INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

MANIPULATIVE DESIGN AS PRIVATE REGULATION: DARK PATTERNS AND THE ARCHITECTURE OF DIGITAL NORMATIVITY

AUTHORED BY - TANISH DAHUJA

ABSTRACT

The regulatory imagination treating dark patterns as a species of deceptive trade practice obscures their constitutive character: they are not aberrations of consumer fraud but instruments of behavioural governance. Through choice architecture engineered to channel users toward platform-preferred outcomes, dark patterns operate as a decentralised, private mode of regulation that structures consent, transactional terms, and the practical conditions of digital autonomy. This article argues that India's current two-track regime, comprising the Central Consumer Protection Authority's Guidelines for Prevention and Regulation of Dark Patterns, 2023 and the consent provisions of the Digital Personal Data Protection Act, 2023, misclassifies an architectural problem as either market deception or consent defect, leaving the governance dimension legally untheorised. Drawing on private ordering theory, platform constitutionalism, and the comparative experience of the European Union and the United States, the paper proposes an architecture-based unfairness test grounded in foreseeable material influence.

I. INTRODUCTION

When a user attempts to cancel an Amazon Prime subscription, she traverses what Amazon's internal engineers branded the *Iliad Flow*, a four-page, six-click, fifteen-option cancellation labyrinth so deliberately arduous that its very name memorialises the friction by which platforms retain unwilling subscribers.[1] The Federal Trade Commission's action against Amazon, which culminated in September 2025 in a USD 2.5 billion settlement, illustrates how interface design can produce regulatory effects no statute formally authorises: it conscripts users into recurring transactions they did not knowingly intend to enter and holds them there

[1] *FTC v. Amazon.com, Inc.*, No. 2:23-cv-00932 (W.D. Wash. filed June 21, 2023); Press Release, FED. TRADE COMM'N, *FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel* (June 21, 2023).

ISSN: 2582-6433

through architectural rather than contractual force.[2]

The Indian regulator has recognised the underlying mischief. In November 2023, the Central Consumer Protection Authority (CCPA), invoking section 18 of the Consumer Protection Act, 2019, notified the Guidelines for Prevention and Regulation of Dark Patterns, 2023, defining and proscribing thirteen specified design practices ranging from drip pricing to confirmshaming to subscription traps.[3] The Digital Personal Data Protection Act, 2023, notified for phased commencement on 13 November 2025, requires that consent for the processing of personal data be 'free, specific, informed, unconditional and unambiguous', and expressly invalidates consent procured through any 'deceptive or manipulative practice'.[4]

The dominant scholarly and regulatory framing of dark patterns is unmistakable: they are deceptive trade practices, sometimes also consent defects, to be policed through disclosure, prohibition, and ex post enforcement.[5] This article argues that the framing is doctrinally underinclusive. Dark patterns are not aberrations of an otherwise honest market, intermittent failures of disclosure to be cured by injunction; they are instruments through which platforms exercise a form of decentralised, private regulatory power.[6] Interface architecture, by configuring defaults, prominence, friction, and the sequencing of choice, governs user conduct ex ante. It prescribes what is easy and what is costly, what is foregrounded and what is hidden, what counts as consent and what counts as exit.[7] In this sense the platform regulates its users not by issuing rules but by engineering the environment in which rules become superfluous.

Three claims follow. First, treating dark patterns merely as deception misclassifies an architectural problem as a transactional one; the harm is not isolated misrepresentation but the systemic shaping of choice environments. Second, India's current regime is structurally bifurcated: the CCPA Guidelines locate dark patterns within unfair trade practice doctrine, while the DPDP Act locates them within consent doctrine, leaving the regulatory-governance

[2] Press Release, FED. TRADE COMM'N, *FTC Secures Historic $2.5 Billion Settlement Against Amazon* (Sept. 25, 2025); Stipulated Order for Permanent Injunction, Monetary Relief, Civil Penalty Judgment, and Other Relief, *FTC v. Amazon.com, Inc.*, No. 2:23-cv-00932 (W.D. Wash. Sept. 25, 2025).

[3] Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. J-25/13/2022-CCPA, Gazette of India, Extraordinary, Pt. III, Sec. 4 (Nov. 30, 2023) [hereinafter CCPA Guidelines], notified under Consumer Protection Act, No. 35 of 2019, § 18, INDIA CODE.

