VOLUME 7 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CONSUMER LAW AND THE INVISIBLE ARCHITECTURE OF PERSUASION

- Kerryn Pahuja[1]

Abstract

The paper examines 'dark patterns' in digital interfaces through the lens of Indian consumer law rather than competition law. It re-describes dark patterns as three underlying mechanisms of manufactured consent, draws on behavioural economics to explain their effectiveness, and proposes a five-factor 'Vitiated Consent Test' for identifying when persuasive design becomes an actionable unfair trade practice or misleading advertisement under the Consumer Protection Act, 2019 and the CCPA Guidelines, 2023. The test is applied to recent CCPA enforcement action against IndiGo and BookMyShow, and the paper closes with a comparative analysis against the United States and European Union frameworks, along with proposals for reform.

Keywords: Dark Patterns; Consumer Protection Act, 2019; Unfair Trade Practice; Misleading Advertisement; Central Consumer Protection Authority (CCPA); Manufactured Consent; Behavioural Economics; Vitiated Consent Test; Digital Markets; Comparative Consumer Law.

I. Introduction

A user in India who wants to unsubscribe from a food-delivery or OTT platform will typically encounter a screen that does not simply ask "cancel?". It asks why they are leaving, offers a discount to stay, restates what they will lose, and only then, several taps later, lets them go. The same platform's sign-up flow asks for none of this. This asymmetry is not a design accident; it is a deliberate allocation of friction, placed precisely where the platform's

---

[1] Student at Delhi Metropolitan Education, Noida (GGSIPU)

revenue is at stake. Interface designers and regulators call this class of techniques 'dark patterns': a user interface deliberately designed to mislead or trick a user into an action they did not originally intend, by subverting or impairing their autonomy, decision-making or choice.[2]

Indian commentary on this problem has repeatedly reached for competition law, arguing that a dominant platform's systematic use of dark patterns should be treated as an abuse of dominance under Section 4 of the Competition Act, 2002, since manufactured consent, deployed at scale, entrenches lock-in and forecloses rivals.[3] This essay resists that pull. Competition law's remedies switch on only once a firm crosses the threshold of dominance or significant market power: a threshold that the great majority of platforms deploying dark patterns in India's market, from regional quick-commerce apps to mid-sized OTT services, will never cross. A user coerced into a subscription trap by a firm with a five per cent market share suffers exactly the same injury to autonomy as one coerced by a firm with fifty. Treating the harm as primarily competitive therefore leaves most of it unaddressed, and reaches the remainder only indirectly, as a side-effect of protecting rivals rather than protecting the user.

This essay argues that Indian consumer law already supplies a more direct and more complete answer. Dark patterns are, first and last, an interference with a consumer's ability to make an informed and autonomous choice, precisely the interest that the Consumer Protection Act, 2019 ('CPA') and the Central Consumer Protection Authority's ('CCPA') Guidelines for Prevention and Regulation of Dark Patterns, 2023 ('the Guidelines') exist to protect. Unlike competition law, this framework applies without proof of market power: any trader, of any size, who deploys a misleading advertisement, an unfair trade practice or an unfair contract term can be reached under Sections 2(28), 2(47) and 2(46) of the CPA respectively. The doctrinal task is therefore not to import a foreign vocabulary of dominance and foreclosure, but to sharpen the tools consumer law already has, and to convert the CCPA's current practice of advisories and case-by-case notices into a durable, systemic enforcement architecture.

[2]Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, cl 3(a) (Ministry of Consumer Affairs, Food and Public Distribution, Government of India, 30 November 2023) accessed 28 April 2026.

[3]See, eg, Ritisha Sinha and Arnav Srivastava, 'Shady Play: How Tech Giants Use Dark Patterns to Distort Competition' (NLIU Law Review Blog, 25 July 2024) accessed 28 April 2026.

The essay makes this argument in six moves. It first re-describes dark patterns not as a list of thirteen named tricks but as three underlying mechanisms of manufactured consent. It then explains, through behavioural economics, why these mechanisms are effective against ordinary users. It develops the chain by which individually unremarkable instances of manipulation become a systemic trade practice, and proposes a five-factor Vitiated Consent Test (‘VCT’) for identifying when persuasive design crosses into an actionable unfair trade practice or misleading advertisement. It applies that test to enforcement action the CCPA has already taken, before situating India’s position comparatively against the United States and the European Union and closing with proposals for reform.

