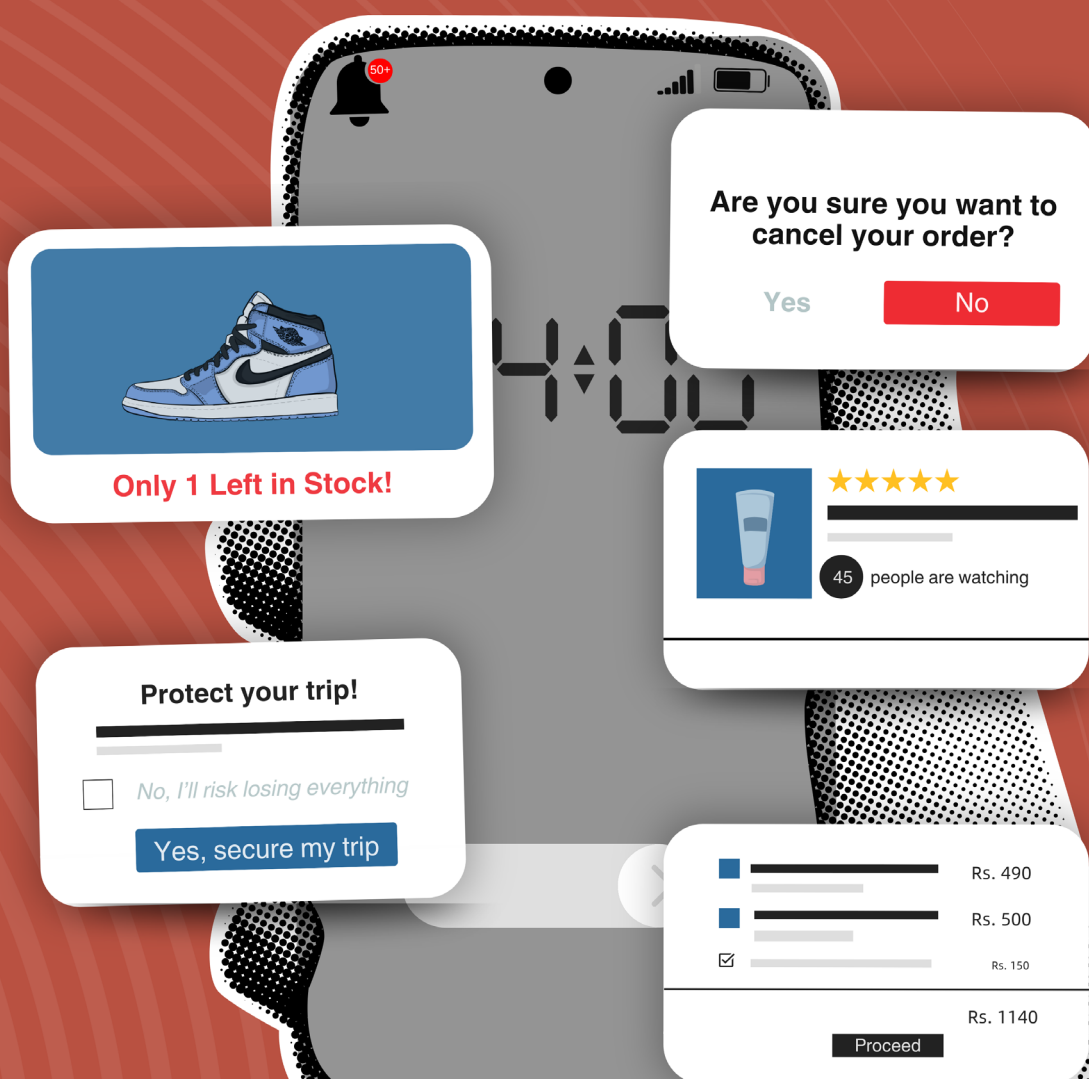


Prime[D] to Buy

Flash Sales & Deceptive Design



By Farheen and Ananyah Kilari

Center For Law And Critical Emerging Technologies,
Advanced Study Institute Of Asia (ASIA)

December 2024

CONTENTS

Acknowledgement.....	1
Executive Summary	2
1. Introduction	5
1.1 Background	5
1.2 What are Deceptive design (Dark Patterns)?	6
1.2.1 Why Deceptive design Work?	6
1.3 Why Flash Sales?	8
1.4 Objective of The Report	8
2. Methodology	10
2.1 Content Analysis framework.....	10
2.2 Limitations.....	13
3. How Platforms Use Deceptiv Design	14
3.1 Overview	14
3.2 Types of Deceptive Design Observed	15
3.3 Industry Wise Deceptive Design	20
3.4 Deceptive Price Strategies	21
3.5 When Persuasion Becomes Manipulation	22
3.6 Where Do These Deceptive Design Appear?	25
3.7 Impact on the User	26
4. Current Regulation	28
4.1 Overview of The Existing Legal Framework on Deceptive Design	28
4.2 Regulatory Challenges in Addressing Deceptive design	32
5. Conclusion.....	35
6. References	37

