
ILLUSORY CONSENT IN THE DIGITAL AGE: A PSYCHOLOGICAL AND LEGAL ANALYSIS OF DARK PATTERNS

Rakshit Sharma, Amity University, Noida.

Prof. Aditi Sharma, Department of Psychology, Amity University, Jharkhand.

ABSTRACT

The architecture of digital platforms has transformed consent into a routine, almost automatic act, raising serious questions about its legal and ethical validity. This paper examines the concept of “*illusory consent*” in the context of dark patterns, interface designs that subtly manipulate user behaviour to secure agreement. While contemporary legal frameworks, including contract law and data protection regimes, treat consent as a manifestation of free and informed choice, this assumption rests on a rational actor model that is increasingly challenged by psychological research. Drawing on theories of bounded rationality and cognitive bias, this paper argues that users’ decisions in digital environments are systematically shaped by design elements such as default settings, framing, and decision fatigue, thereby undermining genuine autonomy.

Through an analysis of Indian legal provisions alongside global regulatory approaches, the paper demonstrates that existing laws focus primarily on the formal expression of consent rather than the quality of the decision-making process. This creates a disconnect between legal validity and psychological reality. The paper proposes reconceptualising consent not merely as a procedural formality but as a substantive standard grounded in fairness and autonomy. It further advocates for regulatory interventions that address manipulative design practices directly, shifting the burden from users to digital platforms. By integrating insights from psychology into legal analysis, the paper seeks to reframe the discourse on consent in the digital age and highlight the urgent need for reform.

Introduction

The digital ecosystem has normalised consent as a routine and often unconscious act. From accessing websites to installing applications, users are repeatedly prompted to click “*I Agree*,” transforming what was once a meaningful legal safeguard into a mechanical interaction. This proliferation of digital consent raises a foundational question: whether such consent continues to retain its legal and ethical significance in an environment structured by persuasive design. While legal systems traditionally treat consent as an expression of free will and informed choice, the realities of digital interaction challenge this assumption in fundamental ways.¹

At the heart of this transformation lies the emergence of “*dark patterns*” interface designs that deliberately steer, coerce, or manipulate users into making decisions they might not otherwise take. These practices exploit predictable cognitive tendencies, including default bias, framing effects, and decision fatigue, to influence behaviour without overt coercion.² The result is a form of agreement that appears voluntary in legal terms but is deeply conditioned by psychological manipulation. This disconnect between formal consent and actual autonomy calls into question the continued reliance on consent as a legitimising mechanism for data processing and contractual obligations.

Contemporary legal frameworks, including the Indian Contract Act, 1872 and the Digital Personal Data Protection Act, 2023, are premised on the assumption that individuals act as rational decision-makers capable of understanding and evaluating the consequences of their choices.³ Similarly, global regimes such as the General Data Protection Regulation (GDPR) require consent to be “*freely given, specific, informed and unambiguous*.”⁴ However, these standards focus predominantly on the procedural validity of consent rather than the cognitive conditions under which such consent is obtained. In doing so, they overlook the growing body of psychological research demonstrating that human decision-making is inherently bounded and susceptible to manipulation.⁵

¹ Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent, 256 Proceedings of the Engaging Data Forum 1 (2009).

² Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, The Dark (Patterns) Side of UX Design, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (2018).

³ The Indian Contract Act, 1872, § 13–19; The Digital Personal Data Protection Act, 2023 (India).

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art. 4(11).

⁵ Daniel Kahneman, Thinking, Fast and Slow 20–45 (Penguin Books 2011).

The theory of bounded rationality, developed by Herbert Simon, challenges the classical economic assumption of fully rational actors by emphasising the limitations of human cognition. Individuals do not optimise decisions; rather, they satisfice within constraints of time, information, and cognitive capacity.⁶ Building on this, behavioural economics particularly the work of Richard Thaler illustrates how subtle changes in choice architecture can predictably influence outcomes without restricting formal freedom of choice.⁷ In digital environments, these insights are not merely theoretical; they are actively operationalised through interface design to guide user behaviour in ways that benefit platforms.

