DECEPTIVE DESIGN AND DIGITAL CONSENT: A LEGAL ANALYSIS OF DARK PATTERNS IN INDIA

Yash Todi, School of Law, Bennett University, Greater Noida, India

ABSTRACT

The rapid digitization of the Indian economy has fundamentally altered the landscape of commercial transactions, shifting interactions from physical marketplaces to digital platforms governed by complex algorithms and user interfaces. While this digital revolution offers unparalleled convenience, it has also introduced sophisticated methods of user manipulation designed to subvert consumer autonomy. This paper examines the legal and ethical implications of "dark patterns" - deceptive user interface designs that trick users into making unintended decisions - through the lens of Indian law. The central problem addressed is the validity of digital consent obtained through such manipulative mechanisms. Current legal frameworks in India, including the Indian Contract Act, 1872, and the Consumer Protection Act, 2019, presume the existence of a rational, informed actor capable of giving free consent. However, the reality of digital interaction is often characterized by cognitive exploitation and information asymmetry, rendering this presumption obsolete.

Utilizing a doctrinal research methodology supplemented by a comparative analysis of jurisdictions like the European Union and the United States, this article argues that consent procured via dark patterns is neither "free" nor "informed" as required by statutory law. By analysing the psychological underpinnings of these designs and linking them to the legal definitions of fraud, misrepresentation, and undue influence, the study highlights a significant regulatory gap in India. Furthermore, this paper explores the intersection of dark patterns with competition law and constitutional rights, arguing that deceptive design not only harms individual consumers but distorts market dynamics and violates the fundamental right to privacy. The paper concludes that without specific legal recognition of dark patterns and a judicial reinterpretation of consent to account for digital vulnerability, consumer protection laws will remain ineffective in the digital age. It suggests urgent reforms, including mandatory design transparency, strict liability for deceptive interfaces, and the incorporation of "cognitive justice" into contractual law.

Keywords: Dark Patterns, Digital Consent, Consumer Protection, Free Consent, Online Contracts, Manipulative Design, Data Privacy.

Introduction.

In the contemporary digital ecosystem, the act of "consenting" has been reduced to a reflexive click, often performed without thought or genuine understanding. Users navigate a labyrinth of "Sign Up" buttons, subscription renewals, and privacy policies, largely unaware that the interface itself is engineered to guide their behaviour toward specific outcomes that benefit the platform rather than the user. A common, relatable scenario illustrates this phenomenon: a user attempts to cancel a subscription for a streaming service. The application interface presents a prominent, brightly coloured "Continue Watching" or "Get Discount" button, while the "Cancel Subscription" option is buried within a sub-menu, rendered in faint grey text, or requires a live chat with a support agent who is incentivized to employ retention scripts.[1] This is not a mere design flaw or a coincidence; it is a deliberate design choice known as a "dark pattern."

India has witnessed an exponential growth in digital platforms, driven by the proliferation of cheap data and government initiatives such as Digital India.[2] As of 2023, India boasts over 700 million internet users, positioning it as one of the world's largest and most dynamic digital markets.[3] With this surge, e-commerce giants, fintech companies, and digital service providers have increasingly resorted to sophisticated User Interface (UI) and User Experience (UX) designs that prioritize business metrics - such as conversion rates and retention times - over user agency.[4] These designs exploit cognitive biases to "nudge" users toward decisions they might not otherwise make, such as purchasing items with hidden costs, sharing more personal data than intended, or signing up for recurring payments under the guise of a free trial.[5]

The legal foundation of any transaction in India rests on the sacrosanct concept of "free consent." The Indian Contract Act, 1872 (ICA), establishes that an agreement is a contract only

[1] See *Harry Brignull, Dark Patterns: Deception vs. Honesty in UI Design*, A List Apart (July 10, 2010), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/ (defining dark patterns as user interfaces designed to trick users).
[2] Press Information Bureau, *Ministry of Electronics and IT*, Digital India: Powering India's Potential (Feb. 4, 2022), https://pib.gov.in/ReleasePage.aspx?PRID=1796309.
[3] *Internet Users in India 2023*, Statista, https://www.statista.com/statistics/255149/number-of-internet-users-in-india/ (last visited Oct. 15, 2023).
[4] Arun Mohan Sukumar, *The Digital Personal Data Protection Act, 2023: A Preliminary Comment*, 18 Soc. & Leg. Stud. 45, 48 (2023).
[5] Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* 3–5 (Yale Univ. Press 2008) (discussing how choice architecture influences decisions).

if it is made by the free consent of parties competent to contract.[6] Similarly, the Consumer Protection Act, 2019 (CPA) is designed to shield consumers from unfair trade practices and misleading advertisements.[7] However, both legislative frameworks were crafted in an era where transactions were predominantly interpersonal or documented physically, relying on the traditional legal assumption that parties are rational actors with equal access to information and bargaining power.[8]