Acknowledgement

We extend our heartfelt gratitude to the Board of Directors of the Advanced Study Institute of Asia (ASIA) for their unwavering support, which has been crucial to this report. Special thanks to Prof. Amogh Dev Rai for his guidance, Neeti Gautam and Priyanka Garodia for their insightful reviews, and Raghav Sibal, and Ananyah Kilari for their design contributions. Additionally, Ananyah's data compilation and efforts were instrumental in shaping this work. We also acknowledge the scholars and experts whose foundational research in behavioural science, digital consumer practices, and regulatory frameworks enriched our understanding of dark patterns and consumer behaviour. This report builds upon their invaluable contributions and the collaborative spirit of academic research. This effort was led by Farheen Yousuf under the guidance of Prof. Amogh Dev Rai.

Centre for Law and Critical Emerging Technologies at ASIA

The Centre focuses on understanding the vulnerabilities and challenges posed by rapidly evolving and interconnected technologies, addressing their security, political, and ethical implications. Recent initiatives include the Progress and Policy Roundtable on Standard Essential Patents (SEPs) and research projects like the Quantum Index, fostering global collaboration and innovation through policy-focused discussions and working papers.

The Advanced Study Institute of Asia (ASIA), established in 2023 and affiliated with Shree Guru Gobind Singh Tricentenary University in Gurugram, India, serves as an interdisciplinary research center dedicated to enhancing the understanding of Asia, particularly South Asia.

Executive Summary

India, with over 900 million internet subscribers, ranks second globally in digital adoption (TRAI, 2024; ICUBE, 2023). The government's "Digital India" initiatives and the Digital Payment Index (DPI) have fostered a vibrant digital financial ecosystem, evident in the impressive rise of digital transactions, particularly through the Unified Payments Interface (UPI), which processed nearly 17 billion transactions in October 2024 (National Payment Corporation of India, 2024). However, this growth raises significant consumer protection concerns.

The Reserve Bank of India (RBI) highlighted the use of "deceptive design" in its 2024 Currency and Financial Report, where digital services manipulate consumer decisions (Report on Currency and Finance 2023-24, 2024). In response, the Central Consumer Protection Authority (CCPA) outlined 13 types of deceptive design in November 2023. Yet, a 2024 survey showed that such manipulative designs are found in 79% of apps (ASCI Academy et al., 2024). These tactics can lead consumers into poorly understood decisions, risking financial stability, especially for vulnerable groups. The use of deceptive design is especially pronounced during high-traffic online periods, like festive flash sales, where urban Indian consumers are expected to spend ₹1.85 lakh crore (\$22 billion) in October 2024.

Given all this, we looked at 26 of the most used digital platforms spanning a range of sectors—including e-commerce, fintech, and travel—all during the grand sales season in October 2024. Here are the main findings of this research, as stated in the report:

Main Findings:

26/26

All the analysed digital platforms used an average of 5 dark patterns.

12%

Analysis of 25 product prices across one platform showed Iphone users paid more, on average, than the Android users.



E-commerce websites used the most dark patterns, followed by quick commerce, travel booking, payment platforms, and gaming platforms.

111%

Flash sales inflate savings by over 100%, but actual discounts are often minimal—just 6% on average.



Flash sales are a hotspot for manipulative tactics, using cluttered designs, false urgency, and data-driven targeting to exploit users, who are susceptible to drive impulsive decisions.



Regulatory frameworks address general deceptive practices but lack specific provisions for emerging patterns observed during flash sales, highlighting a need for focused oversight.



Grab offers on your 1st purchase



FLAT
₹300 OFF

ON ORDERS
ABOVE ₹990

USE CODE:

NEW300

FLAT
₹500 OFF

ON ORDERS
ABOVE ₹2590

USE CODE:

NEW500

FLAT
₹1000 OFF

ON ORDERS
ABOVE ₹4990

USE CODE:

NEW1000

+ ZERO DELIVERY FEE

1. Introduction

1.1 BACKGROUND

Over the past ten years, India's digital transformation has accelerated rapidly due to factors like growing internet access, the proliferation of smartphones, and affordable data plans. About 936 million people in the nation had internet access as of March 2024, and 350 million of those users were actively transacting online (Press Information Bureau, 2024). Consumer behaviour has been greatly impacted by this increase in connectivity, especially in the e-commerce industry.