This paper argues that consent obtained in such environments is often “*illusory*” that is, formally valid but substantively compromised. The concept of illusory consent captures the gap between legal recognition and psychological reality, highlighting how users may appear to consent while lacking genuine understanding, voluntariness, or meaningful choice. By examining the intersection of law and psychology, this paper seeks to demonstrate that existing legal frameworks are ill-equipped to address the manipulative potential of digital design.

In doing so, the paper advances two core claims. First, it contends that the current consent-based model is fundamentally flawed because it relies on an outdated conception of human rationality. Second, it argues for a shift towards a more substantive approach that incorporates fairness, autonomy, and protection against manipulation as central principles. Through this analysis, the paper aims to contribute to an emerging discourse that calls for the integration of behavioural insights into legal standards governing digital interactions.

Anatomy of Dark Patterns

The term “*dark patterns*” refers to user interface designs that intentionally manipulate or coerce users into making decisions that serve the interests of the service provider rather than the user. Unlike traditional forms of deception, dark patterns operate subtly, embedding persuasive techniques within the architecture of digital interfaces. As a result, users often remain unaware that their choices are being influenced, raising serious concerns about the authenticity of their

⁶ Herbert A. Simon, A Behavioral Model of Rational Choice, 69 Quarterly Journal of Economics 99 (1955).

⁷ Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness 6–9 (Yale University Press 2008).

consent.⁸

Dark patterns are not accidental design flaws but deliberate strategies rooted in behavioural insights. Digital platforms increasingly rely on psychological principles to maximise user engagement, data extraction, and revenue generation. By structuring choices in particular ways, designers can predictably steer user behaviour without eliminating the appearance of choice.⁹ This makes dark patterns especially problematic from a legal perspective, as they preserve the formal structure of consent while undermining its substantive validity.

Scholars and regulatory bodies have identified several recurring categories of dark patterns. One of the most common is default manipulation, where pre-selected options nudge users towards a particular outcome. For instance, pre-ticked consent boxes for data sharing or automatically enabled tracking cookies exploit the human tendency to accept default settings, a phenomenon widely documented in behavioural research.¹⁰

Another prevalent category is confirmshaming, where users are subtly pressured into agreeing by framing refusal in a negative or guilt-inducing manner. Phrases such as “*No, I don’t want to save money*” or “*I prefer to miss out*” create psychological discomfort, making refusal less likely.¹¹ While such techniques do not restrict choice outright, they distort the decision-making environment in ways that compromise voluntariness.

Hidden costs and forced continuity represent another set of manipulative practices. In subscription-based services, users may be lured by free trials that automatically convert into paid plans unless actively cancelled. Cancellation processes are often intentionally complicated, requiring multiple steps or being less accessible than sign-up options.¹² This asymmetry exploits inertia and procrastination, leading users to incur financial obligations they did not actively intend to accept.

A further category involves interface interference, where visual design elements such as colour,

⁸ Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You* (2010), available at: <https://www.darkpatterns.org> (last visited Apr. 12, 2026).

⁹ Arunesh Mathur, Mihir Kshirsagar & Jonathan Mayer, *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*, Proceedings of the ACM on Human-Computer Interaction (2021).

¹⁰ Eric J. Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 Science 1338 (2003).

¹¹ Colin M. Gray, Cristiana Santos, Nataliia Bielova & Damian Clifford, *Dark Patterns and the Legal Requirements of Consent Banners*, 2021.

¹² Organisation for Economic Co-operation and Development (OECD), *Dark Commercial Patterns* (2022).

size, and placement are used to prioritise certain choices over others. For example, the “*Accept All*” button on cookie banners is often prominently displayed, while the option to reject or customise preferences is hidden or less accessible.¹³ Such design choices capitalise on users’ limited attention spans and tendency to choose the path of least resistance.

