

NOTES AND COMMENTS

RISK OF DARK PATTERNS IN E-COMMERCE: PREVENTION AND REGULATION IN DIGITAL INDIA

Abstract

The development of e-commerce has raised serious concerns about the safety and security of users over the internet and e-commerce platforms. Rapid technological developments make it easier for these platforms to deceive consumers and this in turn is leading to large number of new legislations to protect the users online. On November 30, 2023 Consumer Protection Authority has issued Guidelines for Prevention and Regulation of dark patterns. The rampant increase in e-commerce over the past few years has made such kind of legislations inevitable. In very simple terms dark patterns are practices that are designed to trick users and to make them do something which they otherwise would not have done. These guidelines though a welcome step forwards towards secure Digital Bharat, but has been a matter of deliberation due to the ever evolving nature of internet. This paper is an attempt to critically analyse these guidelines in the light of EU and California Legal Regime on the subject.

I Introduction

HUMANS ARE living in a digital era. With just one click on phone or laptops, one cannot only connect to the world but also purchase anything. From buying groceries to gold, from booking tickets to planning stay everything can be done *via* internet. Technology has made life so easy that shopping or buying something does not require a visit to market or nearby shops but it requires just a phone with an internet connection making all of us the consumers of digital market places. Internet, which was initially developed as a medium for linking and transmitting information among scientists and researchers,¹ has today taken the shape of a commercial marketplace. Talking specifically about India, it has over 800 million internet users and is the second largest internet market in the world with 125.94 lakh Cr UPI transactions in year 2022. The growth of e commerce has been seen equally on both private selling platforms and online government market places like GEM.² The rise in the number of these online selling market places is increasing the faith of consumers over such platforms.

E-commerce platforms generally choose a very consumer friendly interface on their websites/apps and try to make the entire shopping process as simple and easy as

1 US Department of Commerce, Consumer Bulletin, *Electronic Commerce and the Consumer*, available at :<https://library.unt.edu/gpo/oca/cb12.htm>, (last visited on August 30, 2026).

2 Invest India, *Fatest Growing E Commerce Market in the World*, available at, <https://www.investindia.gov.in/sector/retail-e-commerce/ecommerce#:~:text=With%20over%20800%20Mn%20users,two%20cities%20and%20smaller%20towns> (last visited on Aug. 20, 2025).

possible. The details relating to the products are mentioned comprehensively. Moreover, consumers can also get an idea of the similar products available worldwide on these platforms and their advantages over the one they are planning to purchase. Also, it is very easy to compare the products online not only in terms of their features but also prices and post purchase services, which is add on for the consumers. Coupled with the convenience of getting your products delivered at home without stepping out has made commercial activities online a preferred mode for shopping these days.³ The dependence on e commerce for purchase of services and goods have led to numerous issues concerning the safety and security of consumers online. One of the issues that has been an area of contention since long is related to “Intermediaries”. Unlike shopkeepers who sell their own goods and take responsibility for most of their products, the online selling platforms only act as intermediaries. Meaning thereby these platforms only provide a space for the sellers to sell their products. As a result of this situation in case anything wrong happens with any user, they can safely move out of the situation stating that they are merely intermediaries and the consumers are left remediless. In most of the cases the consumers are unaware about the concept and importance of sellers on e-commerce platforms. However the concept of intermediaries has been a part of legal literature since long. In India, the concept, rights, obligations and safe harbors related intermediaries are provided under the Information Technology Act of 2000. This paper though does not delve into the concept of intermediaries but focus on a newer concept which is referred to as dark patterns. There is not much literature on the concept of dark patterns in India and for the first time a set of guidelines were issued for their prevention in 2023.

II What are dark patterns?

With the rampant increase in the commercial activities online, unfair trade practices are also increasing at a very fast pace in the digital environment. These practices in very simple terms refers to unethical, fraudulent and deceptive practices that are used to obtain business. A large number of activities can be dealt with under this term like false advertising, similar trade dress, horizontal or vertical restraints *etc.* Section 2 (47) of the Consumer Protection Act, 2019 defines the term Unfair Trade practices to mean “a trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice”.⁴ This definition is followed by many examples which includes representations made by way of electronic records but does not clearly specify whether it will be applicable on digital platforms as well.

3 Cream, *Designing User Friendly Interface for E Commerce websites*, available at <https://sennalabs.com/blog/designing-user-friendly-interfaces-for-e-commerce-websites#:~:text=Clear%20Navigation,checkout%2C%20and%20customer%20service%20sections> (last visited on Aug. 30, 2026).

