[17] "Moving Slow and Fixing Things," eCollections, Florida Int'l Univ. College of Law (faculty publications) (last visited Feb. 4, 2026), https://ecollections.law.fiu.edu/cgi/viewcontent.cgi?article=1519&context=faculty_publications (last visited Feb. 4, 2026).

provide, manage, revise, and withdraw consent. This is in line with Data Empowerment and Protection Architecture (DEPA). The promise set out in theory is that a Consent Manager can represent the user and negotiate improved privacy conditions and address the issue of consent fatigue through centralizing permissions.

Nonetheless, there are still some serious risks. Unless Consent Managers are made rigidly independent of Data Fiduciaries, they can be used as a tool to manufacture bulk consent. Moreover, the Act is silent on the liability of Consent Managers in case they do not revoke the consent upon the request of a user. In the absence of a strong fiduciary obligation clearly hooked to the Consent Manager position in the statute, they will merely remain another bureaucratic addition to the statute as opposed to an actual privacy enhancing technology (PET).

V. SECTION 7 AND THE 'LEGITIMATE USES' DOCTRINE: DILUTION OF THE CONSENT NORM

Where in Section 6, the high wall is built in order to create Express Consent, in Section 7 of the DPDP Act, another important counter-narrative is presented in the form of Certain Legitimate Uses. This section allows the processing of personal data without consent under certain conditions, in contrast to the terminology of the 2022 draft, which refers to the so-called Deemed Consent, but retains its substantive meaning. [18]

A. Section 7(a): The "Voluntary" Loophole and the Singaporean Parallel

Under section 7(a), processing may occur when the Data Principal has voluntarily provided personal data for a specified purpose and has not indicated refusal. This formulation closely resembles the "deemed consent by conduct" framework under the Personal Data Protection Act 2012 (No 26 of 2012) (Singapore), s 15(1), which permits reliance on consent where an individual voluntarily provides personal data and it is reasonable to infer consent from conduct in the given circumstances. Nevertheless, the Indian version does not have the contextual guardrails that the

[18] "Promises and Illusions of Data Protection in Indian Law," Indian Data Protection Law (IDPL) / Oxford Academic (journal article) (last visited Feb. 4, 2026), https://academic.oup.com/idpl/article/1/1/47/759660 (last visited Feb. 4, 2026).

Singaporean version has, whereby it is reasonable to expect that the person would have given the data.

Section 7(a) uses the word voluntarily, which is dangerous as far as manipulative User Interface (UI) design is concerned. In case a user is provoked by a Dark Pattern (e.g., a blinking button or a misleading prompt) to import their address book to meet friends, they have still given out the data on their own free will. A Data Fiduciary might defend this act by pointing to Section 7(a) and thus beating the strenuous informed and unambiguous conditions of Section 6. [19] This poses a risky slide: there must be a high standard of express consent, but a lesser one of implied consent through action. It encourages Data Fiduciaries to design interactions with users that elicit the application of Section 7(a) as opposed to pursuing the consent of Section 6, effectively reinstating the opt-out approach that the Act is supposed to disapprove.

B. Legitimate Use vs.Legitimate Interest: Comparative Deficit

In contrast to the GDPR, legitimate interest (Article 6(1)(f)) that mandates the controller to record a Legitimate Interest Assessment (LIA) weighing the interest of the controller against the rights of the data subject, the Indian legitimate uses provision does not have a statutory balancing test. The list in Section 7 is comprehensive yet general especially in State functions. Section 7(b) allows processing to make any subsidy, benefit, service, certificate, license, or permit by the State. This forms a logic of blanketing exemption. In Puttaswamy the Supreme Court required that invasion of privacy have to be thirdly tested as legal, necessary, and proportionate.

Section 7(b) also has an implicit assumption of proportionality of all the State administrative functions and, as such, eliminates the necessity of the State to prove necessity on a case-by-case basis. This brings the State to the level of a Super-Fiduciary, the actions of which in the processing of data are assumed to be legitimate, which essentially undermines the provision of the Constitution of the check on the surveillance of the state and the compilation of data.

[19] "Data protection law: Implications of a fiduciary responsibility," Law.asia (Asia Law), (last visited Feb. 4, 2026), https://law.asia/fiduciary-responsibility-implications/ (last visited Feb. 4, 2026).

