THE GROWING USE OF DARK PATTERNS ON THE WEB: IMPACT ON CONSUMER RIGHTS

Shreya Shekhar, Symbiosis Law School, Pune

ABSTRACT

With the advent of digital consumerism, consumers are exposed to plethora of websites on the web. It is par for the course for consumers to get deceived by 'dark patterns' in the digital domain. Dark patterns are such deceptive user interfaces, which manipulate the consumers into taking actions against their original interest or state of mind. These patterns often go unnoticed and are discretely proliferated on digital domains. Legislative advancements are struggling to keep pace with the ever-evolving challenges posed in the digital consumerism arena. This essay will throw light on the said issue, in a manifold manner. Firstly, it will analyse dark patterns and the tactics used on websites by companies at the expense of consumer rights. Further, the essay will explore the consumer protection laws, and any other existing laws or guidelines regulating the usage of dark patterns and global best practices. Post analysing the adequacy of laws in India and global regulatory responses, a set of recommendations will be laid down to protect consumer rights in an era where digital consumerism is at its peak.

Keywords: dark patterns, deceptive, consumer rights, privacy, legislations, global best practices

Introduction

"Over 1 in 2 consumers surveyed who bought something via app or software platforms said they experienced dark patterns like subscription trap, drip pricing and bait and switch[1]"

- *Survey by Local Circles*

Did you ever come across a notification or message saying "Last chance! Offer expires in the next 15 Minutes"? If it comes again in the future, do not panic, chances are-- it's just another dark pattern.

Dark patterns have gained traction in the recent times after consumers have raised complaints, and also various surveys by different international consumer bodies have released shocking results which create concern about the consumer autonomy in the digital world.

One such eye-opener was the survey conducted by the Federal Trade Commission, where the review scrutinized *642* websites and mobile apps offering subscription services globally. According to the results, nearly *76%* of the examined sites and apps employed at least one dark pattern, and almost *67%* used multiple dark patterns.[2]

For the first time in 2010, **Harry Brignull** had coined the term 'dark patterns'[3], as a tactic to exploit consumers through manipulative UI/UX (User Interface, User Experience) designs which hijack their decision making. These include ambiguous consent mechanisms for data collection, tricking users for certain add-ons (e.g. Automatic Insurance add on while booking a flight), making cancellation of subscription difficult, etc. These tactics might be a tool for efficiency and optimization of the business, but they raise major legal and ethical concerns for the consumers.

Understanding Dark Patterns: New Threat to Consumer Autonomy

Dark patterns are mostly proliferated in sectors like fashion, e-commerce, finance, food and beverages and personal care. Dark patterns exploit human psychology, taking advantage of

[1] Business Standard, 67% of Consumers Experienced Subscription Trap: LocalCircles Survey, Bus. Standard (Feb. 12, 2024)
[2] Subscription Insider, *FTC, ICPEN, GPCEN Announce Results of Review of Dark Patterns in Subscription Services and Privacy*
[3] Harry Brignull, Deceptive Design: How Dark Patterns Trick Consumers, Oxford University Press, 2022.

cognitive biases like **loss** aversion and default bias. As digital markets grow, these manipulative tactics violate consumer protection laws and erode trust in online services. The various types of dark patterns include:

Roach Motel (Easy to sign in, Hard to sign out): This pattern makes the signing up process seamless for the consumer, with lesser clicks and waiting time. However, the process of unsubscription or cancellation is extremely difficult to gauge for the consumers.

In a recent case study, Amazon's **Prime cancellation process** was found to require multiple confirmation steps, discouraging users from leaving.[4]

Sneak Into Basket (Hidden add-ons) – During the shopping process, websites subtly add extra items to a consumer's cart with an underlying hope that they won't notice it before checking out. It is often observed in the aviation industry, where health insurance and flexi cancellation charge are already selected at the time of checkout.

An illustration can be seen in the case study where **GoDaddy** pre-selects unnecessary add-ons like SSL certificates during domain purchases.[5]

Forced Continuity (The Unprecedented Subscription Fee)- Websites lure the consumers with free trials, while taking all the necessary financial details, only to be automatically charged once the trial expires. There are no clear reminders sent to the consumer before the expiry of the trial period, which makes it difficult for the consumer to terminate the subscription.