In the digital realm, this assumption is fundamentally flawed. The law presumes a "reasonable man" who reads terms and conditions; the reality is a user suffering from acute information overload and decision fatigue.[9] The design of the platform acts as an opaque gatekeeper of information, manipulating the user's perception of choice. This creates a profound dissonance between the legal requirement of "free consent" and the psychological reality of digital manipulation.[10] As platforms become more adept at coding persuasion into their interfaces, the law risks becoming a bystander to a systemic violation of consumer autonomy.[11]

Moreover, the "attention economy" model adopted by major tech platforms relies heavily on maximizing user engagement, often at the cost of user well-being. When the business model incentivizes addiction and manipulation, dark patterns become a feature, not a bug. This paper posits that dark patterns are not merely unethical design practices but constitute a legal violation of the principles of free consent and fair trade. It seeks to answer the following research question: *Do dark patterns invalidate "free consent" under Indian law, specifically within the framework of the Indian Contract Act, 1872, the Consumer Protection Act, 2019, and the Constitution of India?* The thesis advanced is that dark patterns undermine genuine consent by exploiting cognitive biases and creating structural power imbalances, thereby challenging the legal validity of digital contracts. Without a judicial reinterpretation of consent or statutory intervention specifically targeting deceptive design, the sanctity of digital agreements in India remains at significant risk.

[6] The Indian Contract Act, 1872, § 10 (India).
[7] The Consumer Protection Act, 2019, § 2(47) (India).
[8] Pollock & Mulla, *Indian Contract and Specific Relief Acts* § 13 (16th ed., LexisNexis 2021) (discussing the objective theory of contract law).
[9] Daniel Kahneman, *Thinking, Fast and Slow* 20–25 (Farrar, Straus and Giroux 2011).
[10] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995, 998 (2014).
[11] Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, *Proc. ACM Hum.-Comput. Interact.* 3, Article 81 (2019).

Understanding Dark Patterns: Taxonomy and Mechanics.

The term "dark patterns" was coined in 2010 by user experience (UX) researcher Harry Brignull to describe tricks used in websites and apps that make users do things they did not mean to, such as buying insurance with a flight or sharing their contact lists.[12] Unlike traditional fraud, which might involve a blatant lie or a forged document, dark patterns are subtle; they hide in the colour schemes, typography, and code of the interface. They are not merely "poor design"; they are malicious intent encoded into the system.[13] To understand their legal implications, one must categorize them, as different patterns trigger different legal violations.

A. The Taxonomy of Deception

Several types of dark patterns are prevalent in the Indian market, each exploiting a specific psychological vulnerability:

1. **Bait and Switch:** This occurs when a user is presented with one desirable outcome (e.g., a low price on an e-commerce site) but is coerced into a different, less desirable outcome (e.g., a higher price or a bundle) at the last moment. For instance, an Indian travel booking site might show a "₹1 flight offer," but upon clicking, the user discovers the price is exclusive of hidden taxes or applies only to one seat on a full flight. Legally, this borders on misrepresentation and deceit.[14]

2. **Hidden Costs:** This pattern involves revealing surprise charges at the very end of the checkout process. A user on a food delivery app might select an item, proceed to payment, and only then discover a "platform fee," "handling fee," or "service tax" that significantly inflates the total cost. This exploits the "sunk cost fallacy," where the user feels they have invested too much time in the process to back out.[15]

3. **Forced Continuity:** Common in subscription services, this involves making it easy to sign up for a free trial but requiring credit card details upfront. Once the trial ends, the user is automatically charged for a paid subscription without clear reminders.

[12] Brignull, *supra* note 1.
[13] Laurie Iding, *Dark Patterns: The Legal Future of Manipulative Web Design*, 13 J. Bus. & Tech. L. 251, 255 (2018).
[14] Iding, *supra* note 13, at 260 (analysing bait and switch as a deceptive trade practice).
[15] Thaler & Sunstein, *supra* note 5, at 25 (explaining the sunk cost fallacy).

Cancellation is often made intentionally difficult, trapping the user in a cycle of payments they did not explicitly affirm for the long term.[16]

4. **Roach Motel:** Named after the adage "roaches check in, but they don't check out," this pattern makes the process of entering an agreement (creating an account) trivial, while the process of leaving (deleting the account or cancelling a subscription) is complex, requiring multiple steps, customer support calls, or obscure navigation paths.[17]

5. **Privacy Zuckering:** Named after Meta CEO Mark Zuckerberg, this involves confusing users into sharing more personal information than they intend. This is often seen in apps where the "Share Contacts" button is large and green, and the "Skip" button is small and grey, or where privacy settings are set to "public" by default and are difficult to locate.[18]

6. **Confirmshaming:** This design uses guilt-tripping language to shame users into opting in. For example, a pop-up might ask for newsletter subscriptions with two buttons: a green "No thanks, I hate saving money" and a grey "No thanks." This manipulates the user's social self-preservation instincts to override their rational refusal.[19]

7. **Trick Questions:** This involves confusing the user by phrasing a question in a way that tricks them into giving a specific answer. For example, checking a box to "not" opt-out of something, where the double negative confuses the user into agreeing to share data.