C. Employment Purposes and Employee Privacy

Section 7(i) permits processing under the reason of employment. Although practically required, it is unfavorable that the definition of what is considered to be a legitimate employment reason is non-existent and leaves the employees exposed to intrusive surveillance (e.g. bossware or keystroke logging) in the name of protecting the employer against loss. In contrast to the GDPR, which restricts the monitoring of employees with the help of the legitimate interest and needle necessity tests, Section 7(i) offers a wide veil to the employers, which may undermine the privacy rights of the workforce without their direct approval.

VI. FIDUCIARY DEFICIT: STRUCTURAL ACCOUNTABILITY AND THE ELIMINATION OF 'HARM'

The DPDP Act presents the nomenclature of Data Fiduciary (Section 2(i)) to designate the term as separate from the Data Controller that is employed in the GDPR. This linguistic decision suggests trust, loyalty and greater care of the entity to the individual. [20]. A structural analysis however indicates that this is a Fiduciary in name only but not in reality, mainly because of the elimination of the idea of by the concept of Harm and because of the lack of compensatory remedies.

A. The Harm Removal: A 2019 Bill Regression

The Personal Data Protection Bill, 2019, had an extensive definition of what constitutes the harm (Clause 3(20)) which consisted of financial loss, loss of reputation, identity theft, discriminatory treatment, and unreasonable surveillance. The 2023 Act entirely eliminated this definition. This exclusion is a disaster to the creation of a privacy tort jurisprudence in India. Under the common law tort of negligence, liability is based on the proving of: (1) Duty of Care, (2) Breach of Duty, (3) Causation, and (4) Damage/Harm.

The DPDP Act effectively renders it painfully hard to prove Damage in a civil court by a Data Principal by depriving them of the statutory acknowledgement of non-

[20] "DPDP Act vs EU GDPR Compliance – A Comparative Analysis," Taxmann (online commentary) (last visited Feb. 4, 2026), https://www.taxmann.com/post/blog/dpdp-act-vs-eu-gdpr-compliance (last visited Feb. 4, 2026).

financial harms (such as reputational injury or observation). There is no statutory peg of privacy harm as a result of which victims of data breaches who do not incur any direct financial loss but merely suffer mental agony or loss of privacy may have no redress under tort law.

B. The Penalty Paradigm: State Restitution more than Individual Restitution

The DPDP Act enforcement mechanism is only regulatory. Under Section 33 read with the Schedule of the Digital Personal Data Protection Act, 2023, the Data Protection Board of India may impose monetary penalties of varying tiers depending on the nature of the contravention, with the most serious violations attracting penalties of up to ₹250 crore.[21] However, such penalties are payable to the State and do not accrue to the affected Data Principal. This structural design separates regulatory punishment from individual restitution. An attempt by a Data Fiduciary to leak the medical records of a user would result in a huge fine to the State but the user would not get a single penny as a result of the act under the DPDP Act.

This is in stark contrast to Article 82 of the GDPR that states clearly that the data subjects have the right to compensation in case of material or non-material damage[22]. Indian model reverses the emphasis of the Restorative Justice (to render the victim complete) to Retributive/Deterrent Justice (to punish the offender). This makes the Data Fiduciary answerable to the Board (the State) and not to the principal (the Individual) and emptying the fiduciary duty of loyalty.

C. The "Standard of Care" and Section 8

Section 8(5) gives Data Fiduciaries a responsibility to carry out reasonable security protection. [23] Although this establishes a statutory standard of care, the absence of a right of action in the DPDP Act on the issue of breach of this duty implies that a breach

[21] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 33, Schedule (India).
[22] "Interplay between the DPDP Act, 2023 and Consumer Protection/E-Commerce Laws," KS&K (blog/analysis) (last visited Feb. 4, 2026), https://ksandk.com/data-protection-and-data-privacy/dpdp-act-consumer-protection-navigating-dual-compliance/ (last visited Feb. 4, 2026).
[23] "Navigating the Intersection of Data Protection and Consumer Protection Laws in India," Sai Krishna Associates (firm note) (last visited Feb. 4, 2026), https://www.saikrishnaassociates.com/navigating-the-intersection-of-data-protection-and-consumer-protection-laws-in-india/ (last visited Feb. 4, 2026).

of this duty does not necessarily result in compensating the victim. The Data Principal is left to make the best of the ad hoc remedies of consumer courts (discussed infra), which results in a Data Principal with the power of a trustee but not the responsibility of one to the beneficiary. [24]

VII. CONSUMER PROTECTION ACT, 2019: THE PARALLEL PRIVACY JURISPRUDENCE

The Consumer Protection Act, 2019 (CPA) has become the default civil action in privacy violations in the vacuum left by the DPDP Act on individual compensation. In this part, the authors examine the ways in which Consumer Commissions are redefining Unfair Trade Practices to regulate the digital economy and in effect establishing a parallel privacy jurisprudence.