4 Consumer Protection Act, 2019, S. 2(47).

Section 94 of the Consumer Protection Act, 2019 authorise the central government to take such measures as may be necessary to prevent unfair trade practices in e-commerce, direct selling to protect the rights of the consumers. With the growing number of e-commerce platforms and use of similar platforms by direct selling entities the focus of the government on these areas have increased considerably. Further Section 18(l) of the Consumer Protection Act authorises the central Consumer Protection Authority (CCPA) “to issue necessary guidelines to prevent unfair trade practices and protect consumers’ interest.” In pursuance of the powers granted under Section 18 the Central Consumer Protection Authority issued certain guidelines to provide for the prevention and regulation of dark patterns which are notified in the Official Gazette on November 30, 2023. Para 2 (e) of these guidelines define the term Dark Patterns and states: ⁵

dark patterns shall mean any practices or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights.

The concept of “Subverting or Impairing Consumer Autonomy” is not unique to these guidelines and can be found in regulations or legislation framed to deal with similar problems in different parts of the world like the Digital Services Act of EU 2022, California Privacy Rights Act (CPRA), 2020, OECD Committee on Consumer Policy etc.⁶ Though there is no clear definition as to what all can be included under the said head but the term is considered to be broad enough to include wide variety of activities impacting consumer rights. To widen the scope an additional aspect of misleading advertisement has been added in the definition of dark patterns which is understandable keeping in mind the increasing cases of such advertisements.

The EU Artificial Intelligence Act though does not refers to “Dark Practices” but indirectly cover them under Article 5. Article 5 (1)(a) of this Act states that the following practices shall be prohibited: ⁷

the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person’s or a group of persons’

⁵ Guidelines on Prevention and Regulation of Dark Patterns, 2023, Para 2(e).

⁶ Department of Consumer Affairs, *Government of India, Using AI to spot dark patterns and help consumers protect themselves*, (2024), available at: https://unctad.org/system/files/non-official-document/ccpb_WGE_Webinar__A1_India_en.pdf (last visited on April 30, 2026).

⁷ EU Artificial Intelligence Act, 2024, Art. 5.

behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm

The provision is much wider and is capable of encompassing within its scope all deceptive or manipulative practices which has the capacity of distorting consumers behaviour. Apart from this article 5(1)(b) of this Act deals with placing in market services or use of AI that exploits the vulnerabilities of any person. Article 5(1)(ba) on the other hand puts a restriction on biometric categorisation system, that categorise people on the basis of their political opinions, philosophical beliefs *etc.* The provision is very wide and deals with every possible way by which artificial intelligence can be used to deceive people or can impact consumers. The reference to the legislations around the world, clearly highlights the fact that not only India, but the entire world has realised that it is crucial to control commercial activities taking place online in order to protect the rights of the innocent consumers. These guidelines can be said to be a welcome step forward by CCPA in this direction.

III History and development of the concept of dark patterns

Though the specific regulations to control these practices came only in 2023 in India but the government of India has taken numerous steps to control any kind of deception or misrepresentation taking place online much earlier and the world has been talking about such practices from even before. "Growth Hacking" is considered to be one of the first trends that led to the development of dark patterns. It was for the first time used by hotmail in around 1996.⁸ Though at that time neither the term growth hacking nor dark patterns was in use, yet it is considered to form the basis of the same. In very simple terms growth hacking refers to the use of cost effective digital tactics to maintain the existing user base and to increase it further. Though it is not inherently deceptive but most of the times it has been used in a manner that led to legal trouble for many platforms. Harry Brignull's is considered to have coined the term "Dark Pattern" in 2010 and has also been running a website since then to make people aware of the same.⁹ Rapid technological developments led to the rapid growth of deceptive practices over the internet. The website run by Harry Brignull's not only lists down many of such dark patterns but also gives a reference to the laws around the world that have been enacted to control such practices. If we specifically refer to

8 Arvind Naryanan, Arunesh Mathur, Marshinni Chetty and Mihir Kshirsagar, *Dark Patterns: Past, present and Future*, (2020), available at: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901>, (last visited on June 20, 2026).

9 Tsaaro, *Dark Patterns: A Cause of Concern* (2023), available at: <https://tsaaro.com/blogs/dark-patterns-a-cause-of-concern/#:~:text=Harry%20Brignull%20coined%20the%20term,would%20not%20otherwise%20have%20done> (last visited on June 30, 2025).

India, in 2019 IRDAI issued a circular¹⁰ on travel insurance products and mandated online selling platforms to give the consumers details about the insurance and its benefits. It is a way to restrict the malpractices taking place by way of pre-ticked insurance section by these websites. After this numerous other regulation like Consumer Protection (E Commerce) Rules 2020, Consumer Protection Direct Selling Rules 2021 *etc.* came into force to deal with such practices taking place online. Though these regulations were dealing with specific dark patterns and are not comprehensive enough to deal with all the dark practices being used by e commerce platforms. Hence came the rules of 2023.

IV Applicability of dark pattern guidelines

Department of consumer Affairs along with the Advertising Standard Council of India constituted a task force as well as conducted interactive session with the stake holders to submit recommendations in relation to dark patterns. Based on these recommendations Dark Pattern Guidelines were issued by the Department of Consumer Affairs. Para 3 of these guidelines limits their applicability to all platforms, systematically offering goods or services in India; advertisers; and sellers.

