

**INTERNATIONAL JOURNAL OF LAW  
MANAGEMENT & HUMANITIES**  
**[ISSN 2581-5369]**

---

**Volume 9 | Issue 5**

---

**2026**

---

© 2026 International Journal of Law Management & Humanities

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

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [support@vidhiaagaz.com](mailto:support@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Consent or Coercion? Dark Patterns and the Illusion of User Autonomy under India's Digital Personal Data Protection Framework

---

GORANTLA UDAI DEEPAK\*  AND GANGAPURI MURALI\*\* 

## ABSTRACT

*Consent is the principal legitimating device of contemporary data-protection law, yet digital interfaces increasingly shape rather than merely record individual choice. This article examines whether consent obtained through dark patterns can satisfy the Digital Personal Data Protection Act, 2023 (DPDP Act) and the constitutional requirement of informational autonomy. It adopts a doctrinal and interdisciplinary methodology, analysing the DPDP Act, the Digital Personal Data Protection Rules, 2025, Indian constitutional privacy jurisprudence, consumer-protection regulation, the European Union's General Data Protection Regulation (GDPR), and behavioural scholarship on interface manipulation. The article finds that section 6 of the DPDP Act imposes a demanding cumulative standard requiring voluntariness, purpose specificity, adequate information, freedom from impermissible conditions and unmistakable affirmative conduct but the framework does not expressly identify manipulative design, specify interface-neutrality duties, or create a direct evidentiary presumption against consent collected through prohibited dark patterns. Fragmented enforcement between data-protection and consumer-protection institutions may therefore permit formal compliance while substantive autonomy is impaired. Comparative experience also shows that disclosure and consent alone cannot correct structural power, cognitive overload and dependency on dominant platforms. The article argues that dark patterns materially affecting a data decision should create a rebuttable presumption that consent is invalid. It proposes coordinated enforcement, symmetrical choice architecture, purpose-specific consent, auditable consent records, design-risk assessments and fiduciary-style duties for high-risk data fiduciaries. The conclusion is that Indian data-protection law should retain consent, but reposition it within an accountability framework in which data fiduciaries bear responsibility for proving not merely that a click occurred, but that the digital environment enabled a genuine choice.*

**Keywords:** Dark patterns, Digital consent, Informational autonomy, Digital Personal Data Protection Act 2023, Data fiduciaries, Privacy, Behavioural manipulation

---

\* Author is a Final-year Law Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: <https://orcid.org/0009-0007-2798-4088>

\*\* Author is a Final-year Law Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: <https://orcid.org/0009-0005-0768-6126>

## I. INTRODUCTION

Consent occupies a paradoxical position in digital governance. It is treated as an expression of personal autonomy and as a legal ground for processing, although the environment in which it is obtained is commonly designed by the party that benefits from disclosure. Privacy notices, cookie banners, registration flows and account settings are not passive containers of information. Their sequencing, color, defaults, friction and timing can determine whether an individual accepts tracking, shares additional data or abandons an attempt to refuse. The central legal question is consequently not whether the user clicked “agree,” but whether the interface allowed a free and informed decision.

The Digital Personal Data Protection Act, 2023 represents India’s first comprehensive statute devoted to digital personal data.<sup>1</sup> Section 4 permits processing for a lawful purpose either on consent or for specified legitimate uses, while section 6 requires a voluntary, purpose-specific and adequately informed agreement, free from impermissible conditions and conveyed through unmistakable affirmative conduct.<sup>2</sup> The statute also requires the ease of withdrawal to be comparable to the ease of giving consent and places the burden of proving compliant notice and consent on the data fiduciary.<sup>3</sup> These provisions appear capable of responding to manipulation. Their effectiveness, however, depends on whether “free” and “unambiguous” consent are interpreted substantively or reduced to evidence of assent.

Dark patterns expose this difficulty. They include interface practices that obstruct cancellation, give visual prominence to acceptance, repeatedly pressure a user, introduce hidden costs or convert silence and fatigue into apparent agreement. India’s consumer-protection framework now expressly regulates several such practices.<sup>4</sup> Yet the relationship between that framework and the validity of consent under the DPDP Act remains underdeveloped. A design may therefore be recognised as an unfair consumer practice without a clear doctrinal consequence for the legality of the resulting personal-data processing.