II. Manufactured Consent: The Mechanisms Behind the Label

The Guidelines catalogue thirteen named practices: false urgency, basket sneaking, confirm shaming, subscription traps, drip pricing, disguised advertising and others.[4] Rather than treat these as a taxonomy to be memorised, it is more useful, particularly for assessing whether a given design amounts to an unfair trade practice, to ask what each practice actually does to a user’s decision. On inspection, nearly every named pattern reduces to one of three underlying mechanisms.

The first is temporal manipulation: compressing the time available for a decision so that deliberation gives way to reflex. Countdown timers, ‘only one left’ messages and limited-time discounts that reappear after they expire all operate this way, exploiting loss aversion, the tendency to weigh a possible loss more heavily than an equivalent gain.[5] The second is informational manipulation: withholding or deferring material facts, such as a bundled insurance add-on, a hidden convenience fee, or a defaulted donation, until the point at which the user is least likely to reconsider. A LocalCircles survey found that roughly sixty-nine per cent of Indian platforms surveyed disclosed additional charges only at the final stage of checkout, well after a user has invested time selecting an item and entering personal details.[6] The third is asymmetric friction: making the platform’s preferred outcome effortless and the

[4]Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Annexure 1 (Ministry of Consumer Affairs, Food and Public Distribution, Government of India, 30 November 2023) accessed 28 April 2026.
[5]Stuti Mazumdar and Symran Bhue, ‘Responsible Design Part 4 of 14: False Urgency’ (Think Design Blog, April 2022) accessed 28 April 2026.
[6]LocalCircles, cited in Dipak Rao, ‘Dark Patterns in India’ (Singhania & Partners Blog, 18 April 2024) accessed 28 April 2026.

alternative laborious: one-click sign-up against a multi-step, survey-gated cancellation, of the kind documented across a substantial share of subscription services in a 2024 international enforcement sweep.[7]

These three mechanisms frequently operate together rather than in isolation. A subscription cancellation flow, for instance, typically combines asymmetric friction (multiple screens) with emotionally coercive language of the kind that turns a neutral decline into a confession, such as the phrase 'No thanks, I don't want to improve my skills', a technique popularised by, among others, the redesigned mascot used by language-learning application Duolingo to register disappointment when a user lapses.[8] What unites these mechanisms is not their surface form but their function: each substitutes engineered behaviour for informed choice, while preserving the outward appearance that the user consented.

This reframing matters for the argument that follows. A single named 'pattern' from the Guidelines' list can look trivial in isolation: a pre-ticked box, a countdown clock. Once the underlying mechanism is identified, however, the same design recurs across checkout flows, subscription flows, consent screens and cancellation screens, because it exploits the same cognitive vulnerability each time. That repetition, rather than any single instance, is what the Vitiated Consent Test developed in Part V is built to capture.

III. Why Manufactured Consent Works

Classical economic models assume a rational, fully informed decision-maker who compares available alternatives before choosing. Behavioural economics rejects this as a description of actual behaviour: consumers exhibit bounded rationality, operate under finite attention, and rely on heuristics rather than exhaustive comparison.[9] Digital platforms do not merely accommodate these limitations; they are architected around them. Default settings exploit status-quo bias, the tendency to stick with whatever requires no action. Manufactured scarcity exploits loss aversion. Multi-step cancellation exploits present bias, the tendency to discount future costs (the effort of leaving) against immediate convenience (staying enrolled).

---

[7]International Consumer Protection and Enforcement Network, ICPEN Dark Patterns in Subscription Services Sweep: Public Report (2 July 2024) accessed 28 April 2026.
[8]Stuti Mazumdar and Symran Bhue, 'Responsible Design Part 3 of 14: Confirm Shaming or Guilt Shaming' (Think Design Blog, April 2022) accessed 28 April 2026.
[9]Cezara Georgiana Radu, Edi Cristian Dumitra and Răzvan-George Cotescu, 'Behavioral Economics in the Era of Digital Subscriptions: Choice or Manipulation' (2024) 4(2) Journal of Academic Opinion accessed 28 April 2026.

This matters for consumer law specifically because the CPA's conception of a consumer's rights is not purely formal. Section 2(9) of the Act recognises, among others, the right to be informed of the quality, quantity and price of goods and services, and the right to be protected against unfair trade practices; a signature obtained through manufactured urgency or a concealed fee is not the exercise of those rights but their circumvention. Manufactured consent does not merely make a transaction commercially advantageous to the platform: it produces the appearance of an informed, voluntary choice while withholding the conditions that would have made such a choice genuine. That gap between the form of consent and its substance is precisely what Sections 2(28) and 2(47) of the CPA are designed to reach, because both provisions look past a transaction's formal validity to ask whether the consumer was misled, and both apply regardless of the trader's size or market position.