As per Para 2(g) of these Guidelines the term platform under the guidelines have same meaning as provided under the E Commerce Rules of 2020. Rule 3 (i) of the Rules of 2020 define:¹¹

platform as an online interface in the form of any software including a website or a part thereof and applications including mobile applications.

The definition is seemingly wide enough to include websites as well as apps/SAAS selling their products online. “Advertiser” was given the same meaning as provided under the guidelines on Prevention of False or Misleading Advertisements and Making Endorsements Relating Thereto 2020, where it has been defined to mean a “person who designs, produces and publishes advertisements either by his own effort or by entrusting it to others in order to promote the sale of his goods, products or services and includes a manufacturer and service provider of such goods, products or services.”¹² The definition is wide enough to make not only the company advertising their products liable but also advertising companies liable. The third sub clause of para 3 make them applicable to sellers as well and the term seller has been given the same meaning as provided under the E Commerce Rules 2020 which define the

10 IRDAI, *Circular on Travel Insurance Products and operational matters*, (2019), available at :<https://irdai.gov.in/document-detail?documentId=392465&ref=static.internetfreedom.in> (last visited on June 30, 2026).

11 E Commerce Rules, 2020, Rule 3 (i).

12 Guidelines on Misleading Advertisements and Making Endorsements Relating Thereto, 2020, Para 2 (b).

seller the same way as it has been defined under the Consumer Protection Act 2019, Section 2 (37) and also adds service providers to this definition. Section 2 (37) states:¹³

product seller”, in relation to a product, means a person who, in the course of business, imports, sells, distributes, leases, installs, prepares, packages, labels, markets, repairs, maintains, or otherwise is involved in placing such product for commercial purpose.

The definition is very clearly worded and includes within its ambit seller in what ever capacity they sell the products. Though the definition comes with an exclusionary clause, which excludes from its ambit the sellers of immovable property, professional services or those who are just acting in financial capacity. It is pertinent to mention that sale and purchase of immovable property has also been excluded from the purview of IT Act 2000.

After carefully understanding all the different aspects of clause 3, it can be safely stated that the guidelines have been given the widest possible applicability.

V Kinds of dark practices

E commerce platforms deploy numerous kinds of dark patterns the number of which is continuously increasing. Para 4 prohibits any person or platform to engage in “any kind” of dark practices. Further elaborating on this provision para 5 states that a platform shall be considered to be engaging in dark patterns if they use any dark patterns specified in Annexure I. This Annexure specifies 13 different kinds of dark patterns that various platforms use to deceive the consumers which are listed and elaborated hereinafter.

False urgency

This simply means creating a sense of urgency or scarcity of a product making the consumers immediately buy the product or take an immediate action in relation to the same. This may also include showing false popularity of the products. Examples of this kind of dark patterns may include statements like: “Sales Ends Soon”, “Few Pieces left”, “100 others viewing this product”, *etc.*

Basket sneaking

This has been defined under the guidelines to mean addition of some extra services, products, payment to charity *etc.* without the permission of the user which results in the user paying more than they actually intended or should have paid for the products. For example : When a user buys a furniture product, the assembling services get added automatically making the consumers pay more for the products or extra hidden charges that are added when you check out like handling charges, *etc.*

¹³ Consumer Protection Act, 2019, S. 2(37).

Confirm shaming

This means using such statements, audio or videos so as to create a sense of fear, shame or ridicule among users for not having used or bought a particular product or service. According to Harry Brignull the U.K.-based UX expert who coined this term confirm shaming refers to the situation where “The option to decline is worded in such a way as to shame the user into compliance.”¹⁴ Some of the examples of this may be : “I hate saving money”

Forced action

Forced action refers to a situation where the users when buy something or take certain services they are made to do something extra that they did not intended or did not wanted. For example: if amazon mandates prime subscription for the purpose of buying anything from their website or app or if you buy an electrical item you are forced to buy the parts also of the same brand. In the case of *Mark Brnovich, Attorney General v. Google, LLC*¹⁵ google was made to pay \$85 million for deceptively obtaining users’ location data to make billions of dollars in profit. In this case “General Brnovich began an investigation of Google after 2018 Associated Press article revealed that the company was misleading and deceiving consumers about the collection and use of their personal location data by tracking smartphones even when consumers disabled the “Location History” setting.”

Subscription trap

This simply refers to a kind of practice in which cancelling the subscription becomes next to impossible for the users due too lengthy process or some kind of hidden charges or the instructions related to the same being confusing or cumbersome. A simple example of this could be when you cancel or pause automatic payments on Paytm, one is made to enter the UPI Pin making them believe that there money can be deducted again in the name of cancellation and hence people hesitate doing the same.