This article addresses that gap. Existing literature compellingly criticises “privacy self-management,” documents the practical impossibility of reading privacy policies, and explains the economic logic of surveillance capitalism.<sup>5</sup> Separate scholarship identifies the behavioural

---

<sup>1</sup> The Digital Personal Data Protection Act, No. 22 of 2023 (India).

<sup>2</sup> *Id.* §§ 4, 6(1).

<sup>3</sup> *Id.* §§ 6(4), 6(10).

<sup>4</sup> *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, Gazette of India, pt. III sec. 4 (Nov. 30, 2023) (India).

<sup>5</sup> Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882–93 (2013); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL’Y FOR INFO. SOC’Y 543, 560–64 (2008); SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 8–12, 94–97 (2019).

techniques through which interfaces influence choice.<sup>6</sup> The unresolved Indian question is how those insights should affect the legal validity and proof of consent under sections 5 and 6 of the DPDP Act, read in light of constitutional informational privacy.

The article advances three claims. First, consent is a process rather than a momentary click; the design conditions preceding assent are relevant to whether it is free and informed. Secondly, a material dark pattern should create a rebuttable presumption that consent is invalid, because the data fiduciary controls both the interface and the evidence. Thirdly, consent cannot bear the entire regulatory burden. It must operate within a broader accountability system containing design duties, auditing, purpose limitation and coordinated enforcement.

The research asks: (i) when does a dark pattern negate valid consent under the DPDP Act; (ii) how should constitutional informational autonomy guide statutory interpretation; (iii) what does comparative experience under the GDPR reveal; and (iv) which remedies can convert formal consent into meaningful choice? Part 2 explains the methodology and literature. Parts 3 and 4 develop the constitutional and behavioural foundations. Parts 5 and 6 analyse Indian and comparative law. Parts 7 and 8 present the findings and proposed accountability model, followed by the conclusion.

## II. LITERATURE, METHODOLOGY AND ANALYTICAL FRAMEWORK

### A. The limits of privacy self-management

Daniel Solove describes the consent model as “privacy self-management”: individuals are expected to understand privacy policies, anticipate future uses and continuously manage disclosure.<sup>7</sup> That model breaks down because individuals face too many separate decisions, small disclosures accumulate, and human reasoning is necessarily constrained. Even a rational person cannot evaluate every downstream use, combination and inference at the moment of collection. Empirical work by Aleecia McDonald and Lorrie Cranor demonstrates the immense time required merely to read privacy policies, quite apart from understanding or bargaining over them.<sup>8</sup> Consent fatigue is therefore not simply carelessness; it is a predictable response to excessive and repetitive decision demands.

Behavioural scholarship adds that preferences are context-dependent. Defaults, salience, framing and friction influence decisions even where the same nominal options remain available.<sup>9</sup> In digital systems these effects are programmable and capable of continuous testing.

---

<sup>6</sup> Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999–1007 (2014).

<sup>7</sup> Solove, *supra* note 5, at 1882–93.

<sup>8</sup> McDonald & Cranor, *supra* note 5, at 560–64.

<sup>9</sup> Cass R. Sunstein, *Nudging: A Very Short Guide*, 37 J. CONSUMER POL’Y 583, 584–88 (2014).

A platform can optimize the placement and wording of prompts against behavioural data collected from millions of interactions. Ryan Calo accordingly describes digital market manipulation as an environment in which firms can identify vulnerability and personalize influence at unprecedented scale.<sup>10</sup>

Shoshana Zuboff situates these practices within surveillance capitalism, an economic order in which behavioural data are extracted and converted into products designed to forecast behaviour.<sup>11</sup> Jack Balkin's theory of information fiduciaries and Ari Ezra Waldman's relational account of privacy respond by shifting attention from isolated transactions to duties arising from dependence, trust and asymmetric knowledge.<sup>12</sup> These accounts support the proposition that consent should be evidence of autonomy, not a waiver that absolves the stronger party from responsibility.

