



JOURNAL OF DIGITAL LAW, PRIVACY & CYBER GOVERNANCE

ISSN No. 9854-4655

Volume 1 | Issue 1

2026

© 2026 Journal of Digital Law, Privacy & Cyber Governance

Follow this and additional works at: <https://www.quillifypub.com/>

This article is brought to you for free and open access by the Journal of Digital Law, Privacy & Cyber Governance. It has been accepted for inclusion in the Journal of Digital Law, Privacy & Cyber Governance after due review.

In case of any suggestions or complaints, kindly contact info@quillifypub.com.

To submit your Manuscript for Publication in the Journal of Digital Law, Privacy & Cyber Governance, kindly email your Manuscript to <https://www.quillifypub.com/submit>.

Shining a Light on the DPDP Act: Battling Dark Patterns and Amplifying Transparency

Chirag Rastogi

Advocate

Dark Patterns and Meaningful Consent under the DPDP Act

Anirudh Alex Victor

Advocate

Abstract

The interface may present a challenge for refusal while a privacy notice can reveal what practices a platform engages in. This paper discusses what Indian law should say about this disconnect between disclosure and choice. It examines the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025 and the Guidelines for the Prevention and Regulation of Dark Patterns, 2023 issued by the Central Consumer Protection Authority (CCPA). The argument goes that a misrepresentation of the interface should only be judged by the type of information operation involved, the legal basis for processing the information, the right the duty is based on, and the evidence of any restriction of the right to choose. However, consent considerations only apply to misleading requests, excessive collection, and hindered withdrawal, and not to all processing operations or all consumer harms. The hypothetical examples illustrate the need for a combination of data-protection and consumer-protection analysis. The paper has also looked into the data of children, government exemptions, institutional independence and amendment to the Right to Information Act. It separates the prospective obligations from provisions as of 17 October 2026. It finds that transparency alone is not enough; it needs to be understandable with usable choices, and cannot be a one-way street, with records that should be available to examine decisions.

Keywords: digital personal data; consent; dark patterns; interface design; transparency; consumer protection; India.

1 Introduction

Consider a service that displays a detailed privacy notice but permits registration only after the user accepts unrelated marketing. The notice may describe the practice accurately. The remaining question is whether the choice offered through the service is legally meaningful. A similar difficulty arises when agreement takes one step but withdrawal requires searching several screens and contacting support. These examples show why the quality of an interface matters to the exercise of privacy rights, even when a platform has published information about its processing.

The Digital Personal Data Protection Act, 2023 (DPDP Act) supplies important standards for examining these practices. Its provisions on notice, consent and withdrawal connect legal requirements to what a user encounters when providing personal data. However, the Act is not a comprehensive prohibition of every deceptive commercial interface. Its application depends on personal-data processing, statutory scope, the processing ground and any relevant exemption. Consumer law supplies a separate route through the Central Consumer Protection Authority

(CCPA) Guidelines for Prevention and Regulation of Dark Patterns, 2023 (Dark Patterns Guidelines).^{1,2}

Aman Tiwari's article, "Shining a Light on the DPDP Act: Battling Dark Patterns and Amplifying Transparency," connects the Act's consent provisions with deceptive design and raises concerns about state power and institutional structure. That discussion is acknowledged as a starting point. The present paper develops a more specific inquiry: how should a particular interface practice be connected to a particular legal duty, and what evidence would justify the connection?³

The central argument is that transparency must be assessed at the point of decision and throughout the subsequent processing relationship. Information matters when it helps a person understand a choice; the structure of the choice matters when it determines whether that understanding can be acted upon. This argument supports a combined assessment of disclosure, refusal, withdrawal and implementation. It also requires restraint: a poor design, a security incident and an unlawful processing operation are distinct problems, even when they occur in the same service.

2 Research approach and scope

This is a doctrinal and analytical study of selected legislation, delegated instruments, judicial materials and research on interface design. The primary materials are the DPDP Act, its commencement notification, the 2025 Rules and corrigendum, and the Dark Patterns Guidelines. The paper also considers the constitutional privacy principle in *Puttaswamy*, the *LinkedIn* litigation as a limited comparative example, and scholarship on privacy-related design practices. The materials are selected for their relevance to consent, transparency and the practical exercise of choice; the discussion is not a systematic review of all privacy scholarship.