This has a further, self-reinforcing consequence for enforcement design. Manipulative consent flows do not only convert individual sales; they extract more personal and behavioural data than users would otherwise volunteer, refining the same interfaces that produced the original manipulation. A regulator relying on individual consumer complaints will therefore always be a step behind a practice that improves itself with every transaction it processes, which is why, as Part IV argues, the CPA's systemic and ex-ante tools, rather than case-by-case adjudication alone, are the appropriate response.

IV. From Individual Manipulation to Systemic Unfair Trade Practice

The link between manufactured consent and a distinctly systemic consumer-law harm can be stated as a five-step chain. First, manipulative interfaces impair autonomous decision-making at the level of the individual user, in a manner that already satisfies the statutory description of a misleading advertisement or unfair trade practice for that single transaction. Second, because the interface is built once and served to every user, the same manipulation recurs identically across the platform's entire user base rather than arising from the idiosyncratic conduct of an individual salesperson or store. Third, this recurrence converts what consumer law traditionally treats as a series of discrete, individually litigated grievances into a single, uniform practice embedded in the platform's default architecture. Fourth, a practice of that kind, uniform, embedded, and affecting an entire user base rather than an identifiable few, is exactly what the CCPA's class-wide and investigatory powers under Sections 18 to 21 of the CPA are designed to reach, as distinct from the individual redressal mechanism available before the District, State and National Consumer Commissions. Fifth, because enforcement against the design itself (rather than against each resulting transaction) removes the harm at its source, it protects future users who have not yet transacted with the platform at all, something individual redress can never do.

Each step in this chain is, on its own, unremarkable; regulators have always distinguished a one-off defective product from a manufacturing defect affecting an entire product line. What converts manufactured consent into a matter for systemic regulatory action rather than isolated complaint is scale of deployment, not market dominance: a platform with a modest user base that hard-codes a subscription trap into its cancellation flow causes the same kind of harm, multiplied across its users, as a much larger rival doing the same thing. This is why the CCPA's own institutional response, guidelines of general application, suo motu notices, and platform-wide self-audits, rather than a market-power threshold, is the correct enforcement model for this conduct.

V. A Test for When Persuasion Becomes an Actionable Dark Pattern

Not every instance of persuasive design is a dark pattern, and consumer law should not be weaponised against ordinary marketing, discounting or upselling. What is needed is a means of separating legitimate persuasion from conduct that warrants scrutiny as a misleading advertisement or unfair trade practice under the CPA. This essay proposes a Vitiated Consent Test ('VCT'), structured around five questions:

1. Was the interface deliberately designed to steer the consumer towards an outcome commercially advantageous to the platform, rather than to inform an independent choice?

2. Did the design exploit an identifiable cognitive bias, such as status-quo bias, loss aversion, present bias or information overload, rather than persuading through price, quality or accurate information?

3. Did the design withhold, obscure or delay information material to the consumer's decision, or make declining, comparing or exiting disproportionately more laborious than accepting, purchasing or continuing?

4. Did the consumer suffer, or was the consumer likely to suffer, actual detriment as a result, such as financial loss, an unwanted charge, an involuntary disclosure of personal data, or the loss of a benefit they would otherwise have retained?

5. Is the practice embedded in the platform's default architecture, so that it recurs systematically across its user base, rather than arising from an isolated or correctable error?

Where factors one through four are satisfied, the practice should be treated as a misleading advertisement or unfair trade practice actionable under Sections 2(28) and 2(47), open to individual redress before the Consumer Commissions or to CCPA investigation on complaint. Deliberately, the test does not require proof of dominance or market power: consumer law's protections apply to any trader. Where factor five is also satisfied, the same conduct additionally warrants the CCPA's systemic tools under Sections 18 to 21, investigation, discontinuance orders, mandatory disclosure and penalty, because the harm is no longer confined to the complainant but is being reproduced against the platform's entire user base. The value of the test lies in this separation: a small trader's aggressive but honest marketing fails factors two and three; a platform's isolated, quickly-corrected design bug fails factor five; only the combination of manufactured bias, material detriment and systemic deployment triggers the CCPA's full institutional response.