[4] Digital Personal Data Protection Act, No. 22 of 2023, § 6(1), INDIA CODE [hereinafter DPDP Act]; Digital Personal Data Protection Rules, 2025, MINISTRY OF ELEC. & INFO. TECH., Notification (Nov. 13, 2025).

[5] *See, e.g.*, Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 49–50 (2021); FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT: AN FTC WORKSHOP STAFF REPORT 8–12 (Sept. 2022).

[6] LAWRENCE LESSIG, CODE: VERSION 2.0 121–25 (2006); Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO. COMM. & SOC'Y 118, 122–26 (2017).

[7] Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REG. 413, 425–30 (2015); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 18–25 (2019).

ISSN: 2582-6433

dimension legally homeless. Third, an adequate response demands a doctrinal device that interrogates design itself: an architecture-based unfairness test predicated on foreseeable material influence over user decision-making.

The article proceeds in four substantive Parts. Part II reframes dark patterns from persuasion to private regulation, drawing on the Lessigian and post-Lessigian tradition of architectural governance and on private ordering theory. Part III maps the Indian two-track regime and identifies the doctrinal gap between consumer protection and data protection. Part IV draws comparative lessons from Article 25 of the EU's Digital Services Act, the FTC's enforcement under the Restore Online Shoppers' Confidence Act, and California's choice-architecture jurisprudence. Part V proposes an architecture-based unfairness test and addresses anticipated objections. A brief Conclusion sets out doctrinal implications.

II. FROM PERSUASION TO POWER: REFRAMING DARK PATTERNS

Harry Brignull's coinage of *dark patterns* in 2010 captured a phenomenon that had already become endemic: interfaces engineered not to assist user goals but to subvert them.[8] The Princeton crawl of approximately 11,000 shopping websites by Mathur and colleagues identified 1,818 instances of dark patterns across 1,254 sites, with prevalence positively correlated with site popularity.[9] Luguri and Strahilevitz's controlled experiment found that even mild dark patterns more than doubled enrolment in an undesired programme, while aggressive variants approached quadrupling.[10] These are not anecdotes of bad design; they describe a regularity of digital commerce.

What this body of evidence resists, however, is the consumer-protection framing it has typically received. The consumer-protection model presupposes a discrete transaction, a misleading representation, and a remedy of disclosure or prohibition. Yet most dark patterns involve no representation at all in the traditional sense. A pre-ticked box does not assert a falsehood. A confusingly placed reject-cookies button does not lie. A multi-step cancellation flow makes no claim. What these designs do, instead, is shape the costs and salience of choices,

[8] Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011); *see also* Colin M. Gray et al., *The Dark (Patterns) Side of UX Design*, *in* PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1, 3–4 (2018).

[9] Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM.-COMPUT. INTERACTION (CSCW), Art. 81, at 1, 5–8 (Nov. 2019) (identifying 1,818 dark pattern instances on 1,254 sites; prevalence positively correlated with site popularity).

[10] Luguri & Strahilevitz, *supra* note 5, at 63–68 (mild dark patterns more than doubled acceptance from 11% baseline to 25.8%; aggressive variants reached 41.9%).

ISSN: 2582-6433

producing predictable behavioural outcomes regardless of the user's stated preferences.[11]

This is why the most analytically productive lens is regulatory rather than transactional. Lawrence Lessig's foundational claim that code can do regulatory work by structuring possibility has become a near-cliché, but the underlying insight retains its force.[12] When platforms configure their interfaces, they perform the same kind of behavioural channelling that statutes and regulations attempt: they render some outcomes systematically more probable and others systematically less so, without recourse to commands or sanctions. Where this is done deliberately, calibrated against measured behavioural response, and at population scale, the difference between interface design and regulation collapses into a question of formal authority rather than functional character.[13]