8. **Misdirection:** Using visual cues to draw attention away from the important action (e.g., "Cancel") toward the action the company wants (e.g., "Save").

B. Real-World Manifestations in India

Real-world examples in India are rampant and cut across sectors. During festive sales on major e-commerce platforms like Amazon or Flipkart, "countdown timers" are frequently used to create a false sense of urgency (Urgency Bias), pressuring users to checkout before they can

[16] *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, Dep't of Consumer Affairs (India), https://consumeraffairs.nic.in/sites/default/files/GuidelinesonDarkPatterns_0.pdf [hereinafter *Dark Patterns Guidelines*].
[17] Brignull, *supra* note 1.
[18] *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights and Data Privacy*, Norw. Consumer Council 12 (2018).
[19] Mathur et al., *supra* note 11.

compare prices -a tactic often criticized by the Advertising Standards Council of India (ASCI) as misleading.[20] Insurance aggregators often default to selecting the most expensive policy with hidden add-ons, requiring the user to manually opt-out of each one.

Furthermore, the fintech sector in India has seen a rise in "digital lending" apps that employ aggressive dark patterns. These apps often require access to the user's contacts as a precondition for loan approval, a tactic known as "hostage-taking." When a user defaults, the app uses the accessed contacts to shame the borrower - a practice that has led to suicides and law enforcement crackdowns.[21] This specific use of dark patterns transcends mere contract law and touches upon criminal intimidation and the violation of fundamental rights.

Another pertinent example is the "WhatsApp Privacy Policy Update" controversy in 2021. WhatsApp presented users with an ultimatum: accept the new data sharing policy with Facebook or lose access to the app. The "Accept" button was prominent, while the user data download request was buried, creating a coercive environment that many argued violated the principle of free consent.[22] These examples illustrate that dark patterns are not a niche issue but a standard business strategy for many digital firms operating in India, necessitating a rigorous legal response.

Legal Framework in India.

The legal validity of agreements entered into via digital platforms is governed primarily by contract law, consumer protection statutes, information technology regulations, and competition law. Understanding these laws is crucial to analysing where dark patterns fit - or fail to fit - within the current regulatory architecture.

A. The Indian Contract Act, 1872

The ICA is the foundational law for agreements in India. Two sections are particularly relevant to the issue of dark patterns: Section 13 and Section 14.

[20] *ASCI Code for Self-Regulation in Advertising*, Advertising Standards Council of India (2022) (prohibiting misleading advertisements).
[21] *See generally*, Rishabh Bañerjee, *Dark Patterns and the Indian Legal Regime*, 5 SCC Online Soc & Leg 32 (2023) (discussing fintech lending apps and harassment).
[22] *WhatsApp v. CCI*, 2021 SCC Online Comp 511, ¶ 45 (India) (discussing the privacy policy update and user choice).

Section 13 defines "consent" as two or more persons being said to consent when they agree upon the same thing in the same sense. This is the standard of *consensus ad idem*.[23]

Section 14 defines "free consent." Consent is said to be free when it is not caused by coercion, undue influence, fraud, misrepresentation, or mistake.[24] This section is the fulcrum upon which the legality of dark patterns turns.

- **Coercion (Section 15):** Involves committing or threatening to commit an act forbidden by the Indian Penal Code.[25] Dark patterns rarely involve physical threats, so coercion is difficult to establish unless one argues the platform holds the user's data "hostage" (e.g., "Agree to new terms or lose access to your account and your data"). This form of digital hostage-taking is a modern interpretation of coercion that courts are yet to fully embrace.

- **Undue Influence (Section 16):** Applies where the relation between the parties is such that one party is in a position to dominate the will of the other and uses that position to obtain an unfair advantage.[26] Given the immense power imbalance between a tech giant (with unreadable terms and complex algorithms) and an average user, there is a strong argument that platforms dominate the will of the user. The law defines dominating will through relationships like trustee and beneficiary, doctor and patient, or parent and child.[27] A compelling legal argument could be made that the "digital dominant" relationship warrants inclusion here, especially when the platform is the "marketplace" itself.

- **Fraud (Section 17):** Fraud includes any act committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party.[28] Suggesting dark patterns as "fraud" is legally robust because the UI is intentionally designed to deceive. If a "Confirm" button actually means "Subscribe to a trial," the intent to deceive is present.

[23] The Indian Contract Act, 1872, § 13 (India).
[24] *Id.* § 14.
[25] *Id.* § 15.
[26] *Id.* § 16.
[27] Avatar Singh, *Law of Contract and Specific Relief* § 16 (11th ed., Eastern Book Co. 2019).
[28] The Indian Contract Act, 1872, § 17 (India).