## **B. Methodology**

This is principally a doctrinal research paper. It interprets the Constitution of India, the DPDP Act, the Digital Personal Data Protection Rules, 2025, the Consumer Protection Act, 2019 and the Guidelines for Prevention and Regulation of Dark Patterns, 2023. Judicial decisions are used to identify the constitutional content of privacy, dignity and decisional autonomy. The analysis is comparative rather than transplant-oriented: the GDPR and decisions of the Court of Justice of the European Union are examined to identify both useful safeguards and the continuing limits of consent-based regulation.

The research is interdisciplinary because legal validity cannot be assessed without understanding how interfaces affect decision-making. It therefore uses established behavioural and privacy scholarship as explanatory evidence. It does not report original experiments or claim statistically representative findings. Its contribution is a doctrinal synthesis: the statutory adjectives “free,” “informed” and “unambiguous” should be interpreted through constitutional autonomy and the observable structure of the consent interface.

## **C. A process-based test for consent**

The article evaluates consent through four connected dimensions. The first is information: whether the individual receives intelligible, purpose-specific notice before the decision. The second is voluntariness: whether refusal is realistically available without disproportionate detriment. The third is interface neutrality: whether the presentation avoids misleading

---

<sup>10</sup> Calo, *supra* note 6, at 1003–07.

<sup>11</sup> Zuboff, *supra* note 5, at 94–99.

<sup>12</sup> Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–09 (2016); ARI EZRA WALDMAN, *PRIVACY AS TRUST* 55–71 (2018).

prominence, obstruction, repeated pressure and disguised options. The fourth is accountability: whether the data fiduciary can demonstrate the notice, screen sequence, defaults and withdrawal route that existed when consent was obtained.

This test does not require every interface to be aesthetically identical. It asks whether design materially distorts the decision concerning personal data. Materiality prevents trivial interface imperfections from invalidating processing, while still recognizing that design can become coercive without physical force or an express threat.

### **III. CONSTITUTIONAL FOUNDATIONS OF INFORMATIONAL AUTONOMY**

#### **A. Privacy, dignity and control**

The Supreme Court's nine-judge decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognised privacy as intrinsic to life and personal liberty under Article 21 and connected it with dignity, autonomy and the freedom to make intimate choices.<sup>13</sup> Informational privacy concerns an individual's interest in controlling the dissemination and use of personal information. That control is not absolute, but State and private data practices capable of affecting fundamental freedom cannot be evaluated solely through contractual formalism.

The constitutional significance of privacy changes the interpretation of statutory consent. If informational autonomy is the value protected, an interface deliberately structured to procure acceptance cannot be treated as neutral merely because the user performed an affirmative action. The form of assent must be connected to its quality. A bright "accept all" button beside a concealed multi-stage refusal route, for example, records conduct but may fail to express autonomous preference.

The proportionality analysis developed in Indian constitutional jurisprudence also illuminates data governance. An interference with privacy requires legality, a legitimate aim, rational connection, necessity and safeguards against abuse.<sup>14</sup> Although this test directly governs State action, its emphasis on necessity and safeguards informs the obligations imposed by legislation on private data fiduciaries. Section 6's requirement that consent extend only to data necessary for the specified purpose reflects the same anti-excess principle.

#### **B. From formal liberty to substantive choice**

Formal liberty exists when options are technically present. Substantive autonomy requires that a person can understand and exercise those options without manipulation. Indian constitutional

---

<sup>13</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 298–300, 320–22.

<sup>14</sup> *Id.* at 509–10; *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1, 157–59.

law has repeatedly treated dignity as more than freedom from physical compulsion. In *Common Cause v. Union of India*, decisional autonomy was central to the recognition of advance directives and end-of-life choice.<sup>15</sup> In *Navtej Singh Johar v. Union of India*, autonomy and identity were protected against majoritarian and institutional constraint.<sup>16</sup> These decisions do not decide data-consent disputes, but they establish an interpretive orientation: choice must be real in the conditions in which it is exercised.

