UPDATES

Guidelines for Prevention and Regulation of Dark Patterns, 2023

26 December 2023

Partner: *Nikhil Narendran,* ***Counsel***: *Jishnu Sanyal,* ***Senior Associate***: *Krati Hashwani,* ***Associates***: *Angeline Priety Franklyn and Muskaan Wadhwa*

This update covers:

1 Background

In a move indicative of the Indian government's inclination to align its regulatory framework with the global approach to the regulation of dark patterns, the Central Consumer Protection Authority (**CCPA**) recently notified the Guidelines for Prevention and Regulation of Dark Patterns, 2023 (**Guidelines**) under the Consumer Protection Act, 2019 (**CPA**). The Guidelines modify certain dark patterns identified in the draft guidelines issued earlier for consultation and add new dark patterns that were not present in the draft guidelines (*discussed in detail below*).

The Guidelines for Prevention and Regulation of Dark Patterns, 2023 were notified on 30 November 2023. This update discusses the various dark patterns identified in the guidelines along with their implications on stakeholders, and the manner in which they are likely to be enforced.

The Guidelines are likely to be a significant step towards safeguarding consumer interests in the digital space. Notably, the Guidelines add to the guidance provided under the '*Guidelines for Online Deceptive Design Patterns in Advertising*' issued by the Advertising Standards Council of India (**ASCI**) in June 2023, which is a self-regulatory organisation in the marketing and media sector.

2 Scope and Applicability

The Guidelines define '*dark patterns*' as *deceptive patterns or practices* deployed in the user interface or user experience (**UI/UX**) interactions that are *designed to mislead or trick users* into doing an action they did not originally intend to do. As a result, they subvert or impair consumer autonomy, decision making or choice, and amount to misleading advertisements or unfair trade practice or violation of consumer rights under the CPA.

The Guidelines apply to:

a. *Platforms systemically offering goods or services in India*, including foreign platforms.

b. *Advertisers*, i.e., any person who designs, produces and publishes advertisements (by themselves or by entrusting it to others) to promote the sale of their goods, products or services. Due to this definition, advertising agencies or endorsers who provide services for such advertisements are likely to be excluded from the ambit of the Guidelines.

c. *Sellers and service providers*, i.e., any person, who in the course of business, imports, sells, distributes, or markets a product or service for commercial purposes, including manufacturers who sell products.

(collectively, **Covered Entities**)

Since the CPA's application is limited to goods and services provided to individual consumers i.e., in a business-to-consumer (**B2C**) context, the Guidelines are likely to not apply to business-to-business (**B2B**) operations.

3 Prohibition on Dark Patterns

The Guidelines prohibit all persons from engaging in any dark pattern practice mentioned in Annexure I of the Guidelines. Notably, Annexure I includes 13 types of dark patterns, and is subject to modification by the CCPA from time to time. The Guidelines also state that the dark patterns and illustrations mentioned in Annexure I are only for guidance and must not be considered as a binding opinion, i.e., it may vary on a case-to-case basis.

4 Types of Dark Patterns

The following dark patterns have been listed under Annexure I of the Guidelines:

a. ***False urgency***: Creating or implying a false sense of urgency or scarcity to mislead a user into immediately taking an action which may result in a purchase. For instance, displaying a false sense of popularity of a product or service in order to manipulate a user's decision, or falsely indicating that the quantities of a product or service are more limited than they actually are, will be considered dark patterns. Such practices are commonly seen in hotel or flight bookings.

   In case of a question on whether such prompts will qualify as dark patterns or not, Covered Entities will be required to prove that there was no *'false'* sense of urgency created, and the prompt was a correct representation.

b. ***Basket sneaking***: Including additional items such as products, services, payments to charity or donation without the user's consent, to increase the amount payable by the user. The Guidelines exclude the inclusion of free samples, complimentary services and necessary fees (*such as those required for the completion of an order or those that are explicitly disclosed to the user at the time of the purchase, such as delivery charges, gift wrapping, additional taxes, etc.*).

   For instance, inclusion of INR 1 towards donation through a pre-checked checkbox while the user is checking out for movie tickets without the user's consent is likely to be considered '*basket sneaking*'. However, imposing additional taxes or a delivery fee that is adequately disclosed to the user is unlikely to be considered as a dark pattern.

c. ***Confirm shaming***: Using emotionally charged design tactics to create a sense of fear, shame, ridicule or guilt in a user's mind using phrases, videos, audios or any other means, to mislead or guilt-trip a user to perform transactions for the commercial gain of the entity deploying the pattern.

For instance, an airline booking website may prompt users to purchase insurance by using phrases such as '*I will stay unsecured*', when a user does not include insurance in their cart.

d. ***Forced action***: Forcing users to purchase additional goods, or subscribe to unrelated services, or share their personal information to buy the product or service they originally wanted.

   For instance, a health and wellness website forcing users to subscribe to their monthly newsletter in order to purchase their products.

e. ***Subscription trap***: Indirectly forcing users to retain their subscription through various means, such as (i) making the cancellation of a subscription an impossible or complex process, (ii) hiding the cancellation option, (iii) requiring user to provide payment details or authorisation for auto debit to avail a free subscription, and (iv) making instructions for cancelling subscription confusing and cumbersome.