Interface interference

As per the guidelines it means “a design element that manipulates the user interface in ways that (a) highlights certain specific information; and (b) obscures other relevant information relative to the other information; to misdirect a user from taking an action as desired.” For example: when you try to cancel the subscription of an app the options read cancel and no cancel, making it difficult for the user to make a

14 Stephen Gossett, *What Is Confirmshaming and Why Should You Avoid It?*, (2021), available at: <https://builtin.com/design-ux/confirmshaming> (last visited on June 30, 2026).

15 Kris Mayes, *Attorney General Mark Brnovich Achieves Historic \$85 Million Settlement with Google* (2022), available at :<https://www.azag.gov/press-release/attorney-general-mark-brnovich-achieves-historic-85-million-settlement-google> (last visited on June 30, 2026).

choice. In 2018¹⁶ yahoo gave a big add when the user tried to change their settings that distracted the users and made it difficult for them to change their settings.

Bait and switch

Bait and Switch is an old tactic where the seller baits the consumer by telling them that the desirable goods and services are available at cheap price but when the user actually tries to buy them they are either sold out or are available on high price or the same offer is available on other items which the seller intended to sell. For Example: you see an add of Myntra on your Instagram or Facebook page and you liked the product shown in the advertisement and the price is also very affordable but when you click the link you find out that the product is no longer available and you end up buying other similar products.

Drip pricing

Drip Pricing has been very broadly defined in the guidelines so as to include any kind of practice with regard to pricing which may be deceptive in nature. The guidelines give the following meaning to drip pricing:¹⁷

- “ (i) elements of prices are not revealed upfront or are revealed surreptitiously within the user experience; or
- (ii) revealing the price post-confirmation of purchase, i.e. charging an amount higher than the amount disclosed at the time of checkout; or
- (iii) a product or service is advertised as free without appropriate disclosure of the fact that the continuation of use requires in-app purchase; or
- (iv) a user is prevented from availing a service which is already paid for unless something additional is purchased.”

Further the guidelines also provide an exception to this rule in cases of price fluctuation of the product.

A very simple example of this kind of dark practice could be swiggy or zomato: when you add the products to the cart the value of the products is less but when you are about to check out different kind of charges are added to the products that you intend to purchase and the cart value increases. Another example which can be seen is of OLA and UBER rides where fair at times get increased when we reach the destination because of varying factors, which at times are not in control of either the driver and user of these services.

16 UXP Dark Patterns, *Yahoo: Distraction While Changing Security Settings*, (2018), available at :<https://darkpatterns.uxp2.com/pattern/yahoo-distraction-while-changing-security-settings> (last visited on June 30, 2026).

17 Guidelines on Prevention and Regulation of Dark Patterns, 2023, Annex. I.

Disguised advertisement

This is an advertising technique where advertising is done in a manner that user believe that they are looking at user generated content or some other article or paper that they may be interested in. Such kind of advertising make website owner generate more revenue from ad impressions, it may also in turn lead to more click through and increased sales.¹⁸

Guidelines provides an explanation with regard to this dark patter which states that “for the purposes of this paragraph, the expression “disguised advertisement” shall also include “for the purposes of this paragraph, the expression “disguised advertisement” shall also include misleading advertisement as defined in clause 2(28) of the Act and the “Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022”. Such advertisements are defined under the Consumer Protection Act as those which falsely describes the products or services or gives a false representation to the nature of the products any representation which can be considered as unfair trade practice.¹⁹ This explanation is giving an amply wide meaning to the term disguised advertisement so as to bring within its ambit any advertisement that is meant to mislead the general public. Further the second part of the explanation puts a burden on the platform/seller or advertiser as the case may be to make necessary disclosure with regard to what they are displaying is an ad.²⁰ Though dealing with the same wrong in two different sets of guidelines may not be the correct approach as consumers may get confused as to which set of legislation is best suited for them. An example of this kind of dark pattern could be the promotions done by online influencers.

Nagging

Nagging is pattern by which the consumers are constantly disrupted by the platforms from doing something by repeated requests to do something else which may not be in the best of their interests. For example : when you watch you tube videos or play games online some adds keep on appearing in between now and then so as to make you take the subscription of you tube or to make you download new games which may be habit forming. The definition uses the term “Disrupted” or “annoyed” while defining this practice. Both these terms are seemingly not very clear. Moreover what may be annoying for one person may not be annoying for another.

Trick question

Trick question or trick wording as it may be said, is use of difficult or confusing language meant to mislead the consumer. Due to the large amount of information

18 Deceptive Patterns, *Disguised Ads*, available at :<https://www.deceptive.design/types/disguised-ads> (last visited on June 30, 2026).

19 Consumer Protection Act, 2019, S. 2 (27).

20 Guidelines on Prevention and Regulation of Dark Patterns , 2023, Annexure I.

available online, users generally scan read the available content. Meaning thereby they do not delve into the details of each and every word and this strategy take benefit of this limitation of the consumers.²¹ An example of this kind of dark pattern could be : Providing the privacy or return policies only in local language while the website is available all around the world.