VI. Applying the Test: Three Illustrations

A. IndiGo's Web Check-In Flow

In 2024, the CCPA took suo motu cognizance of IndiGo's web check-in interface, which obscured a user's ability to skip paid seat selection, effectively steering passengers toward a preferential, payable seating option, and which displayed the message 'No, I will take the risk' to users who tried to decline an add-on such as baggage insurance.[10] Applying VCT: the interface was deliberately designed to steer users toward the paid seating option (factor one); it exploited status-quo bias and the discomfort induced by loss-framed language (factor two); it obscured the free alternative and made declining feel like an admission of recklessness (factor three); users who did not notice the free option paid an avoidable charge (factor four);

[10]Central Consumer Protection Authority, order dated 19 June 2024 in the matter of IndiGo's web check-in process, discussed in 'The End of the Pre-Ticked Box? CCPA's Latest Step Towards Protecting Consumers' (AZB & Partners, 30 June 2025) accessed 6 August 2026.

and the design was served identically to IndiGo's entire booking user base rather than arising from an isolated error (factor five). The CCPA's order accordingly did not stop at compensating individual complainants; it directed IndiGo to redesign the check-in flow so that users are told, clearly and distinctly, that they may complete check-in without selecting a preferred seat, a systemic, design-level remedy of exactly the kind factor five is meant to unlock, and one that a dominance-based competition inquiry would never have reached, since IndiGo's position in India's domestic aviation market was not in issue.

B. BookMyShow's Pre-Ticked Donation

The CCPA separately issued notice to ticketing platform BookMyShow after users found that a ₹1 contribution to the 'BookASmile' charitable initiative had been added to their basket by default, without any affirmative step on their part, a practice the Guidelines classify as 'basket sneaking'.[11] Applying VCT: the pre-tick was designed to convert inattention into a donation (factor one); it exploited status-quo bias, since removing an item requires an active step most users never take (factor two); the additional charge was not meaningfully disclosed before checkout (factor three); consumers paid for something they had not chosen (factor four); and the pre-tick appeared on every transaction rather than a subset (factor five). BookMyShow subsequently added an affirmative opt-in for the contribution. The case is a useful counterpoint to IndiGo: the sums involved were trivial, which is precisely why a competition-law inquiry, concerned with market-level foreclosure, would never have reached it, while consumer law's concern with the integrity of individual consent caught it immediately.

C. WhatsApp's 2021 Privacy Policy, Reframed

In January 2021, WhatsApp updated its Terms of Service and Privacy Policy to require users to accept expanded data-sharing with other Meta group companies, on a take-it-or-leave-it basis, as a condition of continued use. This episode was ultimately pursued through competition law: the Competition Commission of India's order of 18 November 2024 held that the policy amounted to an unfair condition and a denial of market access under Section 4 of the Competition Act, attracting a penalty of ₹213.14 crore, a finding the National

[11] Press Information Bureau, Government of India, notice referenced in 'The End of the Pre-Ticked Box? CCPA's Latest Step Towards Protecting Consumers' (AZB & Partners, 30 June 2025) accessed 6 August 2026.

Company Law Appellate Tribunal substantially upheld on appeal.[12] That route took nearly four years from the policy change to a final order, and required the CCI to establish WhatsApp's dominance in the market for OTT messaging applications before it could reach the conduct at all. Applying VCT instead: the interface was designed to extract consent to data-sharing (factor one); it exploited status-quo bias and the absence of any in-app alternative (factor two); it withheld a genuine choice, since continued use of the application was made conditional on acceptance (factor three); users suffered the loss of the ability to withhold consent to a material change in how their data was used (factor four); and the terms were imposed identically on WhatsApp's entire Indian user base (factor five). Because the take-it-or-leave-it structure caused a significant change in the consumer's rights without any opportunity to negotiate, it also falls within the CPA's definition of an unfair contract. A consumer-law route via Sections 2(46) and 2(47) would not have required proof of dominance, and could in principle have reached any platform, dominant or not, that imposed comparable take-it-or-leave-it terms. The WhatsApp episode illustrates, in other words, exactly the gap this essay is concerned with: a genuine consumer-autonomy harm that consumer law was equipped to reach quickly and without a market-definition inquiry, but that Indian regulators instead routed through the slower, narrower channel of competition law.