   While there are no specific illustrations provided for subscription trap, it can be argued that not providing the option for cancellation in a manner that is similar to that of purchasing/subscribing to a product or service, will be a subscription trap. For instance, when the option to subscribe is available online, however, cancellation requires the user to reach out to the customer support team over call.

f. ***Interface interference***: Highlighting specific information or obscuring relevant information in order to misdirect users from performing their desired action.

   For instance, where a user is required to respond to a pop-up asking if they wish to make a purchase, and *'NO'* is shaded in a light-colour, whereas *'YES'* is in bold and highlighted.

g. ***Bait and switch***: Baiting the user with a particular outcome which is deceptively switched to show an alternate outcome. Typically, this involves requiring the user to go through a purchase process, but revealing that the desired product or service is no longer available at a later stage.

   For instance, a seller may promote a quality product at a cheap price and when the user is about to pay for the product, the seller may suddenly indicate that the product is no longer available and instead offer a similar but expensive product.

h. ***Drip pricing***: Not presenting the user with comprehensive information on the price of a product upfront. This may entail (i) elements of prices being revealed surreptitiously or post confirmation of the purchase, (ii) product being advertised as free without disclosing that continuing usage would attract extra costs, or (iii) requiring that an extra product has to be purchased for the user to avail a service which was already purchased. The Guidelines clarify that marketplace e-commerce entities *would not be liable* for any price fluctuations attributable to third-party sellers or those that are beyond their control.

   One may notice this practice being employed by airline operators or platforms where a user is charged a different amount for a flight ticket as compared to what was displayed to the user at the checkout page.

i. ***Disguised advertisement***: Disguising advertisements as user generated reviews, news articles, false advertisements or other types of content to blend them with the rest of the interface, so as to trick users to click on the advertisement. Disguised advertisements include advertisements considered misleading, which are also subject to the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 issued by the CCPA. Notably, the Guidelines clarify that in case of content posted on a platform, *the responsibility of disclosing that it is an advertisement vests on the seller/advertiser* and not the platform.

For instance, publishing a paid advertisement for a skin care product as user generated content without sufficient disclosures may be considered a dark pattern.

j. *Nagging*: Disrupting or annoying users without their permission through repetitive and persistent requests, information, options or notifications, in order to effectuate a transaction and make commercial gains.

   For instance, platforms sending their users repeated notifications for downloading their mobile application.

k. *Trick question*: Deliberately using vague or confusing language to misdirect users from taking desired actions or leading users to take specific actions. These typically use confusing wording or double negatives to trick the user.

   For instance, websites displaying a pop-up asking if the user wants to cancel a subscription, and presenting options such as to *'continue'* or to *'cancel'*. A user in a hurry may select the continue option leading to an outcome not intended by the user.

l. *SaaS Billing*: Covertly billing users on a recurrent basis in a software as a service (**SaaS**) business model without any notifications.

   For instance, if a free trial is converted to a paid one without any notification or intimation to the user, it may be considered a dark pattern.

m. *Rogue malware*: Misleading users into believing there is virus on their systems, in order to convince them to pay for a fake malware removal tool which instead installs malware in their systems.

   For instance, pop-up notifications prompting user to install an anti-virus but instead being linked to the download of malware.

5 Contraventions

The provisions of CPA will apply to any violations of the Guidelines, and in such cases, Covered Entities may be required to comply with relevant sanctions and directions by the authorities. Non-compliance with such directions may result in fines or imprisonment in the following manner:

a. *Through consumer complaints*: Covered Entities engaging in identified dark patterns may be held liable, by the relevant District Commission, to pay compensation for any loss or injury suffered by the consumer. Additionally, Covered Entities may be required to discontinue the unfair trade practice in question, which may have reputational risks for businesses.

b. *Enforcement by the CCPA*: Under the CPA, the CCPA has the power to investigate complaints relating to violation of consumer rights, unfair trade practices or misleading advertisements. Such investigation can be initiated in three ways: (i) on the CCPA's own motion; (ii) upon receiving a complaint; (iii) upon receiving a reference from the government. The CCPA, upon identifying a violation of consumer rights, unfair trade practices or false/misleading advertisement, may order the discontinuance of such practices.

   Failure to comply with such an order of the CCPA is punishable with imprisonment for a term which may extend to six months or a fine of up to INR 20 lakhs (~USD 24 million) or both. Additionally, causing false or misleading advertisements to be made which are prejudicial to the interests of consumers is subject to criminal liability in the nature of imprisonment up to two years in addition to a fine up to INR 10 lakhs

(~USD 12 million) for the first contravention; and imprisonment up to five years and fine up to INR 50 lakhs (~USD 60 million) for subsequent contraventions.

6 Conclusion

The Guidelines will have a significant impact on Covered Entities, who will now need to reconfigure their user screens and interfaces to ensure they are not engaging in dark patterns. This may even require a substantial overhaul of the existing journeys on websites and mobile applications. That said, the Guidelines come at a time when various businesses are revamping their models to be in compliance with the Digital Personal Data Protection Act, 2023, allowing the opportunity to re-consider their user interactions in light of these laws.