SAAS billing

SAAS refers to Software as a service. It is a software distribution model where the cloud host make the services available to use over the internet. Google workspace, zoom are all examples of SAAS.²²

As per Annexure I

SaaS billing refers to the process of generating and collecting payments from consumers on a recurring basis in a software as a service (SaaS) business model by exploiting positive acquisition loops in recurring subscriptions to get money from users as surreptitiously as possible.

SAAS billing turns into a dark practice when the users are not properly informed about the same. For example when the trial is converted to a paid subscription, using improper card authorisation or payment techniques *etc.* The definition is seemingly not very clear and even the illustrations are not very happily worded. The best example of this kind of dark practice is autopay services which in many cases get activated without permission.

Rogue malware

Malware in very simple words is generally an code or file that attacks the computers to which it is transmitted. It makes the computer attacked to perform the function that attacker wants to perform.²³ Rouge Malware as per the guidelines refer to a technique that forces users to purchase a fake malware because of the scareware used by the platform.²⁴

For example: when you download an app and still keeps on getting pop ups to download another app or click on an link with embedded ransomware in it. When we look at the illustration relating to this dark pattern in the guidelines, they seem to be dealing more with Misleading advertisements with embedded malware in it.

21 Deceptive Patterns, *Trick Wording*, available at :<https://www.deceptive.design/types/trick-wording> (last visited on June 30, 2026).

22 Guidelines on Prevention and Regulation of Dark Patterns, 2023, Annexure I.

23 Paloalto, Malware, *What is Malware & How to Stay Protected from Malware Attacks*, available at: [https://www.paloaltonetworks.com/cyberpedia/what-is-malware#:~:text=Malware%20\(short%20for%20\"malicious%20software,methods%20to%20infect%20computer%20systems](https://www.paloaltonetworks.com/cyberpedia/what-is-malware#:~:text=Malware%20(short%20for%20\) (last visited on June 30, 2026).

24 Guidelines on Prevention and Regulation of Dark Patterns, 2023, Annexure I.

Above mentioned are the dark practices recognized by the government of India. These guidelines though are welcome step but are not complete and there are many other kind of dark practices that are missing here. Moreover even after more than two years, these guidelines are being regularly flouted by the e-commerce platforms. It is because of these reasons the Central Consumer Protection Authority issued an advisory on dark patterns, titled “Advisory in terms of Consumer Protection Act, 2019 on Self-Audit by E-Commerce Platforms for detecting the Dark Patterns on their platforms to create a fair, ethical, and consumer-centric digital ecosystem” (“2025 Advisory”). All e-commerce platforms are mandated to conduct self-audits within three months of the issue of this advisory to make sure that they are not engaging in any kind of dark patterns.²⁵ It is pertinent to mention here that the advisory does not provide any kind of punishment for flouting these guidelines.

VI Artificial intelligence and dark patterns

One of the most coveted developments of the present times is AI. Though its interface with almost every subject is debated. Use of AI comes with its own pros and cons in every field and so as the case with consumer protection and dark patterns as well. AI is being used by almost all major e-commerce platforms to provide the users with personalised interface. AI, can predict the user behaviour through past experiences and also has the capacity to influence it as well. This improved user interface can be used in both ethical and unethical ways. For the purpose of this paper we are concerned with the ways in which AI can manipulate user behaviour.

Luiza Jarovsky proposes that AI dark patterns “would be AI applications or features that attempt to make people:²⁶

- (i) believe that a particular sound, text, picture, video, or any sort of media is real/authentic when it was AI-generated (*false appearance*)
- (ii) believe that a human is interacting with them when it's an AI-based system (*impersonation*)”

False appearance is a very common problem these days where the user believes a content to be original while in reality it is AI-generated. Most of the websites have chatbots these days for helping the consumers, most of the times these chatbots are AI-based while many believe them to be human interactions. These Chatbots can negatively influence consumer behaviour. In fact many consumers especially young and elderly may not be able to distinguish them human interactions. AI based on past

25 Ministry of Consumer Affairs, *E-Commerce Platforms Urged to Self-Audit and Eliminate Dark Patterns: Centre available at* :<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146813#:~:text=As%20an%20outcome%20of%20the,on%205th%20June%2C2025> (last visited on May 30, 2026).

26 Victoria Nduka, *AI-driven dark patterns in UX design*, available at: <https://medium.com/design-bootcamp/ai-driven-dark-patterns-in-ux-design-8cbddee120c4> (last visited on May 30, 2026).

purchase history, future plans may easily make consumers do those expenses which they otherwise would not have. For example: If one ask a AI chatbot to pick a dress for a party and AI being aware of the fact that its your birthday next week or the jewellery you purchased last week may make one buy a much costlier dress that they were intending to purchase by making statements like “it will be a best dress for your birthday party” or “it will look great with the jewellery you purchased last weak.”