VII. The Statutory Basis: Sections 2(28), 2(46), 2(47) and 18–21 of the Consumer Protection Act, 2019

The application above rests on three limbs of the CPA operating, often, in combination. Section 2(28) defines a 'misleading advertisement' to include any representation that falsely describes a product or service, gives a false guarantee, or deliberately conceals material information the consumer needed to make an informed decision: language broad enough to capture a checkout screen or a cancellation flow, not merely a conventional advertisement.[13] Section 2(47) defines 'unfair trade practice' to include any unfair or deceptive method adopted for promoting the sale of goods or services, including false representations as to standard or quality and the non-consensual disclosure of a consumer's personal information: the latter limb bringing consent-based data extraction squarely within the provision's reach.[14]

[12] Competition Commission of India, In re: Updated Terms of Service and Privacy Policy for WhatsApp Users, Suo Motu Case No 01 of 2021 (order dated 18 November 2024); upheld in substance in WhatsApp LLC v Competition Commission of India, Competition Appeal (AT) No 01 of 2025 (NCLAT, 4 November 2025).
[13] Consumer Protection Act 2019, s 2(28).
[14] Consumer Protection Act 2019, s 2(47).

Section 2(46) defines an 'unfair contract' as one that causes significant change in a consumer's rights through terms imposed on a take-it-or-leave-it basis, without meaningful opportunity to negotiate: the provision most directly suited to consent screens and privacy-policy updates of the WhatsApp kind.[15]

None of these provisions requires the harm to operate through price, and none requires the trader to hold any particular share of any market. Sections 18 to 21 vest the CCPA with the power to investigate on its own motion, order the discontinuance of an unfair trade practice or misleading advertisement, order modification of a contract term, and impose penalties, in addition to the individual redressal and compensation available before the District, State and National Consumer Commissions.[16] The Guidelines, issued under this statutory authority, make explicit what the CCPA's enforcement practice already confirms: a dark pattern is not a novel wrong requiring new legislation, but an application of a misleading advertisement, an unfair trade practice or an unfair contract to the medium of the interface itself.

VIII. Comparative Positions: The United States and the European Union

The United States treats dark patterns as 'unfair or deceptive' practices under Section 5 of the FTC Act, documented in the Federal Trade Commission's 2022 staff report Bringing Dark Patterns to Light.[17] Enforcement has followed in individual cases: against Adobe Inc, over concealed early-termination fees and an undisclosed 'annual paid monthly' structure,[18] and, more significantly, against Amazon.com, Inc, resulting in a $1 billion civil penalty and $1.5 billion in consumer refunds over Prime enrolment and cancellation practices.[19] The FTC also attempted, in 2024, to go further by finalising a 'Click-to-Cancel' rule that would have mandated a cancellation mechanism no more difficult than sign-up; the Eighth Circuit vacated the rule in its entirety in July 2025 on procedural grounds, leaving Section 5 of the FTC Act and the Restore Online Shoppers' Confidence Act as the operative federal tools.[20]

[15]Consumer Protection Act 2019, s 2(46).
[16]Consumer Protection Act 2019, ss 18–21; see also 'Explainer: Offences and Penalties under the Consumer Protection Act, 2019' (Lexology, 28 August 2020) accessed 28 April 2026.
[17]Federal Trade Commission, Bringing Dark Patterns to Light (FTC Staff Report, September 2022) accessed 28 April 2026.
[18]United States v Adobe Inc, Maninder Sawhney and David Wadhwani, FTC Case No 222-3055 accessed 28 April 2026.
[19]Federal Trade Commission, 'FTC Secures Historic $2.5 Billion Settlement Against Amazon' (Press Release, 25 September 2025) accessed 28 April 2026.
[20]Custom Communications, Inc v Federal Trade Commission, No 24-3137, 2025 WL 1873489 (8th Cir, 8 July 2025); see 'US FTC Click-to-Cancel Rule Struck Down' (Sidley Austin, 9 July 2025) accessed 6 August 2026.

That episode is instructive for India: it shows that a durable, statute-based unfair-and-deceptive-practices doctrine survived a change in administration and adverse litigation in a way that a freestanding procedural rule did not, an argument for anchoring dark-pattern enforcement, as India already has, in the general unfair-trade-practice and misleading-advertisement provisions of the CPA rather than in a standalone instrument vulnerable to challenge.