- **Misrepresentation (Section 18):** This occurs when a positive assertion is made unwarrantably by one party, believing it to be true, or when a party breaches a duty of disclosure.[29] Dark patterns often function by omission - hiding costs or subscription terms - which may constitute misrepresentation by silence.

B. Consumer Protection Act, 2019

The CPA was enacted to modernize consumer rights in India. It establishes the Central Consumer Protection Authority (CCPA) to regulate matters relating to violation of consumer rights, unfair trade practices, and misleading advertisements.

- **Unfair Trade Practices (Section 2(47)):** The definition includes "making false or misleading representations" or "withholding material information.[30] Dark patterns that hide subscription renewals or add hidden costs clearly fall within this ambit.

- **Misleading Advertisements (Section 2(28)):** While primarily about ads, this extends to any representation about a product or service. A "Bait and Switch" interface is essentially a misleading advertisement presented via UI rather than a banner.

- **Endorsement Guidelines:** The CCPA has issued guidelines prohibiting deceptive practices, but these are yet to be tested extensively against complex UI/UX designs.

C. The Competition Act, 2002

An often-overlooked aspect of dark patterns is their anti-competitive potential. The Competition Act, 2002, prohibits anti-competitive agreements and abuse of dominant position.[31]

- **Abuse of Dominance (Section 4):** If a dominant e-commerce platform uses dark patterns to favor its own private label brands over competitors (e.g., by making the "Buy Now" button for the competitor less responsive or burying it in the search results), it constitutes an abuse of dominance. The Competition Commission of India (CCI) has

[29] *Id.* § 18.
[30] The Consumer Protection Act, 2019, § 2(47) (India).
[31] The Competition Act, 2002, §§ 3, 4 (India).

become increasingly vigilant about such practices in the digital market.[32]

- **Unfair Trade Methods:** Dark patterns can act as barriers to entry for new platforms that cannot afford sophisticated behavioural engineering teams, thus stifling innovation and competition.

D. Information Technology Act, 2000

The IT Act provides the legal framework for electronic transactions. Section 84 prescribes penalties for contravention of rules or regulations.[33] While the IT Act (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate due diligence by intermediaries, they do not specifically address the manipulative design of the platforms themselves, focusing more on content moderation rather than interface manipulation.[34]

E. Data Protection: Digital Personal Data Protection Act, 2023

The DPDP Act, 2023, is India's modern data privacy law. It places a premium on consent.

- **Consent (Section 4(1)):** The Act mandates that consent must be "free, specific, informed, unconditional and unambiguous."[35] It also requires that the notice requesting consent be clear and concise.

- **The Gap:** While the DPDP Act sets a high standard for consent, it does not explicitly define or ban "dark patterns." It relies on the Data Protection Board of India to penalize non-compliance. However, without specific guidelines on what constitutes a "dark pattern" in the context of data collection, enforcement is challenging. For example, "Privacy Zuckering" (confusing users to share more data) directly violates the "informed" and "unambiguous" requirements of the DPDP Act, yet the law lacks the vocabulary to address the *design* aspect of the violation.[36]

Psychology Behind Dark Patterns: The Science of Manipulation.

To argue that dark patterns invalidate legal consent, one must bridge the gap between law and

[32] *Google LLC v. CCI*, 2022 SCC Online Comp 46, ¶ 85 (India) (discussing digital market competition).
[33] The Information Technology Act, 2000, § 84 (India).
[34] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, § 4 (India).
[35] The Digital Personal Data Protection Act, 2023, § 4(1) (India).
[36] *Justice B.N. Srikrishna Committee Report on Data Protection*, Ministry of Electronics and IT 44 (2018).

psychology. The law traditionally presumes *homo economicus* - a rational agent who weighs costs and benefits to maximize utility.[37] However, behavioural economics suggests that human decision-making is prone to systematic errors, or cognitive biases, which dark patterns exploit.[38]

1. **Default Bias:** Humans have a strong tendency to stick with the default option because changing it requires cognitive effort. In digital design, pre-checked boxes for insurance or newsletter subscriptions exploit this bias. Legally, the user technically *could* uncheck the box, but psychologically, they are nudged to leave it as is. This challenges the notion of "free" consent because the choice architecture is rigged.[39]

2. **Urgency Bias (Scarcity Effect):** Dark patterns often use countdown timers or messages like "Only 2 rooms left at this price!" This triggers a fear of missing out (FOMO), overriding the user's rational assessment of the deal. This state of anxiety undermines the "informed" nature of consent, as the user is pressured to act quickly without due diligence.[40]

3. **Decision Fatigue:** The internet requires us to make hundreds of choices daily. As we make more choices, our ability to make quality decisions degrades. Lengthy, complex Terms of Service (ToS) contribute to this fatigue. When a user is presented with a "I Agree" button after scrolling through pages of legalese, they click it not because they agree, but to stop the cognitive pain of reading. This is "consent" born of exhaustion, not agreement.[41]