A. Article 2(47)(ix): Codification of Data Privacy as a Consumer Right

Section 2(47) of the CPA has the meaning of the Unfair Trade Practice. In particular, Section 2(47)(ix) states that the revelation of any personal information provided in confidence by the consumer to any other person without making such disclosure in consonance with the terms of any law is an unfair trade practice. This is a transformational provision. It enables Consumer Commissions to not only address a data breach or unauthorized data sharing as a regulatory breach, but as a consumer tort. In *Nivedita Sharma v. Bharti Tele Ventures*, the Consumer Commission imposed penalties on service providers who illegally disclose personal data and compensates the victim of the harassment. [25] This confirms that any claim of privacy breach is a recoverable deficiency in service, and the victim may seek compensation of the agony

[24] "Intersection of Data Privacy and Consumer Protection Law in India," IJLMH (International Journal of Law Management & Humanities) (article) (last visited Feb. 4, 2026), https://ijlmh.com/paper/intersection-of-data-privacy-and-consumer-protection-law-in-india/ (last visited Feb. 4, 2026).

[25] "Case Comment: Ashwani Chawla v. Flipkart Internet Private Ltd — Formal Recognition of Dark Matter Prevention and Recognition Guidelines," ResearchGate (last visited Feb. 4, 2026), https://www.researchgate.net/publication/399726888_Case_Comment_Ashwani_Chawla_v_Flipkart_Internet_Private_Ltd_-_Formal_Recognition_of_Dark_Matter_Prevention_and_Recognition_Guidelines (last visited Feb. 4, 2026).

of mind under Section 14(1)(d) of the CPA (currently, Section 39 of CPA 2019), which is uncharitably unavailable to victims of the DPDP Act.

B. The Dark Patterns of Jurisprudence: Ashwani Chawla and More

Dark Patterns regulation is one of the most apparent areas of intersection of the two regimes. Guidelines for Prevention and Regulation of Dark Patterns, 2023, published by the CCPA, categorically includes in the list of unfair trade practices deceptive UI/UX designs.

The decision in *Ashwani Chawla v. Flipkart Internet Pvt. Ltd.*, CC/113/2023 (State Consumer Disputes Redressal Commission, U.T. Chandigarh, decided Feb. 20, 2024), primarily concerned the sale of a refurbished mobile phone as a new product and the issuance of dual invoices for handling charges. The Commission invoked the Guidelines for Prevention and Regulation of Dark Patterns, 2023, particularly Section 2(1)(e), to hold that issuing two separate invoices in a single transaction constituted a deceptive design practice amounting to an unfair trade practice. While the case did not centrally address consent mechanisms or personal data processing, its reasoning demonstrates the willingness of Consumer Commissions to scrutinize manipulative interface and transactional designs. By extension, similar reasoning may be applied where deceptive digital architectures affect consumer autonomy in privacy and consent contexts.

Moreover, in 2024 and 2025 (e.g. *Pankaj Chandgothia v. The Coffee Bean & Tea Leaf*; *Mahi Sindhu v. National Watch House*), Chandigarh Commission gave recent orders. The Commission was of the opinion that the requirement to provide a mobile number as a mandatory condition to billing is a breach of the consumer rights and is a form of unfair trade practice. These decisions legitimately impose the Unconditional Consent of DPDP Section 6(1) by remedies provided by the CPA, in which compensation is awarded to the consumers due to invasion of privacy.

C. Unfair Contracts (2(46)) and "Click-Wrap" Agreements

Section 2(46) of the CPA provides a new concept of "Unfair Contracts" giving powers to State and National Commissions to annul the terms of the contract, which are not

reasonable or harmful to the rights of consumers. The implication of this is enormous on the privacy policies of "Click-Wrap".

In the case of Pioneer *Urban Land and Infrastructure Ltd. v. Govindan Raghavan*, (2019) the Supreme Court considered that one-sided terms of a standard form contract where there is no bargaining power on the part of the consumer are an unfair trade practice. Using this in digital scenario, a Privacy Policy which coerces a user to give up legal redress or agree to excessive data collection (bundling) may be found to be an Unfair Contract. This will enable the CPA to invalidate the same terms of service upon which Data Fiduciaries have been reciting to be within the confines of the DPDP Act.