Regulatory authorities have increasingly recognised the risks posed by these practices. The Federal Trade Commission has highlighted how dark patterns can mislead consumers and undermine fair competition, particularly in digital markets.¹⁴ Similarly, the European Data Protection Board has issued guidelines emphasising that consent obtained through deceptive or manipulative design does not meet the standards of validity under data protection law.¹⁵ These developments reflect a growing acknowledgment that the design of digital interfaces is not merely a technical issue but a legal and ethical concern.

What emerges from this analysis is that dark patterns function by exploiting predictable features of human psychology rather than by restricting formal choice. They do not eliminate consent; instead, they reshape the conditions under which it is given. This makes them particularly difficult to regulate within traditional legal frameworks, which are primarily concerned with overt coercion or misrepresentation. By operating in the grey area between persuasion and manipulation, dark patterns challenge the very foundations of consent-based regulation in the digital age.

Legal Understanding of Consent

Consent occupies a central position in legal theory, functioning as a mechanism through which individuals legitimise obligations, waive rights, and authorise the use of their personal data. Across domains such as contract law, data protection, and consumer law, consent is treated as an expression of autonomy and free will. However, this legal understanding is grounded in assumptions that are increasingly difficult to sustain in digitally mediated environments.

Under the Indian Contract Act, 1872, consent is defined as the agreement of two or more persons upon the same thing in the same sense, often described through the doctrine of

¹³ Forbrukerrådet (Norwegian Consumer Council), *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights* (2018).

¹⁴ Federal Trade Commission, *Bringing Dark Patterns to Light* (2022).

¹⁵ European Data Protection Board, *Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces* (2022).

consensus ad idem.¹⁶ For consent to be considered “free,” it must not be caused by coercion, undue influence, fraud, misrepresentation, or mistake.¹⁷ The legal framework thus focuses on the absence of overt external pressures or deceptive practices. As long as parties appear to agree voluntarily and possess the capacity to contract, the law presumes the validity of their consent.

This approach reflects a classical liberal conception of the individual as a rational and self-determining actor. The law assumes that individuals are capable of understanding the terms presented to them and making informed decisions based on their preferences. In the context of digital transactions, this assumption manifests in the widespread enforcement of clickwrap and browsewrap agreements, where users are deemed to have consented simply by clicking an “I Agree” button or continuing to use a service.¹⁸ Courts have generally upheld such agreements, provided that users are given reasonable notice of the terms, regardless of whether those terms are actually read or understood.

In the realm of data protection, consent acquires an even more prominent role. The Digital Personal Data Protection Act, 2023, requires that personal data be processed only with the consent of the data principal, which must be free, specific, informed, and unambiguous.¹⁹ Similarly, the General Data Protection Regulation (GDPR) establishes consent as one of the primary legal bases for data processing, emphasising clarity, specificity, and affirmative action.²⁰ These frameworks attempt to strengthen the quality of consent by imposing procedural requirements, such as transparency obligations and the right to withdraw consent.

However, despite these safeguards, the legal conception of consent remains largely formalistic. It prioritises the presence of clear notice and affirmative action over the substantive conditions under which decisions are made. In doing so, it continues to rely on the notion that individuals engage with information rationally and deliberately. This is evident in judicial reasoning as well. In *Specht v. Netscape Communications Corp.*, the court emphasised the importance of reasonable notice and manifestation of assent, rather than the actual comprehension of terms by users.²¹

¹⁶ The Indian Contract Act, 1872, § 13.

¹⁷ *Ibid.*, § 14–19.

¹⁸ Nancy S. Kim, *Wrap Contracts: Foundations and Ramifications* 45–60 (Oxford University Press 2013).

¹⁹ The Digital Personal Data Protection Act, 2023 (India), § 6.

²⁰ Regulation (EU) 2016/679 (General Data Protection Regulation), art. 6(1)(a), art. 7.

²¹ *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002).