The European Union's core consumer-law instrument, the Unfair Commercial Practices Directive, has been extended by regulators and courts to reach deceptive interface design, while the General Data Protection Regulation independently restricts manipulative consent interfaces for data processing.[21] The Digital Services Act, a platform-regulation rather than a consumer-protection instrument as such, additionally prohibits large platforms from deploying interfaces that materially distort users' ability to make free and informed decisions, and EU authorities have opened proceedings against Meta and TikTok on this basis.[22] India's Guidelines occupy a position the EU has not quite reached: unlike the UCPD, which operates through open-textured 'unfair commercial practice' concepts developed case by case, India is, on the CCPA's own account, the first jurisdiction to have issued a dedicated, enumerated regulatory instrument naming specific dark patterns.[23] What India lacks, by contrast, is not doctrinal vocabulary but enforcement force: the Guidelines' general application has so far been backed mainly by advisories and individual notices rather than by binding, penalised obligations of the kind Section 21 already permits.

IX. Closing the Gap: Proposals for Reform

Four reforms would allow India's existing consumer-law framework to close the enforcement gap identified above, without requiring wholesale statutory reinvention.

First, the CCPA's June 2025 advisory calling on e-commerce platforms to self-audit for dark patterns within three months should be placed on a binding footing, with self-audit reports

[21]European Parliament, Dark Patterns: Deceptive Design Practices in Online Services (European Parliamentary Research Service, 2025) accessed 28 April 2026.
[22]European Commission, 'Commission Opens Formal Proceedings Against TikTok Under the Digital Services Act' (Press Release, 19 February 2024) accessed 28 April 2026.
[23]'The End of the Pre-Ticked Box? CCPA's Latest Step Towards Protecting Consumers' (AZB & Partners, 30 June 2025) accessed 6 August 2026.

filed with the Authority and independently verified, rather than left as a recommendatory advisory with no stated consequence for non-compliance.[24]

Second, the Guidelines should expressly recognise systemic deployment, factor five of the VCT, as an aggravating consideration that moves a complaint from individual redressal toward the CCPA's class-wide powers under Section 18, so that design-level remedies of the kind ordered against IndiGo become the default response to platform-wide practices rather than an exceptional one.

Third, take-it-or-leave-it consent and privacy-policy changes of the WhatsApp kind should be treated as a per se category of unfair contract under Section 2(46) where a platform holds an entrenched user base, removing the need to route such disputes through competition law's dominance inquiry at all.

Fourth, penalties under Section 21 should be calibrated to a platform's reach and revenue for systemic violations; the IndiGo and BookMyShow interventions produced design changes but no significant monetary penalty, a pattern commentators have already flagged as leaving the Guidelines' deterrent effect uncertain.[25] Fifth, because a single dark pattern routinely implicates both the CPA and the Digital Personal Data Protection Act, 2023, the CCPA and the Data Protection Board should coordinate through a joint mechanism, so that a consent screen is not left unaddressed while each regulator waits for the other to act.[26]

X. Conclusion

Dark patterns succeed because they preserve the form of consent while removing its substance. A user who taps 'accept' on a coerced privacy policy, or who abandons a cancellation flow after the fourth confirmation screen, has technically chosen, but the choice architecture was built to produce that outcome regardless of the user's underlying preference. Indian consumer law does not need to borrow competition law's vocabulary of dominance and foreclosure to name this conduct: Sections 2(28), 2(46) and 2(47) of the Consumer Protection Act, 2019, and the CCPA's own Guidelines, already describe exactly what is

[24]Central Consumer Protection Authority, Advisory dated 5 June 2025 to e-commerce platforms on self-audit for dark patterns.
[25]See 'Dark Patterns and Weak Remedies: Why the CCPA Advisory Falls Short' (Internet Freedom Foundation, 23 June 2025) accessed 6 August 2026.
[26]Department of Consumer Affairs, Government of India, 'About Us: Central Consumer Protection Authority' accessed 28 April 2026.

wrong with a manufactured ‘yes’, and they describe it in terms that apply to every trader, not only the largest.

The Vitiated Consent Test offered here is one way of turning that statutory language into a workable enforcement standard, precise enough to filter out ordinary persuasion, but attentive enough to systemic deployment to justify moving beyond individual redress to the CCPA’s design-level remedies. What Indian consumer law now needs is not new doctrine but institutional follow-through: binding audits in place of advisories, penalties scaled to reach, and a settled understanding that a dark pattern deployed against a million users is a single unfair trade practice repeated a million times, not a million separate disputes waiting for a million separate complainants. Until enforcement catches up with that understanding, digital markets will continue to reward whichever platform is most sophisticated at engineering consent, rather than whichever platform earns it.