The analysis separates three kinds of statement. Descriptions of legal requirements are supported by the relevant provision or instrument. Interpretations explain how those requirements might apply to a design practice. Recommendations propose safeguards whose adoption is argued for, rather than assumed to be universally mandated. The examples below are hypothetical analytical scenarios, not findings from an audit of any named platform. No interviews, surveys, experiments or new measurements of dark-pattern prevalence are claimed.

The legal position is assessed as at 17 October 2026. This cutoff is material because the Act and Rules have staged commencement. Discussion of a future duty explains the enacted framework and preparation for its operation; it does not assert that the duty already supports enforcement against conduct occurring before its commencement. The paper does not assess the merits of any pending constitutional challenge or claim that its proposed analytical approach has been adopted by a court.

3 Privacy scholarship and the problem of interface choice

The constitutional foundation is broader than a statutory definition of privacy. In *Puttaswamy*, the Supreme Court recognised privacy as protected through Article 21 and the freedoms in Part III of the Constitution. The absence of a single definition in the DPDP Act therefore does not

1 Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India), ss. 3–7 and 17.

2 Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023 (30 November 2023), guidelines 2–6.

3 Aman Tiwari, "Shining a Light on the DPDP Act: Battling Dark Patterns and Amplifying Transparency," *The Amikus Qriæ* (undated webpage), sections on consent, dark patterns and criticism.

establish an absence of legal protection. The useful inquiry is which aspect of privacy a particular measure affects and whether its interference can be justified. This paper concentrates on informational privacy and practical control over decisions concerning personal data.⁴

Bösch and co-authors analyse privacy dark strategies and patterns as organised ways of threatening privacy through system design. Their contribution helps shift attention from an isolated misleading sentence to the surrounding process that extracts or exploits information. Mathur and co-authors examine shopping websites and develop a taxonomy of practices that affect decision-making. These studies supply analytical vocabulary; their findings should not be treated as a measurement of Indian platforms in 2026.^{5,6}

These strands address related but different questions. Constitutional analysis concerns protected interests and justification. Design research examines mechanisms that influence behaviour. Statutory analysis identifies duties, exceptions and consequences. A finding in one strand does not automatically settle the others. A design may be manipulative without falling within every element of a particular statute, while a processing practice may breach a statutory duty without using an obviously deceptive interface. Keeping these distinctions visible makes criticism more precise and remedies more suitable.

4 The legal framework and its commencement

4.1 Scope roles and processing grounds

Section 3 addresses digital personal data processed within India, including data collected in non-digital form and digitised subsequently. It also covers specified processing outside India connected with offering goods or services to Data Principals within India. Its exclusions include personal or domestic processing by an individual and specified publicly available data. The framework is consequently not expressed simply as protection for Indian citizens, nor as regulation of all information wherever it is held.⁷

The allocation of roles matters when an interface is supplied through several organisations. A Data Principal is the individual to whom personal data relates, with the statutory inclusions for a child and a person with disability who has a lawful guardian. A Data Fiduciary determines the purpose and means of processing, alone or jointly; a Data Processor processes on its behalf. Hiring an external interface or storage provider does not itself answer who determines the relevant purpose or displace the fiduciary's statutory responsibility.⁸

Section 4 recognises processing for a lawful purpose on the basis of consent or the certain legitimate uses specified in section 7. The latter is a statutory list, not an unrestricted permission to invoke a business's interests. An assessment must therefore identify the claimed ground before testing consent. Equally, a platform cannot establish that an activity falls within section 7

4 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; principles summarised in the Supreme Court judgment of 26 September 2018 in the Aadhaar proceedings, discussion of the Puttaswamy principles, Part B, paras. 17–19.

5 Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp and Stefan Pfattheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns," *Proceedings on Privacy Enhancing Technologies* 2016(4), 237–254, doi:10.1515/popets-2016-0038, pp. 237–254.

6 Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty and Arvind Narayanan, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites" (2019), arXiv:1907.07032, abstract and taxonomy.

7 DPDP Act, s. 3.

8 DPDP Act, ss. 2(i)–(k) and 8(1)–(2).

merely by choosing a convenient label for it. The facts and the conditions of the relevant provision remain decisive.⁹

4.2 What is in force at the cutoff date

The commencement notification, G.S.R. 843(E) of 13 November 2025, separates institutional provisions from most operational duties. The immediate group includes sections 18–26 and section 44(3), among other provisions. A one-year stage covers section 6(9) and section 27(1) (d). An eighteen-month stage covers the core processing, consent and rights provisions, together with the principal inquiry and penalty provisions. At the paper’s cutoff, the last two stages have not yet arrived. The notification’s staged periods should therefore accompany any claim about present DPDP enforceability.¹⁰