Indian jurisprudence similarly reflects a limited engagement with the psychological dimensions of consent. While courts have addressed issues of coercion and undue influence, these doctrines are typically confined to overt forms of pressure, such as domination of will or fiduciary relationships.²² Subtle forms of manipulation embedded within digital interfaces fall outside the traditional scope of these doctrines, leaving a significant regulatory gap.

Consumer protection law attempts to bridge this gap by addressing unfair trade practices and misleading representations. The Consumer Protection Act, 2019, prohibits practices that deceive or unfairly influence consumers' decisions.²³ However, its application to dark patterns remains limited, as such practices often operate without explicit falsehoods or misrepresentations. Instead, they manipulate choice architecture in ways that are difficult to categorise under existing legal definitions.

The cumulative effect of these frameworks is a legal system that equates consent with formal agreement while largely ignoring the cognitive processes underlying decision-making. Consent is validated based on its external expression rather than its internal authenticity. This creates a structural vulnerability in the law, allowing digital platforms to secure legally valid consent through mechanisms that systematically undermine user autonomy.

Thus, while the law continues to treat consent as a cornerstone of legitimacy, its current formulation is ill-equipped to address the complexities introduced by behavioural manipulation in digital environments. This tension between legal form and psychological reality sets the stage for a deeper critique of consent, which the subsequent sections seek to develop.

Psychological Reality of Consent

The legal conception of consent rests on an implicit assumption: that individuals engage with information in a rational, deliberate, and informed manner before making decisions. However, decades of research in cognitive psychology and behavioural economics demonstrate that this assumption is fundamentally inaccurate. Human decision-making is neither fully rational nor consistently reflective; instead, it is shaped by cognitive limitations, heuristics, and environmental cues.²⁴

²² Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly, (1986) 3 SCC 156.

²³ The Consumer Protection Act, 2019 (India), § 2(47).

²⁴ Daniel Kahneman, *Thinking, Fast and Slow* 19–30 (Penguin Books 2011).

The theory of bounded rationality, developed by Herbert Simon, provides a foundational critique of the rational actor model. Individuals operate under constraints of limited time, incomplete information, and restricted cognitive capacity. As a result, they do not optimise decisions but rather satisfice choosing options that are “*good enough*” rather than optimal.²⁵ In digital environments, where users are confronted with lengthy privacy policies, complex terms of service, and frequent consent prompts, these limitations become particularly pronounced. The expectation that users will read and comprehend such information before consenting is therefore unrealistic.

Empirical studies consistently show that users rarely read terms and conditions in any meaningful sense. The sheer volume and complexity of information create cognitive overload, leading individuals to rely on shortcuts rather than careful evaluation.²⁶ This phenomenon is further compounded by decision fatigue, where repeated exposure to choices reduces the quality of decision-making over time. Faced with multiple prompts and time constraints, users are more likely to select the quickest or easiest option often clicking “*Accept*” without scrutiny.

In addition to cognitive limitations, human decision-making is heavily influenced by systematic biases. One of the most significant in the context of digital consent is the default effect, which refers to the tendency of individuals to stick with pre-selected options. Research demonstrates that default settings can dramatically influence outcomes, even when alternative choices are easily available.²⁷ Digital platforms exploit this bias by pre-selecting options that favour data sharing or continued engagement, thereby shaping user behaviour without explicit coercion.

Another relevant bias is the framing effect, where the presentation of information influences decisions. Choices framed in positive or negative terms can lead to different outcomes, even when the underlying information remains the same.²⁸ For instance, presenting a data-sharing option as a means to “enhance your experience” may increase acceptance rates, despite potential privacy risks. Similarly, confirmshaming techniques rely on negative framing to

²⁵ Herbert A. Simon, *Models of Bounded Rationality* 198–200 (MIT Press 1982).

²⁶ Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 *I/S: A Journal of Law and Policy for the Information Society* 543 (2008).

²⁷ Eric J. Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 *Science* 1338 (2003).

²⁸ Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 *Science* 453 (1981).

discourage users from opting out.