D. Section 38 and the "Dual Compliance" Conflict

Section 38 of the DPDP Act provides that its provisions are words which are additional to and not derogative of other laws.[26] Section 38 (2) however, has non obstante provision that makes the DPDP Act have precedence in case of conflict. This establishes a possibility of conflict. A Data Fiduciary may claim that its data collection policies are in line with the DPDP Act (e.g. in terms of "Legitimate Use" or a "Consent Manager" model) and thus cannot be criticized as the CPA "Unfair Trade Practice" practice. Nevertheless, the decision of the Supreme Court in *Imperia Structures Ltd. v. Anil Patni* (2020), according to which the CPA remedies are complementary to special laws such as RERA, indicates that the judicial branch will probably not allow the courts to ignore the concurrent jurisdiction of Consumer Courts. The unfairness and harm to the consumer is ruled by the Consumer Court and regulatory non-compliance is ruled by the DPBI. Therefore, companies are charged with a Dual Compliance burden: they need to meet the technical requirements of the DPDP Act in order to escape punishment and the fairness requirements of the CPA in order to escape class-action lawsuits. [27]

[26] "Explore CyberPeace Blogs on Cybersecurity," CyberPeace (resource/blog listing) (last visited Feb. 4, 2026), https://cyberpeace.org/resources/blogs?99fd07b9_page=7 (last visited Feb. 4, 2026).
[27] "Intro 3 | Privacy | Mobile App," Scribd (document) (last visited Feb. 4, 2026), https://www.scribd.com/document/940908481/Intro-3 (last visited Feb. 4, 2026).

VIII. FINDINGS AND SUGGESTIONS

A. Findings

1. **Legal Fiction of Consent:** The "consent fatigue" and "bounded rationality" are structurally disabling of the Legal Fiction of Consent (Section 6): the Notice and Consent model. The Just-in-Time mechanism of notice although an improvement does not solve the underlying power imbalance. The autonomy assumed by the law cannot be practiced by the average user.
2. **Section 7 as a Trojan horse:** The legitimate uses clause, especially section 7(a) of the so-called voluntary provision, opens a loophole that will lead to justification of the data processing through so-called deem consent, avoiding the high standard of Section 6. This is further undermined by the fact that there is no balancing test to State functions in Section 7(b), which makes the proportionality requirement a condition of Puttaswamy.
3. **The Remedial Gap and CPA Primacy:** The elimination of the compensation provisions and the definition of the term "Harm" in the DPDP Act leaves a massive remedial gap. As a result, the Consumer Protection Act, 2019 has become the new civil remedy of privacy harms, and Consumer Commissions hear privacy harms and adjudicate on them as Unfair Trade Practices.
4. **Fiduciary Deficit:** The Data Fiduciary name in the DPDP Act does not have the parallel common law obligations of care and fidelity, namely, the liability of non-financial harm. The Act gives more priority to regulatory compliance and state revenue (penalties) as opposed to individual right and restitution.
5. **Dual Compliance Complexity:** Section 38 introduces a dual-compliance environment in which companies will be forced to operate in a mixed environment. The regulatory conflict between the DPBI and the CCPA on the issue of Dark Patterns presents a major challenge to the legal certainty.

B. Suggestions

1. **Reintroduction of "Harm" in Rules:** The Central Government ought to use its rule making authority to reintroduce a definition of what constitutes "Harm" or "Detriment" to provide the Data Protection Board with guidance in the determination of penalties. Although fines are sent to the State, the amount must be directly proportional to the extent of damage caused on the Data Principal.
2. **Unified Recommendations on Dark Patterns:** The Central Consumer Protection Authority (CCPA) and the Data Protection Board of India (DPBI) should adopt common guidelines on UI/UX design to eliminate regulatory arbitrage. A design that meets the conditions of the DPDP consent ought not to be considered a Dark Pattern in CPA and vice versa.
3. **Compensatory Mechanism through DPBI:** The DPBI should seek an amendment of the DPDP Act in the future, to allow it to order part of the fines to be repaid as compensation to the affected Data Principles, as is the case with victim compensation schemes in criminal law.
4. **Narrow Judicial Interpretation of Section 7(a):** The Judiciary should read voluntarily in Section 7(a) literally to avoid data that was acquired with manipulative designs or that the user lacked the reasonable anticipation of processing, and thus the supremacy of express consent stands.
5. **Privacy Rating System:** To address the issue of limited rationality, the DPBI must require "Privacy Scores" or a style of disclosure that resembles nutrition labels that Data Fiduciaries must display, will enable consumers to make informed quick comparisons without reading long notices.