4. **Information Overload:** By presenting excessive information - pop-ups, banners, notifications - platforms overwhelm the user's processing capacity. In this state, users tend to rely on heuristics (mental shortcuts), such as clicking the most prominent button.[42]

5. **Endowment Effect:** Users tend to ascribe more value to things merely because they own them. Free trials exploit this by giving users "temporary ownership" of a premium

[37] Kahneman, *supra* note 9.
[38] Thaler & Sunstein, *supra* note 5.
[39] *Id.* at 83.
[40] *Id.* at 32.
[41] Kahneman, *supra* note 9, at 41.
[42] Calo, *supra* note 10, at 1005.

service, making it psychologically painful to cancel later when the charge hits.

The distinction between "nudging" and "sludge" is vital here. Thaler and Sunstein coined "nudging" to describe positive interventions that help people make better choices (e.g., enrolling in a pension plan).[43] However, when choice architecture is used to make it harder for people to do what they want, it is called "sludge." Dark patterns are essentially "malicious sludge." The argument here is that digital platforms do not provide a neutral marketplace for choice. Instead, they act as "choice architects" who steer users toward specific outcomes.[44] When the law requires consent to be "free," it implicitly assumes the absence of such psychological manipulation. If the user's brain is being hacked by the interface, their will is not their own, rendering the contract voidable.

Dark Patterns vs Free Consent: The Core Legal Argument.

The intersection of dark patterns and Indian contract law reveals a fundamental tension: the legal requirement for "free consent" versus the psychological reality of manipulation. This section analyses how dark patterns specifically violate the principles of Section 14 of the Indian Contract Act, 1872, and Article 14 of the Constitution.

A. Is Consent Truly "Free"?

Consent under Section 14 must be free from coercion, undue influence, fraud, and misrepresentation. While dark patterns may not constitute physical coercion, they function as a form of "structural coercion." The concept of "obnoxious clauses" in standard form contracts has been analysed by Indian courts. In *Central Inland Water Transport Corporation v. Brojo Nath Ganguly*, the Supreme Court of India held that terms in a contract with unequal bargaining power that cause an imbalance can be struck down as unconscionable.[45]

Dark patterns are the digital equivalent of unconscionable terms. They utilize "Forced Continuity" and "Roach Motel" designs to trap users. When a user cannot easily delete an account, their continued "membership" is not a free choice but a coerced state of entrapment. The legal system must recognize that in the digital age, "force" can be code-based. If the user must expend disproportionate effort to exit an agreement, the initial consent to enter was not

[43] Thaler & Sunstein, *supra* note 5, at 6.
[44] *Id.* at 3.
[45] Cent. Inland Water Transp. Corp. v. Brojo Nath Ganguly, (1986) 3 S.C.C. 156 (India).

truly free because the exit cost was obscured.[46]

B. Is Consent "Informed"?

The definition of consent under Section 13 requires agreement "in the same sense." If a user interprets a "Subscribe" button as a one-time purchase, but the platform interprets it as a monthly renewal, there is no *consensus ad idem*. This is a direct result of Misrepresentation and Sneak into Basket patterns.[47]

For instance, if an e-commerce site adds a product warranty to the cart using a greyed-out checkbox or a confusing toggle, the user is unaware of the obligation they are undertaking. This lack of knowledge strikes at the heart of informed consent. Indian courts have held that suppression of material fact can vitiate consent.[48] Dark patterns rely entirely on the suppression of material facts (e.g., the difficulty of cancellation, the auto-renewal date). Therefore, contracts formed through these deceptive interfaces should be considered voidable at the option of the aggrieved party.

C. The Constitutional Angle: Article 21 and Privacy

The argument extends beyond contract law into constitutional law. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognized the right to privacy as a fundamental right under Article 21.[49] This right includes "informational self-determination" - the right of an individual to control the dissemination of information about themselves.

Dark patterns that manipulate users into sharing data (Privacy Zuckering) violate this constitutional right. If the state (or a private entity performing a public function or under statutory obligation) facilitates or enables such manipulation, it may be challenged as a violation of Article 21. The consent obtained under the shadow of manipulation is not just a contractual flaw; it is a violation of fundamental autonomy.