The 2025 Rules have their own commencement provisions. Rules 1, 2 and 17–21 took effect on publication; rule 4 is assigned a one-year period, while rule 3 and the other deferred rules specified in rule 1(4) are assigned eighteen months. The December 2025 corrigendum must be read with the notified text. Rule 3’s more detailed notice requirements are consequently relevant to readiness and interpretation of the forthcoming regime, rather than a presently operative notice obligation at this cutoff.^{11,12}

The Dark Patterns Guidelines, by contrast, provide for commencement on publication in the Official Gazette. They apply to platforms systematically offering goods or services in India, advertisers and sellers. Their continuing relevance is illustrated by the CCPA’s 2025 self-audit advisory to e-commerce platforms. The difference in timing has a practical consequence: preparation for future DPDP duties does not replace attention to consumer-protection requirements already in operation.^{13,14}

5 Connecting a design practice to a legal duty

5.1 Notice must support a specific decision

Section 5 links a request for consent to information about the personal data, the proposed purpose and the means of exercising relevant rights and making a complaint. Section 6(3) addresses the language and presentation of a consent request. Rule 3 will add an itemised account of the data and purposes and require the notice to be understandable independently of other information. These provisions give transparency a decision-related function: a person should be able to connect the request encountered on screen with the processing it authorises.^{15,16}

This function is weakened if a short invitation to accept is accompanied by a purpose that can be understood only after following several unrelated documents. The legal analysis should

9 DPDP Act, ss. 4 and 7.

10 Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Gazette of India, Extraordinary, Part II, section 3(i) (13 November 2025), paras. (a)–(c).

11 Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, section 3(i) (13 November 2025), read with the December 2025 corrigendum, rr. 1 and 3.

12 Ministry of Electronics and Information Technology, Corrigenda, G.S.R. 892(E) (10 December 2025), Gazette of India, Extraordinary, Part II, section 3(i), corrections to rule 1 and other provisions.

13 Dark Patterns Guidelines, guidelines 1 and 3.

14 Ministry of Consumer Affairs, Food and Public Distribution, “Central Consumer Protection Authority issues advisory to E-Commerce Platforms for self-audit within 3 months to detect Dark Patterns and ensure its resolution,” Press Information Bureau (7 June 2025), advisory and three-month self-audit period.

15 DPDP Act, ss. 5 and 6(3).

16 DPDP Rules 2025, r. 3.

identify exactly which information is missing or obscured and where it should have appeared. The mere length of a notice does not decide compliance. A long notice may explain a complex service accurately; a brief notice may conceal the very fact the person needs to decide. Presentation should be assessed in relation to the decision being requested.

5.2 An affirmative action does not settle consent quality

Section 6(1) requires consent to meet several conditions, including freedom, specificity and an informed, unambiguous affirmative action. It also limits consent to personal data necessary for the specified purpose. A recorded click is therefore evidence that an action occurred, not conclusive evidence that every statutory condition was met. An examination should reconstruct the options, their meaning, the purposes covered and the consequences of declining them.¹⁷

A useful distinction is between data needed to deliver a requested function and data sought for a separate commercial purpose. A retailer may need a delivery address to dispatch an order. Access to the buyer's address book requires a different explanation; it does not become necessary for dispatch merely because the platform includes both permissions in one screen. The analysis should examine each asserted purpose and its factual relationship to the data. It should avoid the opposite overstatement that every condition attached to a digital service is necessarily unlawful.

5.3 Withdrawal exposes continuing interference with choice

Section 6(4) requires the ease of withdrawing consent to be comparable to the ease of giving it. Sections 6(5)–(6) address consequences and cessation, including the statutory qualification for processing required or authorised under the Act, Rules or another law. Withdrawal must thus be analysed separately from cancellation of a subscription, deletion of an account and erasure of every retained record. A service should not represent one of these actions as automatically accomplishing all the others.¹⁸

A workable assessment compares the complete routes into and out of the relevant processing. The number of steps is useful evidence, but cannot be the sole measure. A brief, reasonable identity check may protect a person from an unauthorised request. Repeated sales messages, hidden links or a compulsory explanation of personal motives may instead create avoidable friction. The proposed test is whether the additional steps have a defensible function proportionate to the request, rather than whether the two routes are mechanically identical.