The concept of “*nudging*,” popularised by Richard Thaler and Cass Sunstein, further illustrates how choice architecture can be used to influence behaviour. Nudges are subtle design interventions that steer individuals towards particular decisions while preserving formal freedom of choice.²⁹ While nudging can be used for beneficial purposes, such as promoting public health, its application in digital platforms often prioritises corporate interests over user welfare. In such contexts, nudges evolve into manipulative tools that exploit predictable cognitive tendencies.

Importantly, these psychological influences do not operate in isolation; they interact and reinforce one another within digital environments. A user confronted with a pre-selected default option, framed in positive terms, and presented within a cluttered interface is subject to multiple layers of influence simultaneously. The cumulative effect is a decision-making process that is heavily structured by design rather than guided by independent judgment.

What emerges from this analysis is a fundamental mismatch between legal assumptions and psychological reality. While the law treats consent as a product of informed and voluntary choice, psychology reveals that such choice is often shaped, constrained, and, at times, engineered. Users do not approach digital consent as autonomous decision-makers evaluating options on equal footing; instead, they navigate environments deliberately constructed to influence their behaviour.

This does not imply that individuals lack agency altogether, but it does suggest that their autonomy is significantly mediated by design. Consent, in this context, becomes less an expression of free will and more a predictable outcome of behavioural engineering. This insight is crucial, as it challenges the legitimacy of consent as a regulatory tool in digital environments and sets the stage for reconceptualising consent through the lens of “*illusory consent*” in the subsequent section.

Illusory Consent: Bridging Law and Psychology

The preceding analysis reveals a fundamental tension between the legal conception of consent

²⁹ Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* 6–9 (Yale University Press 2008).

and the psychological realities of decision-making. While the law recognises consent as a manifestation of free will, psychology demonstrates that such will is often shaped by structural and cognitive constraints. This disconnect necessitates a reconceptualization of consent, one that moves beyond formal agreement and engages with the conditions under which decisions are made. It is within this context that the notion of illusory consent emerges as a critical analytical framework.

Illusory consent may be understood as a form of agreement that satisfies the formal requirements of legality but fails to meet the substantive conditions of autonomy, understanding, and voluntariness. In digital environments, users routinely express consent through actions such as clicking “*I Agree*” or accepting default settings. However, as demonstrated in the previous sections, these actions are often the product of behavioural manipulation rather than independent choice. The appearance of consent masks the absence of genuine deliberation, creating a legal fiction that obscures the erosion of user autonomy.

To understand the nature of illusory consent, it is useful to disaggregate consent into three core components: understanding, voluntariness, and meaningful choice. Each of these elements is systematically undermined by the operation of dark patterns.

First, understanding is compromised by the complexity and volume of information presented to users. Privacy policies and terms of service are often lengthy, technical, and inaccessible, making it difficult for users to grasp the implications of their decisions. Even where information is technically disclosed, cognitive overload prevents meaningful comprehension.³⁰ As a result, users may formally agree to terms without possessing a clear understanding of their content or consequences.

Second, voluntariness is undermined by the subtle pressures embedded within interface design. Unlike traditional forms of coercion, which involve explicit threats or force, dark patterns rely on psychological influence to shape behaviour. Techniques such as confirmshaming, visual prioritisation, and default settings create an environment in which certain choices are easier, more attractive, or socially reinforced.³¹ Although users retain the formal ability to refuse, the

³⁰ Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* 3–12 (Princeton University Press 2014).

³¹ Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (2018).

decision-making environment is structured in a way that biases outcomes, calling into question the genuineness of their consent.

Third, meaningful choice is often absent in digital interactions. Many platforms operate on a “take-it-or-leave-it” basis, where access to services is contingent upon acceptance of standardised terms. The absence of viable alternatives limits the practical freedom of users, reducing consent to a binary and often unavoidable decision.³² In such circumstances, consent becomes a procedural formality rather than a substantive expression of preference.

The concept of illusory consent thus exposes a critical limitation in existing legal frameworks: their reliance on external indicators of agreement rather than internal conditions of decision-making. By equating consent with observable actions, the law overlooks the ways in which those actions are shaped by design. This creates a gap between legal validity and ethical legitimacy, allowing practices that undermine autonomy to persist under the guise of consent.