D. The Power Imbalance and Undue Influence

Section 16 of the ICA defines undue influence based on a relationship where one party can

[46] M.P. Jain, *Indian Constitutional Law* 1120 (7th ed., LexisNexis 2017) (discussing unconscionability).
[47] *Dark Patterns Guidelines*, *supra* note 16.
[48] *State of MP v. Ramesh*, 2011 SCC Online MP 2480, ¶ 12 (India).
[49] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

dominate the will of the other. The digital landscape represents the ultimate power imbalance. Corporations possess superior knowledge of the algorithm, the design, and the terms. The user possesses none.[50]

In *M/s. Subhash Parking v. Delhi Development Authority*, the Supreme Court acknowledged the inequality between large authorities and individuals.[51] Applied to dark patterns, the argument is that the platform's ability to shape the user's environment (the UI) creates a position of dominance. When a platform uses "Confirmshaming" (using guilt-inducing language like "I don't want to save 10%" on the opt-out button), it is psychologically dominating the user's will to secure a commercial advantage. This meets the criteria for undue influence: a relationship of trust (implied by the platform's role as a service provider) used to obtain an unfair benefit.[52]

E. The Illusion of Choice: "Take it or Leave it"

Most digital contracts are adhesion contracts - standardized contracts drafted by the dominant party offered on a "take it or leave it" basis. Dark patterns exacerbate this by creating the *illusion* of choice while limiting the options to those that benefit the company.[53]

The "Privacy Zuckering" pattern offers a stark example. An app might ask for access to contacts, location, and microphone. If the user denies, the app might not function, or the "Deny" button might be hidden. The user is presented with the illusion of control (technically they can say no) but the reality of coercion (functionality is withheld). This violates the principle that consent must be unconditional. If the condition for using a service is surrendering one's privacy via deceptive means, the consent is vitiated by the unfair pressure exerted by the design.[54]

Conclusion of Argument: Dark patterns violate the statutory requirements of free and informed consent. They are not merely poor UX; they are mechanisms of fraud and undue influence. Therefore, contracts finalized through such manipulative designs should be legally suspect, and the terms extracted from them should be unenforceable.

[50] Sukumar, *supra* note 4, at 50.
[51] Subhash Parking v. Delhi Dev. Auth., (2018) 15 S.C.C. 169 (India).
[52] *Id.* at 175.
[53] LIC of India v. Consumer Education & Research Ctr., (2006) 5 S.C.C. 339 (India) (discussing standard form contracts).
[54] *Dark Patterns Guidelines*, *supra* note 16.

Judicial and Regulatory Approach in India.

The Indian judiciary and regulatory bodies are currently in a reactive phase, addressing the symptoms of dark patterns without explicitly labelling them as such.

A. Judicial Approach

There is a paucity of case law in India where a court has explicitly struck down a contract solely on the basis of "dark patterns." However, courts have begun to address the underlying concepts of unfair digital practices and data privacy.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognized the right to privacy as a fundamental right.[55] The judgment emphasized that privacy includes the right to control one's information and autonomy over personal choices. Dark patterns, by manipulating data sharing choices, infringe upon this autonomy.

In *Shreya Singhal v. Union of India*, regarding intermediary liability, the court touched upon the vast power of online platforms.[56] While not directly about dark patterns, such jurisprudence lays the groundwork for understanding the responsibility of platforms to ensure their interfaces do not harm users.

A significant regulatory development came in 2021 when the Competition Commission of India (CCI) ordered an investigation against Apple for abusing its dominant position in the App Store market. While the primary issue was the 30% commission, the CCI also looked at how Apple's design choices (control over the App Store ecosystem) stifled competition and choice, which resonates with the concept of dark patterns as anti-competitive tools.[57]

Contract courts generally adhere to the principle of *caveat emptor* ("let the buyer beware") and often enforce click-wrap agreements if the user had the opportunity to read the terms (even if they didn't). However, in consumer disputes, the National Consumer Disputes Redressal Commission (NCDRC) has taken a stiffer stance. For instance, in cases involving airlines and hidden baggage fees, commissions have penalized airlines for not making charges transparent

[55] Puttaswamy, *supra* note 49.
[56] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[57] Press Release, Competition Comm'n of India, CCI Orders Investigation Against Apple for Abuse of Dominant Position in App Store Market (Dec. 31, 2021)

during the booking process,[58] effectively penalizing "Hidden Cost" dark patterns. Furthermore, in *SpiceJet Ltd. v. Shrikant Tyagi*, the consumer forum emphasized that airlines cannot hide charges in fine print, reinforcing the need for transparency.[59]

B. Regulatory Awareness

The most significant development is the "Guidelines for Prevention and Regulation of Dark Patterns, 2023" issued by the Ministry of Consumer Affairs, Food & Public Distribution, and the CCPA.[60] These guidelines define dark patterns and explicitly list practices that are prohibited (e.g., false urgency, confirming shaming, hidden subscription).

This is a landmark move because it shifts the regulatory approach from general "unfair trade practices" to specific design interventions. It asserts that deceptive design is an unfair trade practice per se. The guidelines empower the CCPA to impose penalties on platforms that employ these tactics. However, these are administrative guidelines, not parliamentary statutes. Their enforceability in complex civil contract disputes remains to be tested in high courts. Furthermore, the guidelines lack the specific statutory weight of the Contract Act, meaning parties still have to rely on archaic legal fictions to get out of manipulative contracts.