5.4 Evidence must connect the interface to the processing

The paper proposes four linked questions for analysing a disputed design. First, what personal data operation or consumer decision is affected? Second, which processing ground and applicable instrument are relied upon? Third, what feature interferes with the duty or choice at issue? Fourth, what evidence connects the feature to the resulting processing or transaction? This sequence prevents a pattern label from standing in for a legal explanation.

Useful evidence may include dated screen captures, the applicable notice version, the options presented, the recorded choice, subsequent preference changes and the system response. Section 6(10) places a particular burden on the fiduciary to prove notice and valid consent when consent is the basis of processing and the issue arises in proceedings. Retaining proportionate records is therefore relevant, but should not become an excuse to collect excessive personal data about

¹⁷ DPDP Act, s. 6(1).

¹⁸ DPDP Act, s. 6(4)–(6).

every interaction. The record should explain the decision without recreating an unnecessary profile of the individual.¹⁹

6 The complementary role of consumer protection

The Dark Patterns Guidelines connect deceptive interface practices with impaired consumer autonomy, misleading advertising, unfair trade practices or violations of consumer rights. Their annexure specifies thirteen patterns, including forced action, subscription traps, interface interference, drip pricing and trick questions. These are the relevant Indian regulatory categories. Historical design labels can remain useful in scholarship, but should not be presented as though they are the Guidelines' complete list.²⁰

A late-disclosed price may primarily impair a purchase decision. A disguised advertisement may conceal who is promoting a product. Neither situation requires an analyst to assume that consent to personal-data processing is the principal issue. Conversely, a confusing marketing permission may affect data processing even where no purchase occurs. Where both regimes are engaged, each must be applied on its own terms. The Guidelines expressly operate in addition to other laws; that supports coordination, without making one regime's elements or remedies interchangeable with the other's.²¹

6.1 Hypothetical example of bundled marketing permission

Suppose an online shop presents one mandatory box covering order fulfilment, promotional messages and access to contacts. A consumer-protection assessment would examine whether access to the intended purchase has been made conditional on an unrelated action of the kind addressed in the Guidelines. A prospective DPDP assessment would separately examine the processing ground for each purpose, the specificity and quality of any consent, and whether the data sought are necessary for the specified purpose. The original box and the resulting system permissions would both matter.^{22,23}

The proposed remedy is to separate the necessary purchase information from the additional permissions, explain the additional purpose and make the consequences of refusal intelligible. This is an analytical recommendation based on the scenario, not a finding that every combined screen violates the law. If the facts show that a different processing ground applies, the reviewer must test that ground rather than assume that improving a consent box resolves the issue.

6.2 Hypothetical example of obstructed withdrawal

Suppose a subscription service accepts marketing consent during registration but permits withdrawal only through a concealed support route that repeatedly redirects the user to retention offers. The consumer question may concern a subscription trap or interface interference, depending on the decision being obstructed. The prospective DPDP question concerns withdrawal from the particular consent-based processing. Cancelling the subscription and stopping marketing should be traced as separate operations, even if the interface presents them together.^{24,25}

19 DPDP Act, s. 6(10).

20 Dark Patterns Guidelines, guideline 2(1)(e) and Annexure 1.

21 Dark Patterns Guidelines, guideline 6 and Annexure 1, items 8–9.

22 Dark Patterns Guidelines, Annexure 1, item 4.

23 DPDP Act, ss. 4 and 6(1).

24 Dark Patterns Guidelines, Annexure 1, items 5–6.

25 DPDP Act, s. 6(4)–(6).

The decisive evidence would include the route offered, the time and effort required, the platform's response and whether marketing actually ceased. An accessible withdrawal control with no effective connection to the marketing system is an implementation failure. A functioning system behind an undiscoverable control is a usability failure. Both deserve attention, but the corrective action differs: one requires changing system behaviour; the other requires making the available choice usable.

6.3 What the LinkedIn example can and cannot establish

The LinkedIn litigation is useful because it distinguishes initial invitations from later reminder emails sent using members' identities. The court materials address whether authorisation for one step extended to subsequent communications. The final approval order of 16 February 2016 approved a settlement involving a \$13 million fund and changes to the service. That was a United States class settlement, not an Indian regulatory penalty or a ruling interpreting the DPDP Act.^{26,27}

The limited lesson is that the scope of a permission must be examined across the sequence of actions it is said to authorise. It does not follow that every automated reminder is unlawful or that a foreign settlement establishes an Indian statutory breach. For the Indian analysis, the service's actual purpose, the wording and scope of the request, its processing ground and the applicable instrument would still have to be established.