The shift from persuasion to private regulation has three doctrinal consequences. First, it relocates the legal interest. Where consumer protection law guards against transactional deception, an architectural lens recognises that the protected interest extends to the user's decisional environment itself: her capacity to choose under conditions she has reason to accept.[14] Second, it widens the temporal frame. Consumer protection intervenes after a misrepresentation; an architectural lens insists that regulation must address the ex ante design choices that pre-structure outcomes before the transactional moment arrives.[15] Third, it expands the relevant actor. Deception doctrine identifies the seller as wrongdoer. Architectural analysis recognises that the platform, whether or not it is the seller, is the regulator of the choice environment, and that its design choices are normative artefacts of governance.[16]

Crucially, this is not a turn away from law. It is precisely because architecture functions regulatorily that law must engage it on those terms. The danger of the consumer-protection lens is not that it is wrong but that it is partial: it captures the symptom of individual deception while leaving the engine of population-scale behavioural production legally untheorised.[17] The

[11] Susser, Roessler & Nissenbaum, *supra* note 7, at 20–22; Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003–08 (2014).
[12] LESSIG, *supra* note 6, at 121–25; for an updated articulation in the algorithmic context, *see* Yeung, *supra* note 6, at 122–26.
[13] Calo, *supra* note 11, at 1015–18; *see also* Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 165–70 (2019).
[14] Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 ANTITRUST L.J. 771, 786–91 (2019); *cf. Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 297 (Chandrachud, J.) (locating informational autonomy within Article 21).
[15] Roger Brownsword, *Code, Control, and Choice: Why East Is East and West Is West*, 25 LEGAL STUD. 1, 8–12 (2005); *see also* ROGER BROWNSWORD, LAW, TECHNOLOGY AND SOCIETY: REIMAGINING THE REGULATORY ENVIRONMENT 79–86 (2019).
[16] Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 152–58 (2017); Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 90–94 (2016).
[17] K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1652–58 (2018).

ISSN: 2582-6433

doctrinal task is to import into law the recognition, long established in regulatory theory, that those who structure choice environments wield power that warrants legal accountability.[18]

III. THE INDIAN REGULATORY ARCHITECTURE: A FRAGMENTED TWO-TRACK REGIME

India's regulatory response to dark patterns took shape during a brief window in late 2023 in which two distinct legal instruments addressed the phenomenon from incompatible angles. The CCPA Guidelines came first, treating dark patterns as unfair trade practices under the Consumer Protection Act, 2019. The DPDP Act followed, treating manipulative design as a consent defect under data protection law. The two-track approach mirrors, in attenuated form, the European bifurcation between the Unfair Commercial Practices Directive and the General Data Protection Regulation, and reproduces its doctrinal incompleteness.

A. The CCPA Guidelines and the Unfair-Trade-Practice Frame

The CCPA Guidelines define dark patterns as 'any practices or deceptive design pattern using UI/UX interactions on any platform' that mislead or manipulate users into doing something they did not originally intend, 'subverting or impairing the consumer autonomy, decision making or choice'.[19] Annexure I specifies thirteen practices: false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick question, SaaS billing, and rogue malware.[20] The Guidelines apply to all platforms 'systematically offering goods or services in India', including foreign entities, and operate as a supplementary layer alongside other unfair-trade-practice law.[21]

The Guidelines' analytic structure is unambiguous: dark patterns are species of unfair trade practice or misleading advertisement, enforceable through the CCPA's existing powers under sections 18 and 19 of the Consumer Protection Act.[22] No independent penalty regime is created; recourse runs through the Act's general apparatus for unfair-trade-practice complaints and

[18] Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1153–58 (2018); ALGORITHMIC REGULATION (Karen Yeung & Martin Lodge eds., 2019).
[19] CCPA Guidelines, *supra* note 3, ¶ 2(e).
[20] *Id.* annex. I, ¶¶ 1–13. The thirteen specified practices are: false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick question, SaaS billing, and rogue malware.
[21] *Id.* ¶¶ 3–4; Press Release, PRESS INFO. BUREAU, GOV'T OF INDIA, *Central Consumer Protection Authority Notifies Guidelines for Prevention and Regulation of Dark Patterns, 2023* (Nov. 30, 2023).
[22] Consumer Protection Act, No. 35 of 2019, §§ 18–19, INDIA CODE; CCPA Guidelines, *supra* note 3, ¶ 5.