Another aspect of use of AI as algorithmic bias which is embedded in the AI system. Most common and most used example of such kind of bias is by job search engines where bsaed on the gender of the applicant the available jobs are displayed.

Based on the above discussion it can be easily concluded that AI has the capability of developing dark patterns as per the user meaning thereby personalised dark patterns while being embedded with biases. These dark patterns are developed based on the understanding of the user by AI not only on the platform on which they are employed but also on other platforms like social media, online messaging platforms *etc.* Such dark patterns will not only be difficult to recognise but also to deal with as well.²⁷

In this scenario it becomes inevitable for the law makers to make rules in regard to use of AI by e-commerce platforms. One of the most essential aspect of this would be clear marking of AI generated content.

VII Consent fatigue and the dark patterns

The Digital Personal Data Protection Act 2023 makes consent an essential element for any data fiduciary for processing personal data. Consent under this legislation is required to be “Free, specific, informed and unambiguous”²⁸ The purpose of giving so much importance to consent is to make sure that consumer autonomy us protected. The result is that users of internet have to make a lot of choices. Every webpage ask about the permission to use cookies, the e commerce and social medial platforms have to ask for permissions even while doing routine activities.

Consent fatigue is a phenomenon where because of the huge number of requests, the user start clicking “Accept all” and ticking the checkbox without even reading the contents. The consent in this situation is technically valid but in reality meaningless.

While placing heavy reliance on consent, Indian law makers have forgotten the fact that it is required to be “informed and unambiguous” as well. Indian internet users have grown multifold over the last few years but the literacy rate has not. Most of the platforms show their consent notices in English language which many are not able to comprehend. Those who understand the English language at times do not

27 Krishna Dea Singh Chauhan and AnuPriya, “Dark Patterns? AI-generated Persuasion and the Regulatory Void in Indian Law”, 10 (1) *Journal of Development Policy and Practice*, 80-95, 2025.

28 Digital Personal Data Protection Act, 2023, s. 6.

understand the technical terms used and in case of those who understand both the language as well of the words ignore such notices by just looking at their length and details.

Another aspect of consent fatigue is power imbalance, where many users believe that if they want to use the platform services they have to agree to all the conditions and they have no option to disagree with the terms and conditions. Though DPDP Act does provided for the consent managers but the questions is how many will be able to approach them.

Consent fatigue may indirectly lead to increased use of dark patterns. These platforms ask users to take permission to your their location, phone, social media profiles *etc.* By using the data available the platforms with the help of AI design personalised dark patterns for the purposes of deceiving consumers. This is just one way in which consent fatigue may promote dark patterns and there are many others. Though the author has not come across any research in this regard.

In this scenario, it can be said that most of the e commerce platforms in the name of consent might be misusing consumer data according to their own whims and fancies. Many countries around the world are taking consent fatigue very seriously. EU for example by its Regulation 05/2020 and opinion 28/2024 has made it clear that repeated consent prompts will nullify the consent all together.²⁹

VII Dark patterns around the world

At International level OECD (Organisation For Economic Corporation and Development) held a roundtable conference on Dark Patterns in November 2021. A report of which was published in 2022. The report provided a working definition of Dark Patterns. Apart from this the reports identified certain kinds of dark patterns, most of which also form a part of Indian Guidelines as well. The report further highlights the fact that dark patterns are ever evolving and this taxonomy may not be applicable for future dark patterns.³⁰

Considering the importance of dark patterns almost all countries of the world have come with legislations to control dark patterns. Australia Information Commission has recognised certain dark patterns while EU have framed plenty of Legislations to Protect consumers. In US Federal Trade Commission has issued Guidelines to Protect consumers from deceptive practices. Similarly Argentina, Kenya and almost every

29 *Consent Fatigue and the Illusion of Choice: Rethinking User Autonomy under India's DPDP framework*, available at: <https://dpo-india.com/Blogs/consent-fatigue-illusion-choice/> (last visited on Mar. 30, 2026).

30 OECD Publishing, *Dark Commercial Patterns*, available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf (last visited on Mar. 30, 2026).

country is dealing dark patterns in one way or the other. These are but some of the legislations around the world that aim to control Dark Patterns. For the Purpose of this research author has delved into the legal regime of EU in detail.