7 Government processing children and institutional safeguards

7.1 Government powers require distinct analysis

Section 7(b), section 17(2)(a), section 17(4) and section 36 concern different matters. They address, respectively, specified benefits and services, notified state instrumentalities and purposes, exceptions affecting certain state-processing obligations, and the power to call for information for the Act's purposes. It is inaccurate to combine them into a single assertion that government can disregard the entire framework whenever it chooses. It is equally inadequate to treat the existence of statutory language as a complete answer to concerns about necessity and oversight.²⁸

A stronger critique identifies the data involved, the exact power used, its conditions and the safeguards available. The policy recommendations here are to explain the purpose of a request, limit access to what that purpose requires, maintain reviewable records and subject continuing retention to periodic scrutiny. These recommendations respond to risks of excessive collection and use. They do not claim that consent is the appropriate legal ground for every public function, nor that every power has already been declared unconstitutional.

7.2 Children's safeguards and their limits

Section 9 addresses verifiable parental or guardian consent, processing likely to harm a child's well-being, and tracking, behavioural monitoring and targeted advertising directed at children. Its exemption mechanisms must be described accurately. Section 9(4) concerns subsections (1) and (3), while section 9(5) creates a distinct mechanism tied to verifiably safe processing. These

26 Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1222 (N.D. Cal. 2014), No. 13-CV-04303-LHK, order of 12 June 2014 (ECF No. 47), order of 12 June 2014, discussion of initial and reminder emails.

27 Perkins v. LinkedIn Corp., No. 13-CV-04303-LHK (N.D. Cal.), order granting final approval of class action settlement (16 February 2016), ECF No. 134, order of 16 February 2016, settlement consideration and non-monetary relief.

28 DPDP Act, ss. 7(b), 17(2)(a), 17(4) and 36.

provisions should not be described as a general power to exempt all duties in subsections (1)–(3). Rules 10 and 12 and the Fourth Schedule provide further relevant detail for the deferred framework.^{29,30}

The design issue is not resolved merely by adding a guardian-consent screen. A child-facing service may still use persistent rewards or prompts to induce unnecessary disclosure. Conversely, age or guardianship verification can itself require additional information. The recommended approach is to justify the information needed for verification, avoid unrelated reuse and examine the whole interaction after consent. These are design and governance recommendations; their precise mandatory content depends on the applicable provision, exemption and facts.

7.3 Independence and reasoned decision making

The Act provides for the Data Protection Board of India and delegates the number of members to notification. Section 19(3) requires at least one legal expert, not exactly one. The government's appointment role and the two-year renewable terms under section 20 can be examined as institutional design choices. A useful critique asks how appointments, resources, reasoning and review affect the Board's ability to scrutinise powerful public and private entities. It does not infer incompetence merely from the inclusion of technical or administrative expertise.³¹

The proposed safeguards are transparent selection criteria, adequate technical support, clear reasons for findings and accessible routes of challenge. These would make interface disputes easier to evaluate where legal validity depends on technical behaviour. The recommendation also recognises a practical difficulty: an adjudicator must understand what a screen communicated and what the underlying system did. Legal and technical expertise should inform the same inquiry rather than produce separate conclusions that cannot be reconciled.

7.4 Privacy and access to public information

Section 44(3) substitutes the personal-information exemption in section 8(1)(j) of the Right to Information Act, 2005, and belongs to the immediate commencement group. The effect on access to records warrants separate consideration from the DPDP Act's deferred consent duties. An assessment should also consider the RTI Act's public-interest override in section 8(2) and severability provision in section 10. The amendment does not justify an unqualified assertion that any record containing personal information must always be withheld in full.^{32,33,34}

The concern developed here is that broader exemption language may increase the importance of careful reasoning about public interest and partial disclosure. A public authority should distinguish information that exposes private affairs from information needed to scrutinise public action, without assuming that the distinction will be easy in every case. Transparency about public administration and protection of individuals can be advanced together when decisions explain the interests considered and why redaction would or would not suffice.

²⁹ DPDP Act, s. 9.

³⁰ DPDP Rules 2025, rr. 10 and 12 and Fourth Schedule.

³¹ DPDP Act, ss. 18–20.

³² DPDP Act, s. 44(3).

³³ DPDP commencement notification, G.S.R. 843(E), para. (a).

³⁴ Right to Information Act, 2005, No. 22 of 2005 (India), especially sections 8(2) and 10; section 8(1)(j) amended by DPDP Act, section 44(3), ss. 8(2) and 10, read with the amendment to s. 8(1)(j).