Dark patterns threaten substantive choice in three ways. They distort comprehension, increase the cost of refusal and exploit the user's limited attention. A consent process may therefore be procedurally complete yet constitutionally deficient in purpose. Reading section 6 consistently with Article 21 requires attention to the entire choice architecture.

### **C. Positive duties and private power**

Digital platforms exercise power through access, visibility, defaults and network dependence. A user may “agree” because a service is essential for work, education, finance or social participation, not because its secondary data uses are acceptable. Constitutional rights do not automatically convert every private platform into the State, but legislation enacted to protect privacy should not ignore concentrated private power.

The DPDP Act's fiduciary vocabulary is significant. A “Data Fiduciary” determines the purpose and means of processing.<sup>17</sup> The Act does not expressly impose a general duty of loyalty, but the term accurately identifies control. Because the fiduciary designs the interface and benefits from processing, it should bear the risk of uncertainty about whether consent was freely produced. Section 6(10), which places the burden of proof on the data fiduciary, provides the statutory basis for that allocation.

## **IV. DARK PATTERNS AS STRUCTURAL COERCION**

### **A. Meaning and principal forms**

Harry Brignull popularised the expression “dark patterns” for interface techniques deliberately arranged to steer users toward outcomes serving the designer rather than the user.<sup>18</sup> Under the Indian Guidelines, a design becomes a dark pattern when a platform's interface or user-

---

<sup>15</sup> *Common Cause v. Union of India*, (2018) 5 SCC 1, 168–72.

<sup>16</sup> *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1, 50–54, 215–18.

<sup>17</sup> DPDP Act, *supra* note 1, § 2(i).

<sup>18</sup> HARRY BRIGNULL, DECEPTIVE PATTERNS: EXPOSING THE TRICKS TECH COMPANIES USE TO CONTROL YOU 1–14 (2023).

experience arrangement misdirects users toward conduct they neither planned nor desired and, in doing so, compromises autonomous consumer decision-making.<sup>19</sup>

The Guidelines enumerate thirteen forms: false urgency, basket sneaking, confirm shaming, forced action, subscription traps, interface interference, bait and switch, drip pricing, disguised advertisements, nagging, trick wording, SaaS billing and rogue malware.<sup>20</sup> In a data-protection setting, several have direct consent consequences. Interface interference may visually privilege acceptance. Forced action may condition access on unnecessary data. Nagging may exhaust resistance. A subscription trap may make withdrawal substantially harder than consent. Trick wording may obscure whether an option enables or disables tracking.

Not every nudge is unlawful. Interfaces necessarily organise information and guide attention. The legal distinction should turn on purpose, effect and materiality. A benign nudge may facilitate an informed choice; a dark pattern subverts or obstructs it for the designer's benefit. Relevant evidence includes asymmetry between acceptance and rejection, preselected options, repeated prompts after refusal, misleading labels, hidden consequences and unnecessary loss of service.

## **B. Structural rather than episodic coercion**

Traditional coercion doctrine often searches for an identifiable threat. Digital coercion is frequently structural: the platform creates an environment in which one result is effortless and the alternative is confusing, delayed or costly. The manipulation is distributed across screens rather than expressed in one sentence. Each individual design choice may appear minor, but their cumulative effect can determine the outcome.

This structure explains why disclosure alone is inadequate. More text can increase rather than reduce opacity. A platform may truthfully disclose processing while placing the disclosure behind multiple links, presenting it at a moment of urgency, or combining necessary and optional purposes. The legal inquiry must therefore include how information is presented and what happens when the user refuses.

Dark patterns also exploit market power. Where a dominant service lacks practical substitutes, "take it or leave it" consent to unrelated data uses is not meaningfully voluntary. The issue is not that every imbalance invalidates consent, but that dependency intensifies the scrutiny required for necessity, bundling and detriment following refusal.

---

<sup>19</sup> *Guidelines for Prevention and Regulation of Dark Patterns*, 2023, *supra* note 4, ¶ 2(e).

<sup>20</sup> *Id.* annex. 1.