In a similar case, Adobe's **hidden cancellation fee for Creative Cloud subscribers** led to backlash and legal scrutiny. [6]

Fake Urgency and Scarcity (Creating a False Panic) – Websites display fake countdown timers or send notifications and messages about false stock scarcity which creates a pressure amongst consumers and forces them to make quick purchases.

A leading case study can be observed, where Flipkart and Amazon have been accused of **misleading urgency tactics**, showing *"Only 2 left!"* notifications when stock was actually

[4] Norwegian Consumer Council, You Can Log Out, But You Can Never Leave: How Amazon Manipulates Consumers into Staying Subscribed, Forbrukerrådet (2021)
[5] Cory Doctorow, *GoDaddy's Shopping Cart Shenanigans: A Dark Pattern Case Study*, BoingBoing (Aug. 2022)
[6] Brian Barrett, *Adobe's Subscription Cancellation Fees Are Infuriating Customers*, Wired (Feb. 2023),

replenished frequently. [7]

Bait and Switch (Not adhering to the Promise Made) – In this tactic, the website lures the consumer with a promise, but then switches it for another less desirable action.

For example, when a user clicks on a link to read a blog but is directed to the app store, aggressively promoting to download a certain app.[8]

These tactics have adverse effects on the consumers as it can often lead to financial loss, weaker or distorted competition, harm to autonomy as the consumer's choices were based on false aspects of the website.

This whole deception results in reduced consumer trust and engagement with businesses and the digital e-commerce platforms. The privacy of the consumers is deprived as their data is shared for billions of dollars in the name of personalization, at the cost of their protection and privacy.

Indian Legislations and Regulations

The **Consumer Protection Act of 2019** [9]acts as the cornerstone of consumer's rights and protection in India. It encompasses both traditional and digital markets in its ambit and safeguards consumers against 'unfair trade practices' in both. **Section 2(47)** [10]defines unfair trade practice as something which adopts any unfair method or unfair or deceptive practice. The exercise of dark patterns on the web clearly falls under the ambit of unfair trade practice, and therefore under the Consumer Protection Act, 2019.

Under **Section 10(1)** [11]of the act, the **Central Consumer Protection Authority (CCPA)** is established as a regulatory authority, safeguarding consumer rights and flagging unfair trade practices. The CCPA is entrusted with extensive powers to investigate complaints, conduct inquiries, and take corrective actions against entities in violation of consumer rights.

Exercising its powers under Chapter III of the Consumer Protection Act, 2019, the CCPA, in

[7] Arun Prabhudesai, Flipkart's Fake Discounts & Dark Patterns Exposed, Trak.in (Oct. 2023),
[8] Harry Brignull, Dark Patterns (2010)
[9] Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India)
[10] Consumer Protection Act, 2019, § 2(47), No. 35, Acts of Parliament, 2019 (India)
[11] Consumer Protection Act, 2019, § 10(1), No. 35, Acts of Parliament, 2019 (India)

November 2023 issued the **"Guidelines for Prevention and Regulation of Dark Patterns, 2023".**

These guidelines were the need of the hour and still play a crucial role in deterring deceptive practices on the web. The guidelines identify and prohibit 13 specific types of dark patterns, explicitly targeting deceptive design practices in digital interfaces. The task of enforcing these guidelines is entrusted with the CCPA, and it is further empowered to impose penalties in case of non-compliance. The 13 prohibited practices under guidelines are as follows:

(i) creating false urgency — falsely implying urgency or scarcity, misleading a consumer to make an immediate purchase;

(ii) basket sneaking — adding extra items during checkout;

(iii) confirm shaming — employing language to shame, guilt or influence a consumer to purchase a product or service;

(iv) forced actions — compelling a consumer to purchase to unrelated products or services;

(v) subscription trap — making cancellation of a paid subscription extremely complicated;

(vi) interface interference — manipulating the user interface to emphasise or conceal information;

(vii) bait and switch — promoting an outcome of the user's action, but serving an alternate outcome;

(viii) drip pricing — not revealing prices upfront or charging a higher price at checkout;

(ix) disguised advertising — posing advertisements as content, tricking consumers to click on them;

(x) nagging — disrupting the user experience through repeated interaction to facilitate a transaction;

(xi) trick question — use of confusing or vague language aimed at misdirecting a consumer;

(xii) software as a service (SaaS) billing — collecting recurring payments from consumers on a SaaS business model through positive acquisition loops; and

(xiii) rogue malwares — deceiving consumers into believing that there is a computer virus and tricking them into buying a fake malware removal tool[12]

Any e-commerce platform based in India, or one that is not based in India but provides goods or services to consumers in India, falls under the ambit of the Guidelines. The patterns discussed in the guidelines are not uncommon or new to the Indian market and therefore, the Guidelines have been a cause of relief and not a surprise.