8 Organisational responsibilities and practical compliance

A useful compliance review begins with a purpose-based account of data flows. For each operation, an organisation should identify the data, the responsible fiduciary and processor, the claimed processing ground, the interface through which information or consent is obtained, and the route for exercising relevant rights. This joins legal analysis to system design. A general assurance that the organisation values privacy cannot reveal whether a withdrawn preference reaches an outsourced marketing service.

The Act's enacted structure supports this operational focus. Section 8 addresses fiduciary responsibility, contracts with processors, safeguards and grievance arrangements. Sections 11–14 concern access to information, correction and erasure, grievance redressal and nomination. The Act does not create a general data-portability right. Section 10 imposes additional obligations on Significant Data Fiduciaries; a statutory DPO appointment must not be described as mandatory for every organisation merely because specialist advice may be useful.³⁵

Interface review should therefore involve legal, product and technical personnel. Before changing a consent screen, they should identify which processing permissions it actually controls. After release, they should verify that choices are stored accurately, communicated to relevant processors and reflected in later processing. Staff training should use concrete examples from the service. These measures are recommended ways of translating the framework into practice; they do not replace the need to identify the exact duties applicable to the organisation and commencement date.

Evidence retention must itself be proportionate. Versioned notices and interface specifications can document what users encountered without storing unnecessary copies of personal communications. Access to consent records should be controlled, and retention should have a stated purpose. Small organisations may use simpler systems than large platforms, but simplicity should not obscure the processing ground or make refusal and withdrawal ineffective. The aim is a defensible account of decisions, rather than the largest possible collection of compliance documents.

Penalties should be discussed with equal precision. Section 33 and the Schedule provide the enacted framework for monetary penalties after the specified inquiry and assessment, while section 34 directs the amounts realised to the Consolidated Fund of India. They do not establish that every interface labelled a dark pattern automatically attracts a particular DPDP fine or an individual compensation award. At the cutoff date, the principal penalty provisions remain in the deferred commencement group.^{36,37}

9 Emerging technologies and further research

Personalised interfaces create a further analytical problem: different users may encounter different routes to the same decision. An AI system may alter the timing, language or ordering of requests. Blockchain-based storage may complicate a requested change or erasure, depending on what information is stored and how. Connected devices may distribute notices and controls across a device and an app. These are possible design problems requiring investigation, not evidence that a particular technology is inherently unlawful or exempt from ordinary processing duties.

³⁵ DPDP Act, ss. 8 and 10–14.

³⁶ DPDP Act, ss. 33–34 and Schedule.

³⁷ DPDP commencement notification, G.S.R. 843(E), para. (c).

Future work should compare interface versions with actual preference records and system behaviour. An empirical study could measure the time, errors and successful completion of refusal and withdrawal tasks across languages and devices. It would need a stated sample, an ethics protocol, reliable legal classification and a method for distinguishing necessary verification from avoidable obstruction. Such evidence would help test the proposed approach; the present doctrinal analysis cannot establish prevalence, causal behavioural effects or the performance of any named platform.

Regulatory coordination is another priority. Where one interface creates both a consumer harm and a personal-data issue, investigators need a shared factual account while preserving each authority's jurisdiction and legal tests. Coordinated evidence collection could reduce duplication without assuming identical remedies. The practical goal is to correct the source of the harm, such as a hidden permission or an ineffective withdrawal mechanism, rather than require cosmetic changes that leave the processing untouched.

10 Conclusion

The DPDP Act's relevance to dark patterns lies in identifiable duties concerning processing grounds, information, consent and the exercise of rights. Its contribution should not be exaggerated into a complete design code. A convincing assessment links a particular interface feature to a particular duty, establishes the facts and respects the difference between enacted provisions and those in force. The Dark Patterns Guidelines supply a complementary consumer-protection route whose relevance does not depend on every dispute being recast as a privacy problem.

The paper's proposed approach follows the decision from presentation to implementation. It asks what the person was invited to authorise, whether the available route supported that decision, what processing followed and whether a later change of choice had effect. This makes transparency an operational question as well as a question of wording. It also supplies a more useful basis for organisational review than assuming that a detailed notice or a recorded click establishes valid consent.

Government powers, children's protections, institutional design and access to public information require their own careful treatment. Criticism is stronger when it identifies the relevant provision and explains a practicable safeguard. The priorities developed here are understandable choices, proportionate evidence, effective implementation and reasoned oversight. Together, they offer a defensible way to assess deceptive design while preserving the distinctions on which accurate legal analysis depends.