ISSN: 2582-6433

misleading-advertisement orders.[23] In June 2025, the CCPA reinforced this position through an advisory directing e-commerce platforms to conduct three-month self-audits to identify and remediate dark patterns on their interfaces, an enforcement strategy whose efficacy depends almost entirely on platform cooperation.[24]

Three doctrinal limitations follow from this framing. The first is conceptual. By assimilating dark patterns into the misleading-advertisement and unfair-trade-practice categories, the Guidelines retain those categories' transactional and representational architecture. They require, at minimum, that the design 'mislead' or 'deceive', a vocabulary ill-fitted to designs that operate through friction, salience, and default rather than through representation.[25] The second is institutional. Enforcement runs through complaint-driven mechanisms ill-suited to addressing population-level design choices that may individually appear innocuous but cumulatively produce regulatory effects. The third is remedial. The Act's toolkit (cease-and-desist orders, advertising injunctions, refunds, and limited penalties) addresses past harms rather than ex ante design configuration; it neither demands a baseline of design fairness nor establishes preventive obligations of fairness-by-design.[26]

B. The DPDP Act and Architecturally-Procured Consent

Section 6(1) of the DPDP Act offers a parallel but distinct route. Consent must be 'free, specific, informed, unconditional and unambiguous', and the statutory gloss on 'free' expressly requires that it be 'given without her being subjected to any deceptive or manipulative practice'.[27] Section 6(2) supplies the remedial consequence: any part of consent which infringes the Act is 'invalid to the extent of such infringement'.[28] In principle, this offers a powerful tool. Consent obtained through architectural manipulation is not merely actionable as an unfair trade practice; it is legally void as a basis for processing.

---

[23] Consumer Protection Act, No. 35 of 2019, § 2(47) (defining "unfair trade practice"); *id.* § 21 (powers of CCPA against misleading advertisements).

[24] Press Release, DEP'T OF CONSUMER AFFAIRS, GOV'T OF INDIA, *CCPA Advisory to E-Commerce Platforms on Self-Audit for Dark Patterns* (June 2025); *see also* Shreya Tewari & Sidharth Deb, *India's CCPA Guidelines on Dark Patterns: Welcome Signal, but Law Is Still Soft*, IAPP (Feb. 17, 2026), https://iapp.org/news/a/india-s-ccpa-guidelines-on-dark-patterns-welcome-signal-but-law-is-still-soft.

[25] CCPA Guidelines, *supra* note 3, ¶ 2(e); *cf.* Regulation 2022/2065, art. 25(1), 2022 O.J. (L 277) 1 (employing the broader formulation of "deceives or manipulates" or "materially distorts or impairs").

[26] Consumer Protection Act, No. 35 of 2019, § 21, INDIA CODE; *cf.* Mark Leiser & Cristiana Santos, *Dark Patterns, Enforcement, and the Emerging Digital Design Acquis*, 14 EUR. J. RISK REG. 1, 11–15 (2023) (arguing for "fairness-by-design" obligations).

[27] DPDP Act, *supra* note 4, § 6(1) (defining valid consent and requiring it to be "free, specific, informed, unconditional and unambiguous"); *id.* § 6(1) Explanation cl. (a) (free consent must be "given without her being subjected to any deceptive or manipulative practice").

[28] *Id.* § 6(2).

ISSN: 2582-6433

Yet the consent route has its own limits. First, the DPDP Act applies only to the processing of digital personal data; transactional dark patterns unconnected to personal data, such as drip-pricing checkout flows that disclose mandatory fees only at the final step, fall outside its scope.[29] Second, the Act locates the harm in the procurement of consent, not in the broader behavioural-governance effects of design. A subscription trap that does not, strictly speaking, involve a consent transaction for personal data processing but instead exploits cancellation friction falls awkwardly between the two regulatory frames. Third, the substantive standard remains transactional in orientation: the question is whether a particular consent is tainted, not whether the system of design that produced consent is itself regulatory in character.