This gap is particularly evident in the context of data protection law. While regulations such as the GDPR emphasise the need for “freely given” and “informed” consent, their implementation often focuses on procedural compliance rather than substantive fairness.³³ As long as users are presented with notice and provided with an opportunity to agree or refuse, consent is deemed valid, even if the surrounding environment is manipulative. Similarly, under Indian law, the emphasis remains on the presence of agreement rather than the quality of the decision-making process.

Recognising consent as potentially illusory does not require abandoning it altogether as a legal concept. Rather, it calls for a shift in how consent is understood and evaluated. Instead of treating consent as a binary indicator of legitimacy, the law must engage with the conditions under which it is obtained. This involves acknowledging that autonomy is not merely a matter of formal choice but is deeply influenced by context, design, and cognitive limitations.

By integrating insights from psychology into legal analysis, the concept of illusory consent provides a more nuanced understanding of digital interactions. It highlights the need to move beyond formalism and towards a substantive evaluation of consent that accounts for

³² Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* 33–50 (Princeton University Press 2013).

³³ Regulation (EU) 2016/679 (General Data Protection Regulation), art. 7.

behavioural manipulation. In doing so, it lays the groundwork for rethinking regulatory approaches to digital platforms an issue that the following section seeks to address through proposals for legal reform.

Case Studies and Regulatory Responses

The abstract concerns surrounding dark patterns and illusory consent become more concrete when examined through real-world practices and regulatory interventions. Across digital platforms, manipulative design techniques are not isolated incidents but systemic features embedded within user interfaces. These practices demonstrate how consent is routinely engineered, raising questions about the adequacy of existing legal responses.

One of the most visible examples is the widespread use of cookie consent banners. While ostensibly designed to comply with data protection laws, many such banners are structured to nudge users toward accepting all cookies. Typically, the “*Accept All*” option is prominently displayed, often highlighted in colour and easily accessible, whereas options to reject or customise preferences are less visible or require multiple steps. This asymmetry exploits default bias and user impatience, leading to high rates of acceptance.³⁴ Although such interfaces formally provide a choice, the design significantly influences the outcome, rendering consent questionable in substance.

Another common practice involves subscription traps and forced continuity mechanisms. Digital services frequently offer free trials that automatically convert into paid subscriptions unless cancelled within a specified period. While users technically agree to these terms, cancellation processes are often deliberately complex or obscured. In some cases, users must navigate multiple pages or interact with customer support to terminate services.³⁵ This design leverages inertia and procrastination, effectively locking users into financial commitments they may not have actively intended to undertake.

Mobile applications provide further examples through permission requests and data access prompts. Users are often presented with requests for access to contacts, location, or media in contexts that do not clearly justify such permissions. These prompts are frequently bundled

³⁴ European Data Protection Board, Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces (2022).

³⁵ Organisation for Economic Co-operation and Development (OECD), Dark Commercial Patterns (2022).

with essential functionalities, creating a situation where refusal may impair the usability of the application.³⁶ As a result, users may consent not because they fully understand or agree with the data practices, but because the alternative is inconvenient or impractical.

Regulatory authorities have increasingly begun to address these practices, though with varying degrees of effectiveness. The Federal Trade Commission has taken action against companies employing deceptive interface designs, emphasising that manipulative practices can constitute unfair or deceptive acts under consumer protection law.³⁷ In its report on dark patterns, the Commission highlighted how such designs can subvert consumer choice and distort market outcomes.

Similarly, European regulators have adopted a more structured approach under the GDPR framework. The European Data Protection Board has issued detailed guidelines clarifying that consent obtained through misleading or manipulative interfaces does not satisfy the requirement of being “*freely given*.”³⁸ National data protection authorities in Europe have also imposed fines on companies for employing deceptive cookie banners and consent mechanisms, signalling a growing intolerance for such practices.