EU legal regime on dark patterns

There is no single legislation dealing with dark patterns in EU. The concept was for the first time dealt in the Unfair Commercial Practices Directive (UCPD).³¹ However the directive does not use the term dark pattern but deals only with misleading commercial practices. Following this a lot of new legislations were added in the EU legal framework to deal with those problems which UCPD could not resolve. The Digital Services Act (DSA)³² in its recital 67 defines Dark Pattern as “practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions”. The Recital excludes from its purview the dark patterns covered under UCPD and General Data Protection Regulation 2016. EU’s Data Act³³ in its Recital 38 deal with data minimisation and dark patterns and require third party to use the data only for the purpose agreed by the users. For this purpose the Act requires third parties to not to engage in Dark Patterns. The EU’s AI Act³⁴ also deals with dark patterns, Article 5 of which is discussed above in this paper. It can be said that EU AI Act is much wider in its scope and requires case by case interpretation of dark patterns. Another legislation that can be referred here is EU’s Digital Market Act. This Act deals with large tech companies referred to as gatekeepers. This legislation in its Recital 13 prohibit these gatekeepers to engage in any kind of dark patterns.³⁵

A carefully analysis of the EU legislations show that there multiple legislations dealing with dark patterns which is the case with India as well. Inge Gref³⁶ argues that “While useful complementarities may arise when parallel sets of rules target different concerns or protect different values, there are also risks of inconsistencies that may lead to either under- or over enforcement due to the fragmentation of the overall regulatory framework.”

31 EU Unfair Commercial Practices Directive, Directive 2005/29/EC.

32 The Digital Services Act , Regulation (EU) 2022/2065.

33 Data Act, Regulation (EU) 2023/2854.

34 Artificial Intelligence Act, Regulation (EU) 2024/168.

35 *Regulating Dark Patterns in EU: Towards Digital Fairness*, available at :[https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA\(2025\)767191_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf), (last visited on Mar. 20, 2026).

36 Inge Graef, *The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?*, available at. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4411537 (last visited on Mar. 20, 2026).

Despite its short comings EU legislative regime in relation to dark patterns is far ahead of the Indian guidelines especially the EU AI Act. The Act in Recital 70 is also able to deal with the problems associated with personalisation of AI.

Another aspect of EU legislations is that most of them are open ended and thus have the capacity to curb every kind of dark pattern. Thus, it can be said that they are futuristic in nature. While after above discussions it can be safely stated that Indian legislations are narrower in scope especially unable to deal with AI based dark patterns.

California 's legal regime on dark patterns

California Consumer Privacy Act , 2018 has gained a lot of attention being one of the first US legislation to protect consumer privacy and dark patterns. The “right to opt out of the sale and sharing of Personal Information” are the corner stone on which this legislation rests.³⁷ The definition of consent in the legislation clearly state that the use of dark patterns does not constitute consent.³⁸ Another interesting aspect of this legislation is that it is based on the Right of Consumers to Know what information is being collected and how it will be used. This legislation further recognises the right of the consumers to limit the use of their sensitive personal information. The enforcement mechanism is also provided in CCPA which is missing in many legislations dealing with dark patterns, which is the case with India as well. Though the CCPA was amended by California Privacy Rights Act of 2020 (“CPRA”). CPRA defines Dark patterns to “means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation”³⁹ Though it is believed that the provisions applies in relation to privacy rights and thus un applicable to many kinds of dark patterns. One of the important aspect of CPRA is that it moves beyond opt out notices.

Another important and interesting aspect of California's Legal Regime dealing with Dark patterns is California Age-Appropriate Design Code Act which requires business engaging in activities likely to be accessed by children shall not adopt dark patterns that may make children share their private information or engage in harmful activities.⁴⁰

After analysing the legislations of California that deals with dark patterns it can be safely stated that the focus is on consumer data and consumer rights to know, which is not the case with other countries. These two aspects forms the basis of every kind of dark patterns which other countries have not realised and not focused on. India and most of the countries deal with dark patterns in commercial laws and not in

37 Von Hong Tran, Aarushi Mehrotra et al., Dark Patterns in the Opt-Out Process and Compliance with the California Consumer Privacy Act (CCPA), *available at* <https://dl.acm.org/doi/10.1145/3706598.3714138> (last visited on Mar. 20, 2026).

38 California Consumer Privacy Act , 2018, S. 1798.140 (8)(h)

39 California Privacy Rights Act, 2020, S. 1798.140

40 CAB-2273 The California Age-Appropriate Design Code Act.

privacy legislations, though dark patterns are part of both. Another interesting aspect of these legislations is the special status given to children under 18 years of age which is the need of the hour. This aspect is of special importance to protect children from any kind of deception and India should incorporate it in its legislation.

IX Concerns and suggestions

When these guidelines are notified many agencies highlighted numerous concerns and suggested certain changes in these guidelines. Let us discuss few areas of concern with regard to these guidelines:

Regulatory overlap

Already existing regulatory frameworks like the Consumer Protection Act, Guidelines on Misleading Advertisements of 2022 etc provides remedy against some of these dark patterns both in online and offline. Moreover few of the Dark Patterns discussed above raise privacy concerns as well and can be dealt with under the other existing legislations Digital Personal Data Protection Act of 2023. So, there is a need to clearly delineate the scope and applicability of these guidelines vis a vis the other existing legislations.