C. The Doctrinal Gap

The two tracks together produce a structural blind spot. Architectural choices that systemically channel user behaviour but neither involve outright representational deception nor turn on a discrete consent transaction occupy a doctrinal interstice. India lacks an instrument analogous to Article 25 of the Digital Services Act, which directly addresses platform interface design as such, regardless of whether the conduct also falls under consumer or data protection law.[30] Nor does Indian competition law currently treat manipulative interface design as a competition concern, despite its evident foreclosure effects on user choice and rivalry.[31]

The constitutional backdrop deepens the gap. *Justice K.S. Puttaswamy (Retd.) v. Union of India* established informational privacy as constituent of Article 21, with consent and autonomy as core values informing data protection regulation.[32] If, however, consent itself can be architecturally produced, the constitutional safeguard becomes precarious unless the doctrinal frame extends to the architectures that produce it. The Indian regime presently regulates the moment of consent but not the conditions under which consent becomes possible.

IV. COMPARATIVE CURRENTS: DSA, FTC, AND CALIFORNIA

The comparative landscape is instructive but uneven. Article 25 of the Digital Services Act provides the most direct doctrinal model. Providers of online platforms must not ‘design,

[29] *Id.* § 3 (scope limited to processing of digital personal data); *id.* § 2(t) (definition of “personal data”).
[30] Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC, art. 25, 2022 O.J. (L 277) 1 [hereinafter DSA].
[31] Competition Act, No. 12 of 2003, §§ 3–4, INDIA CODE; *cf.* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION 100–08 (2016); Inge Graef, *Differentiated Treatment in Platform-to-Business Relations*, 56 COMMON MKT. L. REV. 1373, 1380–84 (2019).
[32] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 297–301 (Chandrachud, J.); *id.* ¶ 638 (Kaul, J.) (recognising informational self-determination as constituent of privacy).

ISSN: 2582-6433

organise or operate their online interfaces in a way that deceives or manipulates' recipients, or 'otherwise materially distorts or impairs' their ability to 'make free and informed decisions'.[33] The provision is striking for what it does not require. There is no need to identify a misrepresentation, locate a specific consent transaction, or quantify monetary loss. The wrongful act is the design itself, assessed against its distortive or impairing effect on autonomous decision-making.[34] The Commission's enforcement powers, including fines of up to six percent of global turnover, give the prohibition real bite.[35]

Article 25 nonetheless carries doctrinal scars. Its lex specialis carve-out in paragraph 2, which disapplies the prohibition to practices 'covered by' the Unfair Commercial Practices Directive or the GDPR, has drawn criticism for fragmenting enforcement and producing parallel regimes for substantively similar conduct.[36] The forthcoming Digital Fairness Act, slated for proposal in mid-2026, is intended to remedy this fragmentation through a horizontal fairness-by-design principle, an evolutionary direction Indian law would do well to study.[37]

The American regime, by contrast, operates through layered statutory and case-law accretion. The FTC Act's section 5 prohibition of unfair or deceptive acts or practices, supplemented by the Restore Online Shoppers' Confidence Act and the FTC's 2024 Negative Option Rule, supplied the doctrinal route in the Amazon Prime litigation, which yielded a USD 2.5 billion judgment in September 2025.[38] Earlier, in 2023, Epic Games agreed to a USD 245 million settlement over Fortnite's use of dark patterns directed at minors.[39] The FTC's 2022 staff report *Bringing Dark Patterns to Light* articulated the architectural concern explicitly, framing design as the locus of unfairness in subscription and consent flows.[40] The American approach remains, however, fundamentally transactional. It asks whether a particular design tricks particular consumers, rather than addressing design as governance.

---

[33] DSA, *supra* note 30, art. 25(1).
[34] *Id.* recital 67; Leiser & Santos, *supra* note 26, at 11–15; *see also* EUR. COMM'N, BEHAVIOURAL STUDY ON UNFAIR COMMERCIAL PRACTICES IN THE DIGITAL ENVIRONMENT: DARK PATTERNS AND MANIPULATIVE PERSONALISATION 21–27 (May 2022).
[35] DSA, *supra* note 30, art. 74 (fines of up to 6% of global annual turnover for material breaches).
[36] *Id.* art. 25(2) (carve-out for practices covered by Unfair Commercial Practices Directive or GDPR); *see* Inge Graef, *A Two-Pronged Approach to Regulating Manipulative Practices Online*, 28 EUR. L.J. 1, 12–15 (2022).
[37] EUR. COMM'N, *A New Consumer Agenda: Strengthening Consumer Resilience for Sustainable Recovery*, COM (2020) 696 final (Nov. 13, 2020); EUR. COMM'N, *Public Consultation on the Digital Fairness Fitness Check* (2024); legislative proposal expected mid-2026.
[38] *FTC v. Amazon.com, Inc.*, No. 2:23-cv-00932 (W.D. Wash. 2023); Stipulated Order, *supra* note 2; Negative Option Rule, 16 C.F.R. pt. 425 (as amended 2024) (codifying the "as easy to cancel as to subscribe" principle).
[39] *United States v. Epic Games, Inc.*, No. 5:22-cv-00518-BO (E.D.N.C. Mar. 14, 2023) (stipulated order requiring USD 245 million in consumer refunds for the use of dark patterns to facilitate unauthorised in-game purchases by minors); Press Release, FED. TRADE COMM'N, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars Over FTC Allegations* (Dec. 19, 2022).
[40] FED. TRADE COMM'N, *supra* note 5, at 8–12.