In the Indian context, regulatory engagement with dark patterns remains at a relatively nascent stage. However, recent developments indicate an increasing awareness of the issue. The Central Consumer Protection Authority (CCPA) has issued guidelines identifying and prohibiting certain dark patterns in digital commerce, including practices such as false urgency and disguised advertisements.³⁹ While these guidelines represent a significant step forward, their enforcement and integration with existing legal frameworks remain evolving challenges.

Despite these efforts, a consistent pattern emerges: regulatory responses tend to focus on specific instances of deception rather than addressing the broader structural issue of behavioural manipulation. Enforcement actions are often reactive, targeting egregious cases rather than the underlying design practices that enable illusory consent. This piecemeal

³⁶ Niva Elkin-Koren & Maayan Perel, Algorithmic Governance by Online Intermediaries, 58 Harvard International Law Journal 261 (2017).

³⁷ Federal Trade Commission, Bringing Dark Patterns to Light (2022).

³⁸ European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (2020).

³⁹ Central Consumer Protection Authority (India), Guidelines for Prevention and Regulation of Dark Patterns, 2023.

approach limits the effectiveness of regulation, as it fails to account for the cumulative and systemic nature of dark patterns.

Moreover, the global nature of digital platforms complicates enforcement. Companies operating across jurisdictions may adopt varying design practices to comply with different regulatory standards, creating inconsistencies in user protection. This highlights the need for a more harmonised and principle-based approach that transcends jurisdictional boundaries.

The case studies and regulatory responses examined in this section underscore a critical insight: while the law is beginning to recognise the problem of dark patterns, it has yet to fully grapple with their implications for consent. Existing interventions, though valuable, remain insufficient to address the deeper issue of illusory consent. This reinforces the need for a more comprehensive rethinking of legal frameworks, which the next section seeks to develop through proposals for reform.

Rethinking Consent: Towards Legal Reform

The analysis thus far demonstrates that the traditional model of consent is increasingly inadequate in addressing the realities of digital interaction. While consent remains a foundational concept in law, its current formulation rooted in formal agreement and rational choice fails to account for the behavioural dynamics that shape decision-making. The persistence of dark patterns and the resulting phenomenon of illusory consent highlight the need for a fundamental shift in regulatory thinking.

At the core of this shift lies the recognition that consent, as presently conceived, cannot serve as the primary mechanism for legitimising digital practices. When individuals are systematically influenced by interface design, the burden of ensuring fairness cannot rest solely on their ability to make informed choices. Instead, legal frameworks must move towards a fairness-based model, where the emphasis is placed on the conduct of platforms rather than the decisions of users.⁴⁰

One key reform involves the explicit prohibition of manipulative design practices. Rather than attempting to refine consent through additional disclosure requirements, regulators should directly target dark patterns as a category of unfair or deceptive conduct. This approach has

⁴⁰ Ryan Calo, *Digital Market Manipulation*, 82 *George Washington Law Review* 995 (2014).

already begun to emerge in certain jurisdictions, where guidelines identify and restrict practices such as false urgency, confirmshaming, and interface interference.⁴¹ Codifying such prohibitions within binding legislation would provide greater clarity and enforceability.

A second reform concerns the reallocation of responsibility. Under current models, users bear the burden of reading, understanding, and managing complex digital interactions. This expectation is unrealistic given the cognitive limitations discussed earlier. Legal frameworks should instead place a positive obligation on platforms to design interfaces that respect user autonomy and minimise manipulation. This could include requirements for neutral default settings, symmetrical choice architectures, and simplified consent mechanisms.⁴²

Third, there is a need to recognise psychological harm as a form of legal injury. Traditional legal doctrines often prioritise tangible harms, such as financial loss or physical injury, while overlooking the impact of sustained behavioural manipulation. However, the erosion of autonomy and the exploitation of cognitive vulnerabilities constitute harms that are no less significant. Acknowledging these harms within legal frameworks would enable more effective remedies and strengthen regulatory enforcement.