Harmonious construction with available legal framework

The term platform can be given the same meaning as Intermediary which is defined under the Information Technology Act 2000. Intermediaries are provided certain safe harbours while no such provision is available in these guidelines and hence needs to be harmoniously construed or a clear provision in this regard should be added.⁴¹ Though guideline 6 clearly specifies that where an existing legislation deals with any dark patterns the Guidelines should be in addition to such legislation and not in derogation of it but in the situation like the one discussed the provision seems to be not of much help.

Commercial gains

The guidelines defines the term Commercial Gain to mean “monetary gain or financial advantage of any kind.” This term has been used in Annexure I while dealing with Nagging and Confirm Shaming. The author feels that keeping in mind the nature of the internet restricting it merely to financial gains may not be correct.

Dark patterns and specified dark patterns

The guidelines uses two terms i.e. Dark Patterns as defined in Guideline 2 and Specified Dark Patterns with reference to dark patterns listed in Annexure I. There may be

41 Surya Pratap Singh Naruka, Shewta Khandelwal, *Reshaping India's dark Pattern Guidelines: Towards a Better Digital Landscape* (2024) , available at: <https://www.lawrbit.com/article/reshaping-indias-dark-pattern-guidelines-towards-a-better-digital-landscape/> (last visited on Mar. 20, 2026).

cases where the reference to Dark Patterns may cause confusion and in certain situations can be restricted to the dark patterns specified in Annexure I. This will narrow down the scope of these guidelines and hence the use of two different terms should be avoided.

No offence or penalty specified

Though Guideline 4 prohibits the platforms to engage in any kind of Dark Patterns and Guideline 5 raises a presumption if any platform engages in any practice specified in Annexure I but does not specifies as to what will be the nature of such act and neither specifies the penalty for the same. The guidelines also does not deal with the mens rea or intention aspect. Also these guidelines does not specify what penalty will be imposed or how compensation will be granted.⁴²

Artificial intelligence

Artificial Intelligence can help us in various ways and that includes in dealing with Dark Patterns as well. Artificial Intelligence can help consumers in making right selection or it may be used to deceive consumers as discussed above. These guidelines do not refer to AI at all and thus are unable to deal with AI based dark patterns.

Way out

The guidelines nowhere talks about how a lay consumer can detect the existence of Dark Patterns on any platforms or what kind of add ons/safety features/ filters etc should a platform apply to make sure that such kind of dark patterns are not available on their platforms. Moreover, it nowhere talks about how the consumers should be educated with regard to the existence of such patterns

Vague wordings

While defining certain kind of dark pattens the terminology used is not clear For Example Nagging: this dark pattern required the user to be disrupted or annoyed but the term is very vague as what can annoy one person may not annoy another. More over mere annoyance and disruption in certain situations may not meet the requirement of specified dark pattern as well.⁴³ Similar is the case with few other kind of Dark patterns like Disguised Advertisements, SAAS Billing, *etc.*

42 Dylan Sharma, *The Guidelines on Dark Patterns – Effective or Incomplete?*, (2024) , available at :<https://lawschoolpolicyreview.com/2024/03/25/the-guidelines-on-dark-patterns-effective-or-incomplete/> (last visited on Mar. 10, 2026).

43 Arun Prabhu, *Anirban Mohapatra and Mansi Jain, 'Dark Pattern Guidelines: Illuminating Or Illusory?* (2023), available at :<https://corporate.cyrilamarchandblogs.com/2023/12/dark-pattern-guidelines-illuminating-or-illusory/> (last visited on Mar. 10, 2026).

Lack of penalty/punishment

One of major reason for compliance of any legislation is fear of punishment or penalty of some kind, which these guidelines are lacking. This can be apparent from the fact that even after two years many platforms are still using these dark patterns to woo their customers.

X Conclusion

All in all it can be safely concluded that these guidelines are a way ahead towards secure Digital Bharata. However the guidelines miss on some very important aspects and are not happily worded at few places and need to be re looked. The need to protect the consumers from dark patterns especially on the e commerce platforms is something that almost every country has realised. Though there is need to have a balanced approach to make sure that both consumers and business houses do not suffer. Technology is ever evolving and the these guidelines do not seem to deal with this problem and stringent in its approach. A very important point to highlight here is that many consumers are not even aware of the fact that they are being mislead or deceived. It thus becomes pertinent to adopt certain measures to educate common men about the same. Empowering users is one of the most important step to deal with such kind of practices which is missing in these guidelines. Apart from this the guidelines do not focus on the vulnerabilities of children and old people on these platforms . The above discussion highlights various problems with these guidelines. Also it is apparent that 2025 advisory do't solve much of these problems. In these circumstances it may be safely concluded that these guidelines though a welcome step but are not complete in them self to deal with present as well as future problems in relation to dark patterns.

*Archa Vashishtha**

* Assistant Professor, Faculty of Law, University of Delhi, New Delhi.