India's e-commerce market has grown swiftly, with projections indicating that it will reach USD 116 billion by 2023. The market is predicted to reach USD 111.40 billion by 2025, continuing on its current growth trajectory (Statista, 2023; India E-Commerce Market Size, 2024). During the holiday season, when there are significant sales events like Flipkart's "Big Billion Days" and Amazon's "Great Indian Festival," this expansion is particularly noticeable. Millions of customers nationwide are drawn to these events because they provide significant discounts and special offers. With credit card transactions totalling ₹2.01 trillion in October 2024—a 13% year-over-year increase over October 2023—consumer credit has also increased dramatically (Reserve Bank of India, 2024). This suggests that during this time, people are depending more and more on credit for festive purchases.

But this expansion is also accompanied by a rise in the use of deceptive design, which are deceptive design strategies that influence users' choices and frequently lead to unintended purchases or actions. The festive season is a prime time for such manipulative tactics because of the competitive nature of the digital marketplace and the high volume of consumer traffic. Addressing the moral ramifications of deceptive design is essential to protecting consumers and preserving confidence in the online marketplace as India's e-commerce industry grows.

1.2 WHAT ARE DECEPTIVE DESIGN (DARK PATTERNS)?

The Central Consumer Protection Authority (CCPA) of India, in its Guidelines for Prevention and Regulation of Dark Patterns, 2023, defines it as:

“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.

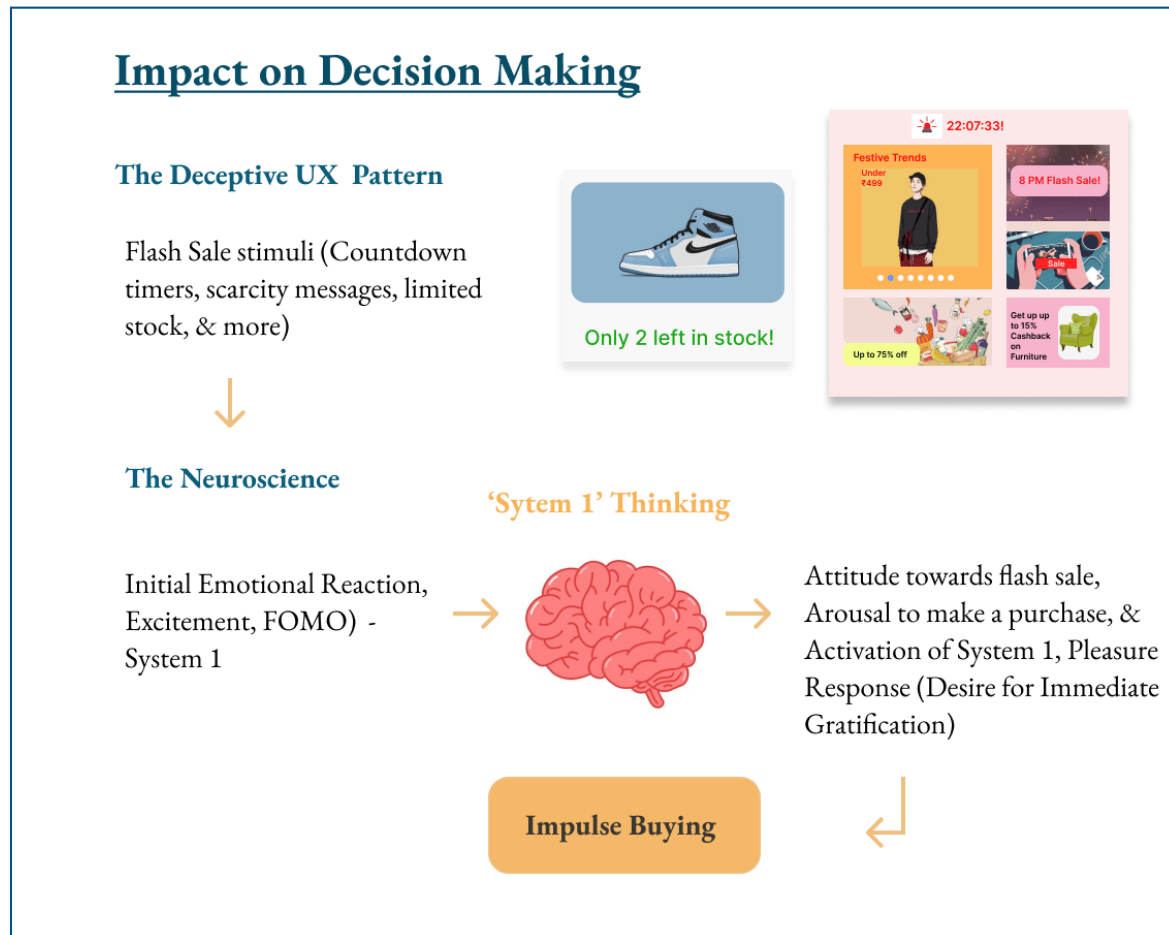
These practices often manifest in common scenarios like hidden costs during the checkout process, confusing subscription cancellation processes, or fake urgency tactics, such as countdown timers that pressurise users to make immediate decisions.