ISSN: 2582-6433

The California regime, embedded in the California Consumer Privacy Act and the California Privacy Rights Act, is the most explicitly architectural of the US frameworks. Its regulations define dark patterns as user interfaces that have the 'substantial effect of subverting or impairing user autonomy, decision-making or choice', and treat consent procured through such interfaces as legally void.[41] In September 2024, the California Privacy Protection Agency issued an enforcement advisory targeting choice architectures designed to discourage opt-out, signalling a willingness to regulate design rather than only outcomes.[42]

What these comparative regimes share is a willingness to treat design itself as the regulated object. What they diverge on is whether the inquiry remains transactional or genuinely architectural. The DSA represents the strongest move toward an architectural standard, but its lex specialis exception leaves uncertain what is captured in practice. The FTC remains essentially transactional. California has the doctrinal vocabulary but limited enforcement scale. India's task, accordingly, is not to replicate any single model but to draw from the architectural impulse of the DSA the recognition that design itself is the wrong, while grounding it in a workable Indian doctrinal anchor.

V. TOWARD AN ARCHITECTURE-BASED UNFAIRNESS TEST

If the foregoing diagnosis is correct, India's regulatory response requires a third doctrinal track, distinct from the CCPA's deception-oriented Guidelines and the DPDP Act's consent-oriented provisions. The proposal here is modest in form but consequential in implication: an architecture-based unfairness test, articulated either through judicial elaboration of section 2(47) of the Consumer Protection Act or through CCPA guidance under section 18, that interrogates design as such.

The test has three elements. The first is *material influence*. A design element is presumptively suspect where it is reasonably foreseeable that it will, at population scale, channel users toward a platform-preferred outcome they would not have selected under symmetrical conditions.[43] This element draws from the DSA's material-distortion language but anchors it in foreseeability, a familiar doctrinal device that avoids requiring proof of specific user deception. It also draws on the comparative-counterfactual reasoning the FTC has begun

[41] CAL. CIV. CODE § 1798.140(l) (West Supp. 2024); 11 CAL. CODE REGS. § 7004 (2023) (requirements for symmetric consumer choice mechanisms).
[42] CAL. PRIVACY PROT. AGENCY, *Enforcement Advisory No. 2024-01: Applying CCPA Requirements to Choice Architectures That Subvert or Impair Consumer Decision-Making* (Sept. 4, 2024).
[43] *Cf.* Susser, Roessler & Nissenbaum, *supra* note 7, at 24–26 (proposing foreseeability as the operative criterion for online manipulation).

ISSN: 2582-6433

to deploy in subscription-flow cases.[44] The proof required is statistical rather than individual: evidence that the design measurably alters aggregate user behaviour relative to a neutral baseline.

The second element is *asymmetry of cost*. Where the design imposes meaningfully greater friction on the user-preferred outcome (rejecting cookies, cancelling a subscription, declining an upsell) than on the platform-preferred outcome, the asymmetry is itself probative of architectural unfairness.[45] This element captures what the FTC has termed the 'as easy to cancel as to subscribe' principle, formalised in its 2024 Negative Option Rule, and aligns with the Court of Justice of the European Union's holdings in *Planet49* and *Orange România* that consent options must be symmetrically accessible.[46]

The third element is *justification*. Drawing on the structure of constitutional proportionality, the platform should be entitled to demonstrate that the contested design serves a legitimate, non-manipulative purpose proportionate to its behavioural effect.[47] Genuine usability constraints, fraud prevention, or accessibility considerations may justify asymmetries that would otherwise be presumptively unfair. The justification stage performs important doctrinal work. It distinguishes manipulation from legitimate persuasion without collapsing the inquiry into intent.