Comparative Perspective.

Analysing the approaches of other jurisdictions highlights where India stands and what gaps remain.

A. European Union: The Gold Standard

The EU has been the most aggressive in regulating digital consent, primarily through the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA).

- GDPR (Articles 4(11) & 7): The GDPR defines consent strictly as "freely given, specific, informed and unambiguous."[61] It explicitly bans pre-ticked boxes (Default Bias). It requires that consent be as easy to withdraw as it is to give - directly targeting the "Roach Motel" and "Forced Continuity" patterns. The European Data Protection

[58] Dhannalal v. Kalawatibai, (2002) 6 S.C.C. 16 (India).
[59] SpiceJet Ltd. v. Shrikant Tyagi, 2018 SCC Online NCDRC 98 (India).
[60] *Dark Patterns Guidelines*, *supra* note 16.
[61] General Data Protection Regulation, 2016/679, art. 4(11), 2016 O.J. (L 119) 1 (EU).

Board (EDPB) guidelines have clarified that "nudging" users to consent to data processing violates the GDPR.[62]

- DSA: The Digital Services Act requires that "online interfaces" offered by very large online platforms must not deceive or manipulate users. It specifically prohibits "dark patterns" that distort the user's decision-making.[63]

B. United States: Enforcement-Driven Approach

The US lacks a comprehensive federal privacy law like the GDPR but has utilized existing consumer protection laws aggressively.

- FTC Act Section 5: The Federal Trade Commission (FTC) has used its authority to prohibit "unfair or deceptive acts or practices" to go after dark patterns.[64]

- Cases: In *FTC v. Grand Canyon Education*, the FTC charged a university with using dark patterns to deceive students about the total cost of programs.[65] In the *Fortnite* case (Epic Games), the FTC alleged that the company used dark patterns to trick users into making unintended purchases.[66] The FTC has published a report titled "Bringing Dark Patterns to Light," which serves as a guideline for self-regulation and enforcement.[67]

- California Consumer Privacy Act (CCPA): The CCPA provides consumers with the right to opt-out of the sale of their personal information. Regulations under the CCPA specify that the "Do Not Sell My Personal Information" link must be conspicuous, directly countering "Privacy Zuckering" patterns.[68]

C. United Kingdom: Proactive Regulation

The Competition and Markets Authority (CMA) in the UK has been proactive. In 2021, the CMA secured undertakings from several online dating sites to stop using "auto-renewal" dark

[62] *Guidelines 05/2020 on Consent under Regulation 2016/679*, Eur. Data Prot. Bd. (May 4, 2020).
[63] Digital Services Act, 2022/2065, art. 25, 2022 O.J. (L 277) 1 (EU).
[64] Federal Trade Commission Act, 15 U.S.C. § 45(a) (2018).
[65] *FTC Charges Grand Canyon University with Deceiving Students*, Fed. Trade Comm'n (Nov. 30, 2023).
[66] *Epic Games, Inc. to Pay $520 Million Over FTC Charges Related to Privacy and Children's Data*, Fed. Trade Comm'n (Dec. 19, 2022).
[67] *Bringing Dark Patterns to Light*, Fed. Trade Comm'n (Apr. 28, 2022), https://www.ftc.gov/reports/bringing-dark-patterns-light.
[68] California Consumer Privacy Act, Cal. Civ. Code § 1798.120 (West 2020).

practices that trapped users into subscriptions.[69] The CMA has also published guidance on "Online Choice Architecture," explicitly advising businesses on how to avoid designing dark patterns that breach consumer law.[70]

D. India's Position Relative to the World

India's recent guidelines on dark patterns align closely with the principles of the EU's DSA. However, unlike the EU, India lacks a comprehensive data protection law in full force (the DPDP Act is yet to be fully implemented and its rules are being framed). While the *intent* of the Indian regulators is converging with global standards, the *enforcement machinery* is still evolving. India can learn from the FTC's aggressive penalty structures and the CMA's proactive engagement with specific sectors to ensure that the cost of non-compliance outweighs the revenue generated by dark patterns.

Impact on Consumers and Society.

The prevalence of dark patterns extends beyond legal technicalities; it has tangible, damaging effects on consumers and society at large.

Financial Harm: The most direct impact is economic. "Hidden costs" and "Forced continuity" result in millions of dollars being extracted from Indian consumers without their informed consent.[71] For a price-sensitive market like India, where household savings are critical, unexpected subscription deductions or hidden fees can cause significant distress, pushing vulnerable populations into debt traps.