Another important dimension of reform lies in rethinking the role of consent itself. Rather than treating consent as a universal legitimising tool, it should be supplemented or in certain contexts, replaced by alternative regulatory bases such as legitimate interest, fiduciary duties, or strict limitations on data collection.⁴³ This would reduce the over-reliance on consent and address situations where meaningful choice is structurally absent.

From a broader perspective, these reforms require a shift from a procedural to a substantive understanding of autonomy. Procedural autonomy focuses on the presence of choice, whereas substantive autonomy considers the conditions under which that choice is exercised. In digital environments, where design plays a central role in shaping behaviour, autonomy cannot be meaningfully protected without addressing the architecture of choice itself.

⁴¹ Central Consumer Protection Authority (India), Guidelines for Prevention and Regulation of Dark Patterns, 2023.

⁴² Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 85–110 (Harvard University Press 2018).

⁴³ Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 *Stanford Technology Law Review* 431 (2016).

Regulatory innovation must also be complemented by interdisciplinary integration. Law cannot operate in isolation from psychology, particularly in contexts where behaviour is a central concern. Incorporating behavioural insights into legal standards would enable a more realistic and effective approach to regulation, bridging the gap between legal theory and human experience.

Finally, there is a need for proactive and systemic regulation. Instead of relying solely on ex post enforcement actions, regulators should adopt preventive measures, including design audits, compliance certifications, and ongoing monitoring of digital platforms. Given the scale and complexity of the digital ecosystem, such measures are essential to ensure that legal protections remain meaningful in practice.

Taken together, these reforms reflect a broader transformation in how consent is understood and regulated. The goal is not to abandon consent altogether, but to situate it within a framework that acknowledges its limitations and addresses the conditions under which it operates. By shifting the focus from user behaviour to platform responsibility, the law can move closer to safeguarding genuine autonomy in the digital age.

Conclusion

The evolution of digital environments has fundamentally altered the meaning and function of consent. What was once conceived as a deliberate and informed expression of individual autonomy has, in many contexts, become a routine and conditioned response shaped by interface design. This paper has argued that the widespread use of dark patterns exposes a critical flaw in the legal conception of consent: its reliance on a rational actor model that fails to reflect the realities of human decision-making.

By examining the psychological foundations of behaviour, it becomes evident that users do not engage with digital choices in the manner presumed by law. Cognitive limitations, biases, and environmental cues systematically influence decisions, often without conscious awareness. In such conditions, the act of clicking “*I Agree*” cannot be taken at face value as an indication of genuine understanding or voluntariness. Instead, it reflects a form of illusory consent a formal compliance with legal requirements that masks the erosion of meaningful autonomy.

The persistence of this illusion reveals a deeper structural issue within existing legal

frameworks. Contract law, data protection regimes, and consumer protection laws continue to validate consent based on its external manifestation, placing insufficient emphasis on the conditions under which it is obtained. As a result, practices that undermine user autonomy can operate within the boundaries of legality, creating a disconnect between legal validity and ethical legitimacy.

Addressing this challenge requires more than incremental reform. It calls for a reorientation of legal thought, one that moves beyond procedural notions of consent and embraces a substantive understanding of autonomy grounded in behavioural realities. This includes recognising the manipulative potential of design, shifting responsibility towards digital platforms, and developing regulatory frameworks that prioritise fairness over formal compliance.

The concept of illusory consent offers a lens through which this transformation can be understood. It highlights the limitations of existing approaches while providing a foundation for rethinking how consent should function in the digital age. By integrating insights from psychology into legal analysis, the law can better respond to the complexities of contemporary digital interactions.

Ultimately, the legitimacy of consent as a regulatory tool depends on its ability to reflect genuine choice. If consent continues to be shaped by invisible forces that distort decision-making, it risks becoming a symbolic gesture rather than a meaningful safeguard. The challenge, therefore, is not merely to preserve consent, but to reclaim its substance ensuring that it once again serves as a true expression of human autonomy in an increasingly engineered digital world.