### C. Evidentiary significance

Interface design is controlled and recorded by the data fiduciary. Users rarely retain screenshots of every version of a consent flow, and interfaces may be altered remotely. If the user alone must prove manipulation, section 6's protection becomes illusory. The data fiduciary should preserve versioned records of the notice, choices, defaults, screen sequence, language and withdrawal mechanism associated with each consent event.

A proven material dark pattern should establish a rebuttable presumption that consent was not free or unambiguous. The fiduciary could rebut it by showing that the challenged design did not concern the processing at issue, that an equally accessible refusal was provided, or that consent was subsequently renewed through a neutral process. This approach aligns evidence with control and gives practical effect to section 6(10).

## V. THE INDIAN STATUTORY FRAMEWORK

### A. Consent under the DPDP Act

The DPDP Act distinguishes consent from “certain legitimate uses.”<sup>21</sup> It is therefore inaccurate to describe consent as the exclusive ground for processing. Where consent is relied upon, however, section 6 establishes demanding cumulative conditions. In the Act's terms, consent must be “free, specific, informed, unconditional and unambiguous with a clear affirmative action,” signify agreement to processing for the specified purpose, and extend only to the personal data necessary for that purpose.<sup>22</sup>

Section 5 requires a preceding or accompanying notice identifying the personal data and purpose, the manner of exercising withdrawal and grievance rights, and the mechanism for complaining to the Data Protection Board.<sup>23</sup> The request must be presented in “clear and plain language” and remain accessible in English or any language listed in the Eighth Schedule. The withdrawal mechanism must impose no greater difficulty than the original consent process. These requirements supply doctrinal tools against common dark patterns: bundling conflicts with specificity, hidden purposes undermine informed consent, pre-ticked boxes contradict affirmative action, and labyrinthine cancellation conflicts with comparable ease.

The 2025 Rules add operational detail concerning notices, consent managers, security safeguards, breach notification and the exercise of rights.<sup>24</sup> They improve procedural specificity

---

<sup>21</sup> DPDP Act, *supra* note 1, §§ 4, 7.

<sup>22</sup> *Id.* § 6(1).

<sup>23</sup> *Id.* §§ 5, 6(3).

<sup>24</sup> *Digital Personal Data Protection Rules, 2025*, Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025) (India).

but do not establish a comprehensive catalogue of forbidden consent-interface practices. The result is a regulatory space in which the Act's open-textured standards must perform substantial work.

## **B. Gaps in protection**

The first gap is the absence of an express design-fairness duty. "Clear and plain language" governs wording, but an individually clear sentence can still be embedded in a manipulative flow. The second is remedial ambiguity. The Act states that consent infringing the Act, rules or other law is invalid to the extent of infringement,<sup>25</sup> but does not specify the consequence of a dark pattern prohibited under consumer law. The third is institutional fragmentation: the Central Consumer Protection Authority addresses unfair consumer practices, while the Data Protection Board addresses contraventions of the DPDP framework.

The fourth gap concerns remedies. The statutory penalty structure primarily operates through regulatory proceedings. It does not itself create a broad compensatory cause of action for every individual affected by manipulative consent. Regulatory enforcement is therefore crucial, particularly where small harms are distributed among millions of users.

The fifth concern is the breadth of certain legitimate uses and exemptions. Consent reform cannot protect processing that lawfully proceeds without consent. Accountability obligations, purpose limitation, security, erasure, grievance redress and risk assessment, must therefore apply robustly across all lawful grounds, subject only to carefully construed statutory exceptions.

## **C. Consumer law as a complementary regime**

The Consumer Protection Act, 2019 prohibits unfair trade practices and empowers the Central Consumer Protection Authority to protect consumer rights.<sup>26</sup> The 2023 Dark Patterns Guidelines translate these general principles into interface-specific regulation. Their recognition of autonomy impairment is doctrinally valuable for interpreting whether consent under section 6 is free and unambiguous.

The regimes should be read complementarily. A consumer-law violation does not mechanically decide every data-protection issue, because the statutes have different elements and purposes. Nevertheless, where the same interface both violates the Dark Patterns Guidelines and obtains permission for personal-data processing, the violation is powerful evidence against valid

---

<sup>25</sup> DPDP Act, *supra* note 1, § 6(2).