IX. BIBLIOGRAPHY

1. Central Consumer Protection Authority (Prevention and Regulation of Dark Patterns) Guidelines, 2023, F. No. CCPA-1/1/2023-CCPA (Nov. 30, 2023) (India).
2. Consumer Protection Act, 2019, No. 35 of 2019, Acts of Parliament, 2019 (India).

3. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
4. General Data Protection Regulation, Regulation (EU) 2016/679 (2016).
5. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).
6. Personal Data Protection Act 2012, No. 26 of 2012 (Singapore).
7. Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India).
8. Ashwani Chawla v. Flipkart Internet Pvt. Ltd., Consumer Complaint No. 113 of 2023 (State Consumer Disputes Redressal Commission, U.T. Chandigarh, Feb. 20, 2024).
9. HDFC Bank Ltd. v. Jesna Jose, Revision Petition No. 3366 of 2017 (National Consumer Disputes Redressal Commission, 2020).
10. Imperia Structures Ltd. v. Anil Patni, (2020) 10 SCC 783 (India).
11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
12. Karmanya Singh Sareen v. Union of India, SLP (C) No. 804 of 2017 (Supreme Court of India).
13. Mahi Sindhu v. National Watch House, Complaint No. 34 of 2025 (State Consumer Disputes Redressal Commission, U.T. Chandigarh, Dec. 15, 2025).
14. Nivedita Sharma v. Bharti Tele Ventures, Appeal No. FA-06/660 (Delhi State Consumer Disputes Redressal Commission, 2006).
15. Pankaj Chandgothia v. The Coffee Bean & Tea Leaf, Consumer Complaint No. 99 of 2023 (State Consumer Disputes Redressal Commission, U.T. Chandigarh, Dec. 28, 2023).
16. Pioneer Urban Land and Infrastructure Ltd. v. Govindan Raghavan, (2019) 5 SCC 725 (India).
17. Acquisti, Alessandro et al., The Economics of Privacy, 54 J. ECON. LIT. 442 (2016).

18. Degeling, Martin et al., We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on the Design and Decision-Making Process of Cookie Consent Notices, PROC. IEEE SYMP. SEC. & PRIVACY (2019).

19. Future of Privacy Forum, The Digital Personal Data Protection Act of India Explained, FPF BLOG (Aug. 14, 2023), https://fpf.org.

20. Jain, Aditya S., Decoding Consent Managers Under the Digital Personal Data Protection Act, 7 J. DATA PROT. & PRIVACY 406 (2025).

21. Khandelwal, Pankhudi, The Story of Data Portability in India: A Lack of Clarity, LAW SCHOOL POL'Y REV. (2024).

22. Matthan, Rahul, PRIVACY 3.0: UNLOCKING OUR DATA-DRIVEN FUTURE (HarperCollins India, 2018).

23. Porwal, Ishaan & Ravi, Manasa, Fiduciary Duties in the Digital Age: A Critical Examination of the Digital Personal Data Protection Act 2023, 5 INDIAN J. INTEGRATED RSCH. L. 1388 (2024).

24. Rai, Shivkrit, Saving Indian Consumers from Unfair Contract Terms – The Impact of Section 2(46) Consumer Protection Act, 2019, 10 INT'L J. ON CONSUMER L. & PRAC. 7 (2022).

25. Schaub, Florian et al., A Design Space for Effective Privacy Notices, SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2015).

26. Sridhar, Sriya, The Elephant Not in the Room: The DPDPA's Failure to Regulate Behavioural Tracking, LAW SCHOOL POL'Y REV. (May 7, 2024).

27. Taylor, Mark & Paterson, Jeannie, Protecting Privacy in India: The Role of Consent and Fairness in Data Protection, 16 INDIAN J. L. & TECH. 71 (2020).

28. The Right to Pry-vacy: Understanding India's Dystopian Data Protection Legislation, 55 NYU J. INT'L L. & POL. (2023).

29. Utz, Christine et al., Informed Consent in the Digital Age: A Legal Fiction?, LAWVS (2023).