CIVIL

Are You Being Misled While Shopping Online? Govt Cracks Down On E-Commerce Dark Patterns

AUTHOR Rahul Sundaram, Asav Rajan Arora

PUBLISHED 2 June 2025

In a significant move aimed at enhancing consumer protection in the digital economy, the Indian government has taken enforcement action against several leading e-commerce and technology platforms for continuing to deploy "dark patterns" deceptive user interface practices that mislead consumers. On May 28, 2025, the Ministry of Consumer Affairs issued formal notices to eleven companies, including well-known platforms citing violations of the 2023 guidelines on the prohibition of dark patterns.

This enforcement action marks the first major step in implementing the **"**Guidelines for Prevention and Regulation of Dark Patterns, 2023", issued by the Central Consumer Protection Authority (CCPA) under the Consumer Protection Act, 2019. While the guidelines have been in effect since November 30, 2023, the recent notices signal the government's growing determination to hold digital businesses accountable for manipulative design choices that undermine consumer autonomy.

Table of contents

Understanding Dark Patterns

Dark patterns are design techniques in user interfaces that are intentionally crafted to manipulate consumers into taking actions they may not have intended such as making additional purchases, subscribing to services they did not actively choose, or sharing personal data without meaningful consent. These patterns take advantage of cognitive biases and exploit gaps in user attention, often leading to unfair commercial gains at the expense of consumer welfare.

Such practices are increasingly prevalent across e-commerce platforms, travel booking websites, food delivery apps, and subscription-based services. For example, drip pricing is often used by food delivery and travel apps, where additional charges like "convenience fees" or "packaging charges" are revealed only at the final checkout stage. In ride-hailing apps like Uber or Rapido, basket sneaking occurs when optional items such as insurance or donations are pre-selected, requiring the user to manually deselect them. Similarly, subscription traps are found on OTT platforms, where cancelling a subscription is intentionally made difficult or confusing. These practices, all classified as unfair under the 2023 guidelines, mislead consumers and restrict their ability to make informed choices

The 2023 Guidelines: A Regulatory Framework

The CCPA's Guidelines for Prevention and Regulation of Dark Patterns, 2023, were notified on 30 November 2023, under Section 18 of the Consumer Protection Act, 2019. They are legally binding and apply to all platforms, websites, mobile applications, digital advertisers, sellers, and intermediaries offering goods or services in India.

The guidelines identify and define thirteen types of dark patterns, including:

1. **False urgency**: Defined as creating a false sense of urgency or scarcity (e.g., "Only 1 room left!" when that's not accurate) to pressure users into immediate action
2. **Basket sneaking**: Adding additional products, services, or charges (like insurance or tips) to the cart without clear and affirmative consent from the consumer.
3. **Confirm shaming:** Using guilt-inducing language or emotionally manipulative choices (e.g., "No, I don't care about saving money") to steer users toward a preferred action
4. **Forced action**: Forcing users to take an action unrelated to their original intent, such as having to sign up for a newsletter to complete a purchase
5. **Subscription trap:** Making it easy to subscribe but difficult to cancel, including hiding cancellation options, requiring long processes, or providing misleading steps
6. **Interface interference:** Manipulating the visual design to hide or de-emphasize alternatives (e.g., bold "Yes" buttons with faded or hard-to-see "No" buttons).

7. **Bait and switch**: Advertising something as free or available, but switching it at the last step with an alternative requiring payment or other action.
8. **Drip pricing**: Revealing additional mandatory costs late in the purchase process, such as delivery or handling fees not disclosed at the outset.
9. **Disguised advertisement**: Designing sponsored content or ads to look like genuine editorial or organic content, without clear disclosure that it's an ad.
10. **Nagging**: Constantly interrupting the user with pop-ups, overlays, or prompts, especially after they've declined an offer.
11. **Trick question:** Using confusing wording, double negatives, or misleading phrasing in options to misdirect the user (e.g., "Uncheck this box if you don't want to receive emails").
12. **SaaS-based auto-renewal without transparency:** Not informing users clearly about auto-renewal terms or renewal charges in SaaS subscriptions
13. **Rogue malware-like practices**: Using design patterns that mimic system alerts, create fear of virus/malware, or hijack user action (e.g., fake "your device is infected" pop-ups).

The guidelines also encourage consumers to report violations through grievance mechanisms, including the **National Consumer Helpline** (www.consumerhelpline.gov.in), thereby enabling both proactive and reactive enforcement. While the CCPA did not prescribe a formal compliance timeline, platforms were expected to align their interfaces with the guidelines immediately upon notification. The expectation was clear: eliminate manipulative design or face legal consequences.

The May 2025 Enforcement Action

Despite the clarity of the guidelines, several companies continued to use interface practices that fell within the definition of dark patterns. In response, the Ministry of Consumer Affairs issued notices to eleven companies in May 2025.

The government's concerns centered around persistent use of:

- Auto-added charges at checkout (drip pricing),
- Hidden or misleading unsubscribe buttons (subscription traps),
- Interface obstructions that nudged users toward accepting additional services.

These practices constituted a clear violation of the guidelines and the broader mandate of consumer protection under Indian law. The companies were warned that failure to rectify their platforms would result in legal action under the Consumer Protection Act, including penalties and potential restrictions on operations.

Implications for Consumers and Businesses

The enforcement action is a pivotal development in India's consumer rights landscape. For consumers, it promises greater transparency, fairer pricing, and more meaningful control over their online interactions. It ensures that consent, once manipulated by design, is now being protected by regulation. For businesses, however, this moment represents both a challenge and an opportunity. Platforms must undertake compliance reviews of their user interfaces, checkout flows, consent mechanisms, and communication strategies. Practices once justified by performance marketing goals now carry real legal risk.

The guidelines also present an opportunity for ethical design and responsible innovation. Companies that proactively align with consumer rights are likely to gain trust and differentiate themselves in a crowded digital marketplace.

Conclusion

The government's latest action on dark patterns marks a significant step toward safeguarding digital consumer rights in India. It is not merely about regulating design it is about ensuring that online commerce respects choice, transparency, and consent. As enforcement accelerates, both businesses and consumers must adapt to this new era of ethical digital engagement.

For more details, write to us at: contact@indialaw.in

Related Practice Areas

E-Commerce