<sup>26</sup> The Consumer Protection Act, No. 35 of 2019, §§ 2(47), 10, 18 (India).

consent. Regulators should establish referral and information-sharing procedures so that findings about interface design are not confined to separate institutional silos.

## VI. COMPARATIVE ANALYSIS: THE GDPR AND GLOBAL EXPERIENCE

### A. The GDPR standard

The GDPR defines consent as a “freely given, specific, informed and unambiguous” indication of wishes, communicated “by a statement or by a clear affirmative action.”<sup>27</sup> Article 7 requires the controller to demonstrate consent, permits withdrawal at any time, and requires withdrawal to be as easy as giving consent. Recital 42 stresses genuine or free choice, while Recital 43 warns that consent may not be freely given where there is a clear imbalance or where separate processing operations are unnecessarily bundled.

The Court of Justice of the European Union has rejected pre-ticked boxes as valid consent in *Planet49*.<sup>28</sup> In *Meta Platforms v. Bundeskartellamt*, the Court connected data-protection analysis with the market power of a dominant social network and emphasised that dominance is relevant though not automatically decisive to whether consent is freely given.<sup>29</sup> These authorities demonstrate that affirmative action and voluntariness require more than nominal acceptance.

European regulatory guidance also directly addresses deceptive design patterns in social-media interfaces.<sup>30</sup> The comparative lesson is not that the GDPR has solved consent. Rather, it shows the value of integrating substantive consent standards with design guidance, demonstrability and scrutiny of power imbalance.

### B. Persistent limits of consent

Even a stronger consent doctrine cannot eliminate information asymmetry or surveillance-based incentives. Users remain exposed to repeated requests and cannot realistically forecast every inference. Neil Richards and Woodrow Hartzog describe pathologies of digital consent arising when permission is used to legitimize practices that remain harmful, unexpected or exploitative. On that account, formal permission may be invoked to excuse data practices whose substance remains harmful or exploitative.<sup>31</sup>

---

<sup>27</sup> Regulation (EU) 2016/679, arts. 4(11), 7, 2016 O.J. (L 119) 1.

<sup>28</sup> Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände v. Planet49 GmbH*, ECLI:EU:C:2019:801, ¶¶ 52–63.

<sup>29</sup> Case C-252/21, *Meta Platforms Inc. v. Bundeskartellamt*, ECLI:EU:C:2023:537, ¶¶ 143–54.

<sup>30</sup> EUROPEAN DATA PROTECTION BOARD, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* 10–16 (version 2.0, adopted Feb. 14, 2023).

<sup>31</sup> Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463–75 (2019).

For that reason, the GDPR also imposes controller obligations independent of consent, including fairness, transparency, purpose limitation, data minimization, accountability, data protection by design and impact assessment.<sup>32</sup> India should draw the structural lesson: the quality of consent improves when the controller must first design lawful, proportionate and accountable processing. Choice should supplement those duties, not replace them.

## **VII. PRINCIPAL FINDINGS**

The analysis produces five principal findings. First, the DPDP Act already contains textual foundations for invalidating consent obtained through material dark patterns. “Free,” “informed,” “unconditional” and “unambiguous” are substantive conditions, not decorative adjectives. The comparable-ease rule for withdrawal directly addresses obstruction.

Secondly, statutory interpretation should be informed by constitutional autonomy. Puttaswamy requires attention to dignity, control and the conditions of choice. A purely click-based approach would protect records of assent while disregarding the value the legislation is intended to secure.

Thirdly, the present framework is fragmented. Consumer law expressly identifies dark patterns, whereas data-protection law defines valid consent without explicitly connecting prohibited design to invalidity. Coordination is needed to prevent inconsistent findings and duplicated proceedings.

Fourthly, proof is central. The fiduciary controls the interface and can modify it without leaving evidence accessible to the user. Section 6(10) should therefore require proof of the consent environment, not merely a timestamp and user identifier.

Fifthly, consent alone cannot govern structural data power. Even perfectly designed prompts cannot make every user understand future aggregation, inference and third-party use. Independent duties of minimization, fairness, security and purpose limitation remain indispensable.