Another legislation having an impact on consumers online is the **Digital Personal Data Protection Act, 2023 (DPDP).**[13] While the Indian data protection laws do not explicitly incorporate the concept of dark patterns in within their privacy laws like the United States does, however, the mandate of consent provides protection to the consumers. It indirectly addresses the deceptive design practices that infringe upon consumer autonomy which violates the concept of a free, unambiguous, specific, informed consent.

The overall legislative ecosystem for dark patterns in India entails the Consumer Protection Act, the 2023 guidelines on dark patterns and the DPDP Act[14], which together complement measures ensuring deterrence of unfair trade practices, prohibition of 13 specific types of dark patterns and ensuring consent and data protection.

However, the effectiveness depends majorly on the enforcement and monitoring of these enactments. Additionally, only after a substantial number of consumers are made aware of these practices and their rights, the framework can get truly strengthened. The CCPA must mark a proactive role in monitoring and penalizing such violations.

[12] Ministry of Consumer Affairs, Food & Public Distribution, Government of India, Dark Patterns Buster Hackathon (2024)
[13] Digital Personal Data Protection Act, 2023, No. 30, Acts of Parliament, 2023 (India)
[14] Ibid

Global Regulatory Responses

The **Federal Trade Commission** (FTC) of United States has been the forerunner for combatting dark patterns. In the year 2024, the Federal Trade Commission (FTC) sent refunds of more than $72 million to consumers who were manipulated by **Epic Games** (maker of Fortnite video game), to make unwanted purchases[15]. The dark patterns used by Epic Games included levying unwanted charges based on the press of a single button. They let children add up unauthorized charges without any consent or involvement of parents. The FTC is sending the refund payments in various rounds.

In the year 2023, **Google** agreed to pay *$93M* [16]to settle accusations of misleading consumers on location data. Google informed the users that it would no longer track their location once they have opted out, but still continued to track its users for commercial gain. Even after disabling location tracking, the company used hidden settings to track users, violating their privacy and autonomy.

The FTC has also taken action against e-commerce behemoth Amazon. Amazon was charged for enrolling consumers in the **Amazon** Prime Subscription using manipulative user interface designs [17]and making cancellation of the subscription extremely difficult. The US-based ISP (Internet Service Provider) **Vonage** was asked to refund *$100m*[18] to the customers for having a lengthy subscription cancellation process.

Under Section 5 of the Federal Trade Commission Act[19], dark patterns are considered as 'unfair or deceptive" business practices. The state privacy laws of *California[20], Colorado[21] and Connecticut,[22]* exclude agreements where consent was obtained through dark pattern techniques. Sever penalties have also been laid down in case of non-compliance, which can

[15] Federal Trade Commission (FTC), FTC Sends Refund Payments to Consumers Impacted by Epic Games' Unlawful Billing Practices, FTC Press Release (Dec. 2024)
[16] The Guardian, *Google to Pay $391.5m Settlement Over Location Tracking Data*, The Guardian (Sept. 14, 2023)
[17] Federal Trade Commission, *FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel*, (June 2023)
[18] Federal Trade Commission, *FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service*, (November 2022)
[19] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2018).
[20] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199.100 (West 2020).
[21] Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 to -1313 (2021).
[22] Act Concerning Personal Data Privacy and Online Monitoring, Public Act No. 22-15, 2022 Conn. Acts 22-15 (Reg. Sess.).

amount to up to *$7,500 per violation in California*[23]*, $5,000 in Connecticut*[24]*, and $20,000 per violation in Colorado*[25]; which creates a deterrent for the businesses and ensures ethical practices.

The European Union has the **EU Guidelines for Dark Patterns**[26] with respect to Social Media platforms. It regulates how users are unable to protect their personal information and make conscious choices on social media. With many businesses selling goods and services on social media and using it as a platform for e-commerce, such guidelines become crucial for securing consumer rights. The **Digital Services Act, 2022**[27] explicitly bans dark patterns in online platforms. It mandates digital service providers to design their user interfaces in a manner that respects consumer autonomy.