The doctrinal payoffs of this approach are considerable. By focusing on foreseeable material influence rather than deception, the test captures designs that operate through friction and salience rather than through representation. By formalising asymmetry of cost, it gives doctrinal content to the otherwise impressionistic notion of subverting autonomy. By incorporating justification, it preserves space for legitimate design while shifting the persuasive burden onto the platform once foreseeable distortion is shown. The test would slot naturally into the CCPA's existing unfair-trade-practice jurisdiction and, by feeding into the meaning of 'deceptive or manipulative practice' under section 6(1) of the DPDP Act, could bridge the current two-track gap.

Three objections deserve brief response. The first is overinclusion: the test may capture

[44] *FTC v. Amazon.com, Inc.*, No. 2:23-cv-00932, ¶¶ 102–110 (W.D. Wash. filed June 21, 2023) (employing counterfactual reasoning to identify the distortive effect of design).
[45] Luguri & Strahilevitz, *supra* note 5, at 70–75 (asymmetric friction as predictive of behavioural distortion).
[46] Negative Option Rule, 16 C.F.R. pt. 425 (2024); Case C-673/17, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände*, ECLI:EU:C:2019:801, ¶ 65 (Oct. 1, 2019) (pre-ticked consent boxes do not constitute valid consent); Case C-61/19, *Orange România SA v. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal*, ECLI:EU:C:2020:901, ¶ 41 (Nov. 11, 2020) (consent must not be "unduly affected" by the friction imposed on refusal).
[47] *Cf. Modern Dental Coll. & Rsch. Ctr. v. State of M.P.*, (2016) 7 SCC 353, ¶ 60 (articulating the four-prong proportionality test); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1, ¶¶ 310–315 (applying proportionality in the data protection context).

ISSN: 2582-6433

legitimate persuasion such as targeted recommendations. The justification element addresses this. Not all influence is illegitimate, only that which fails proportionality. The second concerns evidentiary asymmetry. The behavioural data on which the test relies sits primarily with platforms, raising risks of self-serving disclosure. Properly designed, the test would impose a regulatory disclosure duty: platforms whose interfaces produce measurable behavioural channelling should be obliged, on regulatory request, to surface A/B testing and conversion-funnel data, analogous to the audit obligations under DSA Article 37 for very large platforms.[48] The third is the charge of judicial overreach into design choices. The response is that the inquiry is no more intrusive than the established unfair-contract-term doctrine, which routinely interrogates the architecture of bargaining without dictating its outcome.[49]

VI. CONCLUSION

The case made here is not that consumer protection and data protection law have failed but that they have, in their handling of dark patterns, mistaken the part for the whole. The transactional and consent-based frames apprehend individual harms while leaving the structural mechanism, the use of interface architecture as an instrument of decentralised behavioural governance, doctrinally invisible. India's two-track regime is a thoughtful first step that fails to take the second.

The architecture-based unfairness test proposed here is offered not as a closed doctrinal formula but as a starting point. Its constitutive elements, foreseeable material influence, asymmetry of cost, and justification, are familiar materials drawn from existing law. The novelty lies in their combination and in their object: design itself. As Indian platforms scale and Indian users become an increasingly significant share of global digital commerce, the question of who governs the digital choice environment, and through what doctrinal accountability, will move from peripheral to central. The argument of this article is that the question is not finally one of consumer fraud or even of consent, but of regulatory power exercised through architecture, and that Indian law must, accordingly, develop a doctrinal grammar adequate to the form.

[48] DSA, *supra* note 30, arts. 34, 37 (risk assessment and independent audit obligations for very large online platforms).
[49] *LIC of India v. Consumer Educ. & Rsch. Ctr.*, (1995) 5 SCC 482, ¶¶ 53–60 (judicial review of unfair contract terms in standard-form contracts); Indian Contract Act, No. 9 of 1872, § 23, INDIA CODE.