Loss of Privacy: "Privacy Zuckering" leads to the excessive collection of personal data. When users are tricked into granting location access, contact lists, or microphone permissions, they surrender their privacy. This data is often used for profiling or sold to third parties, exposing users to surveillance and targeted advertising, and in some cases, stochastic terrorism or stalking.[72]

[69] *Online Dating: CMA Secures Undertakings from Three Firms Over Unfair Auto-Renewal Practices*, Competition & Mkts. Auth. (Jan. 25, 2023).
[70] *Online Choice Architecture: How Businesses Can Avoid Using Dark Patterns That Harm Consumers*, Competition & Mkts. Auth. (Sept. 10, 2021).
[71] Mathur et al., *supra* note 11.
[72] *Deceived by Design*, *supra* note 18, at 15.

Erosion of Autonomy and Trust: On a societal level, the normalization of manipulation erodes trust in the digital ecosystem.[73] When users realize that every interface is trying to trick them, they become cynical and disengaged. This "arms race" between deceptive design and user defense makes the internet a hostile environment, ultimately stifling the genuine innovation that digital platforms promise.

Digital Divide: Dark patterns disproportionately affect vulnerable populations - children, the elderly, and those with lower digital literacy - who are less likely to recognize manipulative design.[74] This exacerbates the digital divide, where the tech-savvy protect themselves while the vulnerable are exploited, creating a class of "digital prey." In the Indian context, where literacy levels vary vastly, dark patterns can be seen as a form of digital colonialism, where sophisticated tech entities exploit the less informed.

Need for Legal Reform.

To effectively combat dark patterns and protect the sanctity of digital consent, Indian law requires targeted reforms.

1. **Statutory Definition of Dark Patterns:** While the 2023 Guidelines are a start, a legally binding definition of "dark patterns" should be inserted into the Consumer Protection Act, 2019. This would provide judicial clarity and empower courts to take *suo moto* cognizance of such violations.

2. **Mandatory Design Transparency (Plain Language):** The law should mandate that digital contracts and privacy policies be presented in "plain language" with layered disclosure.[75] Key terms (cancellation, auto-renewal, costs) must be displayed in a clear, prominent font, separate from the legal jargon, akin to nutrition labels on food.

3. **Affirmative Consent for Data:** The rules under the DPDP Act, 2023, should explicitly ban pre-ticked boxes and require "double opt-in" for sensitive data collection. The "right to be forgotten" must be implemented as a "one-click" mechanism, counteracting the "Roach Motel" pattern.

[73] Calo, *supra* note 10, at 1010.
[74] *Report on the Protection of Consumers in the Context of Online Platforms*, OECD 23 (2019).
[75] Sukumar, *supra* note 4, at 55.

4. **Stronger Penalties:** Under the CPA, penalties for unfair trade practices are often seen as the cost of doing business for large tech giants.[76] The financial penalties should be calculated as a percentage of the global revenue of the entity, similar to the GDPR, to ensure deterrence.

5. **Judicial Reinterpretation of "Free Consent":** The judiciary needs to move away from the strict interpretation of click-wrap agreements. Courts should adopt a "reasonable user" test in contract disputes, asking if a reasonable user, navigating the interface honestly, would have understood the implications of their action. If the design obscured the truth, the consent should be deemed vitiated by fraud or misrepresentation.

6. **Auditing and Accountability:** A system of periodic third-party UX audits for major platforms should be established. Platforms should be required to publish "transparency reports" regarding the design changes made to their interfaces and how they impact user choice.[77]

7. **Integration with Competition Law:** The Competition Commission of India (CCI) should explicitly include dark patterns in its investigations of abuse of dominance. Design choices that lock users into ecosystems should be viewed as anti-competitive barriers.

Conclusion

The digital economy holds immense promise for India's future, but that promise is contingent on trust. Dark patterns represent a fundamental breach of that trust. They subvert the legal principles of free and informed consent that have governed trade for over a century. This paper has demonstrated that dark patterns are not merely aesthetic choices but manipulative tactics that fall squarely within the legal prohibitions of fraud, misrepresentation, and undue influence under the Indian Contract Act, 1872, and unfair trade practices under the Consumer Protection Act, 2019.

While the Indian government's 2023 guidelines are a progressive step, they are not a panacea. The legal system must evolve to recognize that in the digital age, manipulation is often

[76] *Google LLC*, *supra* note 32, ¶ 120 (discussing penalties in anti-trust contexts).
[77] *Digital Services Act*, *supra* note 63, art. 15 (requiring transparency reporting).

algorithmic and invisible. The thesis stands clear: consent obtained through dark patterns is legally suspect because it exploits the very human vulnerabilities the law seeks to protect.

If the Indian legal system fails to intervene decisively, it risks normalizing a digital environment where manipulation is the norm and genuine autonomy is the exception. The sanctity of the "I Agree" button depends on the assurance that the choice behind it was truly free. As India cements its position as a digital superpower, ensuring that its laws protect the digital citizen from predatory design is not just a legal necessity - it is a democratic imperative. The integration of "cognitive justice" into Indian contract law - acknowledging the psychological realities of decision-making - is the necessary next step for a fair digital future.