## **VIII. RECOMMENDATIONS: AN ACCOUNTABILITY-BASED MODEL**

### **A. Rebuttable presumption of invalid consent**

The rules or authoritative regulatory guidance should provide that use of a material dark pattern in connection with a personal-data decision creates a rebuttable presumption that the resulting consent is invalid. Materiality should depend on whether the design was reasonably capable of

---

<sup>32</sup> Regulation (EU) 2016/679, *supra* note 27, arts. 5, 24–25, 35.

affecting acceptance, refusal, scope or withdrawal. This standard would avoid invalidating consent for inconsequential design defects.

### **B. Symmetrical choice architecture**

Acceptance and refusal should be presented with substantially equivalent prominence, language and accessibility. Optional purposes should not be bundled with processing necessary to deliver the requested service. Rejection should not require more screens, time or cognitive effort than acceptance. Repeated requests after refusal should be limited unless circumstances or purposes materially change.

### **C. Consent receipts and design records**

Data fiduciaries should maintain auditable records containing the operative notice, purpose, categories of data, interface version, defaults, language, time, affirmative action and withdrawal route. Data principals should receive a concise consent receipt and a persistent dashboard through which permissions can be reviewed and withdrawn. Proof should concern the quality and context of consent, not merely the existence of a database entry.

### **D. Design-risk assessment**

Significant Data Fiduciaries and platforms processing sensitive or high-volume behavioural data should incorporate interface manipulation into data-protection impact assessments. Assessments should test whether users understand the principal purposes, whether refusal produces disproportionate detriment, and whether vulnerable groups are especially susceptible to the design. Controlled user testing can supplement doctrinal compliance.

### **E. Coordinated enforcement**

The Data Protection Board and Central Consumer Protection Authority should adopt a coordination protocol covering referrals, evidence sharing and remedial consistency. A finding that an interface employs a prohibited dark pattern should be transmitted where the practice also affects data processing. Coordinated enforcement would preserve institutional jurisdiction while recognising that the same design may simultaneously impair consumer choice and data autonomy.

### **F. Fiduciary-style duties for high-risk processing**

For high-risk data practices, India should move toward duties of care and loyalty that prevent fiduciaries from using interface control to obtain permissions contrary to the user's reasonable interests. Such duties would not prohibit legitimate persuasion or personalization. They would

prohibit exploiting dependency, confidential access or known vulnerability to secure unnecessary processing.

## **IX. CONCLUSION**

The research problem is whether consent obtained within a manipulative interface can constitute valid consent under Indian data-protection law. The answer is not determined by the presence of a button or recorded affirmative action. Section 6 of the DPDP Act requires a qualitative judgment encompassing genuine voluntariness, purpose specificity, adequate information, freedom from impermissible conditions and unmistakable assent. Dark patterns that obscure purposes, privilege acceptance, penalize refusal or obstruct withdrawal are directly relevant to each of those requirements.

India's constitutional privacy jurisprudence reinforces this interpretation. Informational privacy protects autonomy and dignity, not the administrative convenience of collecting assent. A legal framework faithful to Puttaswamy must examine the conditions under which the individual chose. Consumer-protection regulation already recognises that interface design can impair autonomy, but its relationship with the DPDP Act must be made operational through coordinated enforcement and evidentiary consequences.

The article does not propose abandoning consent. Consent remains important because individuals should retain authority over optional and context-dependent uses of their data. The error lies in treating consent as sufficient. In environments characterised by cognitive overload, platform dependency and asymmetrical information, an isolated click cannot absolve the data fiduciary from duties of fairness, necessity and accountability.

A rebuttable presumption against consent obtained through a material dark pattern offers a principled bridge between existing statutory language and practical enforcement. Symmetrical interfaces, purpose-specific choices, versioned design records, risk assessments and coordinated regulation would further align legal form with genuine autonomy. The decisive shift is from asking whether the platform can prove that the user clicked to asking whether it can prove that the user was permitted to choose. Only then can consent function as an instrument of informational self-determination rather than a legal fiction legitimizing extraction.

\*\*\*\*\*