In the year 2022, websites faced a crackdown in EU for using deceptive cookie banners. The crackdown was launched by the European Data Protection Board. EU focusses on a two-fold approach, namely: punitive through GDPR[28] fines and preventive through legislative bans and crackdowns.

Recommendations: Policy and Technological

India has a threefold set of legislation already in existence. To strengthen its applicability, online platforms should be vested with the duty of ensuring compliance with the guidelines. They must be tasked with designing user interfaces devoid of dark patterns and in case of non-compliance, a crackdown or ban must be put on such websites, similar to the stringent action taken by EU. This shall prevent future violations and promote trust and consumer protection.

Drawing from California Consumer Privacy Rights Act, 2020[29] as was discussed in the paper, the India Guidelines can also underline the fact that contracts resulting from dark patterns

[23] Cal. Civ. Code § 1798.155(b) (West 2020)
[24] Colo. Rev. Stat. § 6-1-1311(1)(a) (2021)
[25] Conn. Gen. Stat. § 42-110o(b) (2022)
[26] European Data Protection Board, Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them, (Mar. 2022)
[27] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 2022 O.J. (L 277) 1.
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[29] Supra note 19

would be void ab initio due to an invalid consent obtained.

There exists ambiguity on penalty provisions in the Guidelines regulating dark patterns. Clear penalty provisions must be laid down in order to ensure transparency and proper enforcement of the guidelines.

As the Consumer Law of 2019[30] amended the 1986 act[31], in order to adapt with evolving consumer needs, the current act is in dire need of expansion of its scope to include: AI-generated dark patterns, algorithmically driven manipulation and other tactics used to the detriment of consumers.

The challenge of deepfake generated products, aggressive advertising on digital domains, must be addressed by the legislation as AI has become an integral part of digital platforms and the consumer lives.

A decentralised consumer feedback forum based on blockchain technology can be a laudable step towards ensuring an anonymous but impacting review of consumers. This will compel the firms to take corrective actions in order to save their reputation and market presence.

Unlike the USA and EU, Indian Judiciary and regulatory bodies have not been proactively penalising such acts of deceptive patterns on the web. Doing so can create a deterrent effect as quite a lot depends on reputation and trust in the Indian market for consumers. A legal suit and penalty can have a direct impact on the same, compelling businesses to indulge in fair practices and comply with the law.

A mandatory website U/UX audit can create a streamlined process, where websites hosting more than a certain number of users (e.g. 5 Million) must undergo a bi-annual design audit to ensure that no deceptive practices are used by the platform.

A right balance of legislative and technological developments is required to create a strong ecosystem of consumer rights. Without enhancement of technology and the help of tech tools to flag such practices, the regulatory bodies will not be able to keep up their pace with the evolving wrongful acts exercised by developers. AI tools can scan millions of websites to

[30] Supra note 9
[31] Consumer Protection Act, 1986, No. 68, Acts of Parliament, 1986 (India).

identify non-compliant activities, saving time and resources of the regulatory authorities. However, there is no room for complacency as the technology for misuse also keeps evolving and is dynamic in nature.

Conclusion

Dark patterns in digital markets pose a significant threat to consumer autonomy, trust, and fair competition. These deceptive design tactics exploit cognitive biases, making it difficult for users to make informed choices about their data, subscriptions, and purchases. While the growing awareness of dark patterns has led to regulatory interventions across jurisdictions, enforcement remains a challenge.

Technological advancements will continue to evolve, leading to new forms of manipulation. Thus, policy interventions should be dynamic, adapting to emerging dark patterns while ensuring businesses remain accountable. Consumer education and digital literacy campaigns are equally crucial in empowering individuals to recognize and resist deceptive online tactics.

A harmonized global response, fostering cooperation among regulatory bodies, is necessary to tackle dark patterns that transcend borders. Companies that prioritize ethical design, transparency, and user-centric practices will gain long-term consumer trust, while those relying on manipulation risk legal action and reputational damage.

Ultimately, addressing dark patterns is not merely a legal challenge but a moral one. Digital markets should be designed to respect consumer agency rather than exploit vulnerabilities. By strengthening regulations, enforcing compliance with the aid of technology and top-down executive approach, while raising awareness amongst the consumers, we can ensure that the digital economy remains fair, competitive, and consumer-friendly.