The primary distinction between deceptive design and legitimate persuasive design lies in the purpose and intended beneficiary. While nudges are often employed to help users make decisions that align with their long-term interests, deceptive design solely benefit the service provider by distorting or undermining the consumer’s ability to make an informed and voluntary choice (Brignull, 2018; Nouwens et al., 2020).

1.2.1 WHY DECEPTIVE DESIGN WORK?

Deceptive design are particularly effective because they are designed to exploit System 1 thinking, the automatic and intuitive mode of human decision-making (Kahneman, 2011). This mode is driven by psychological triggers like loss aversion, urgency bias, and social proof (Stanovich & West, 2000). For instance, phrases such as “only 1 left!” trigger urgency and scarcity bias, leading users to make quick, emotion-driven decisions without considering the long-term consequences.(Luguri & Strahilevitz, 2020). Similarly, the default effect, where pre-selected options (such as opting in for additional services or subscriptions) are hard to change, leads users to passively accept conditions they may not have consciously chosen.

These designs, which increase impulse buying, also reduce consumer satisfaction over time, as users often regret purchases made under pressure (Nilsson, 2022).



Created based on Liu et al. (2019), Vannisa et al.(2020), Y. Wu et al. (2020), Frederick et al. (2009) and Lamis et al. (2022)

From a decision-making perspective, the manipulative nature of deceptive design causes a shift from rational, deliberate choices (System 2) to faster, less controlled ones (System 1). This shift is particularly concerning in contexts where consumers might overspend, share excessive data, or commit to services they do not need (Di Geronimo et al., 2020). The impact extends beyond financial consequences, as users may feel deceived, eroding trust in digital platforms (Gerber et al., 2023). Research also shows that deceptive design can exacerbate economic and social inequalities, disproportionately affecting users with lower digital literacy or socioeconomic vulnerability

(Luguri & Strahilevitz, 2021).

These manipulative tactics are not limited to e-commerce alone; they extend to various digital services, including social media, financial services, and online privacy settings, affecting consumer autonomy in decision-making. As digital markets grow, the prevalence of deceptive design has become a global concern, prompting regulatory responses from bodies like the European Data Protection Board (EDPB), Central Consumer Protection Authority (CCPA) in India, and the Federal Trade Commission (FTC) in the US, which aim to protect user rights and foster trust in digital environments.

1.3 WHY FLASH SALES?

Flash sales differ from typical sales in that they are time-sensitive, with big reductions available for a limited time. This urgency capitalises on customer behaviour by encouraging impulsive decision-making, as demonstrated by platform studies (Mathur et al. 2019). Unlike traditional sales, which allow for more contemplation, flash sales thrive on instilling an immediate “fear of missing out” (Shi & Chen, 2015). This method frequently leads to speedy purchasing decisions, which benefits e-commerce platforms by increasing traffic and sales volume. This is consistent with previous research, which has found that an ecommerce dark pattern leads to inadvertent consumption (Koh & Seah, 2023). As a result, the bundle of deceptive patterns during the peak of flash sales appears to be a hotspot for manipulative design.

1.4 OBJECTIVE OF THE REPORT

This report aims to study the use of deceptive design during India’s festive flash sales, a period characterised by heightened consumer participation and heavy reliance on digital platforms. The focus is on distinguishing between ethical persuasion and manipulative practices, particularly how deceptive design breach ethical boundaries in e-commerce. Ethical persuasion enables informed decision-making by presenting clear and truthful information, aligning with consumer interests. In contrast, manipulation distorts user choice by obscuring critical details or creating deceptive narratives

(Thaler & Sunstein, 2008; Spencer, 2020). The global relevance of this issue is underscored by a recent study of 11,000 websites, which revealed that approximately 183 employed deceptive design. This demonstrates how pervasive such manipulative design tactics are, further highlighting the need to examine their specific prevalence and impact within India's unique context of flash sales (Mathur et al., 2019).

In this report we do the following:

- Identify the most common deceptive design.
- Analyse how frequently they appear, especially during sales events.
- Review existing regulations to see how well they address these tactics.

2. Methodology

This report employs a content analysis framework inspired from insights into how deceptive design are identified, categorised, and analysed in prior research (Gray et al., 2023), the study examines their use and impact on Indian e-commerce platforms during flash sales.

This methodological approach ensures the findings are aligned with best practices in the academic study of manipulative design.

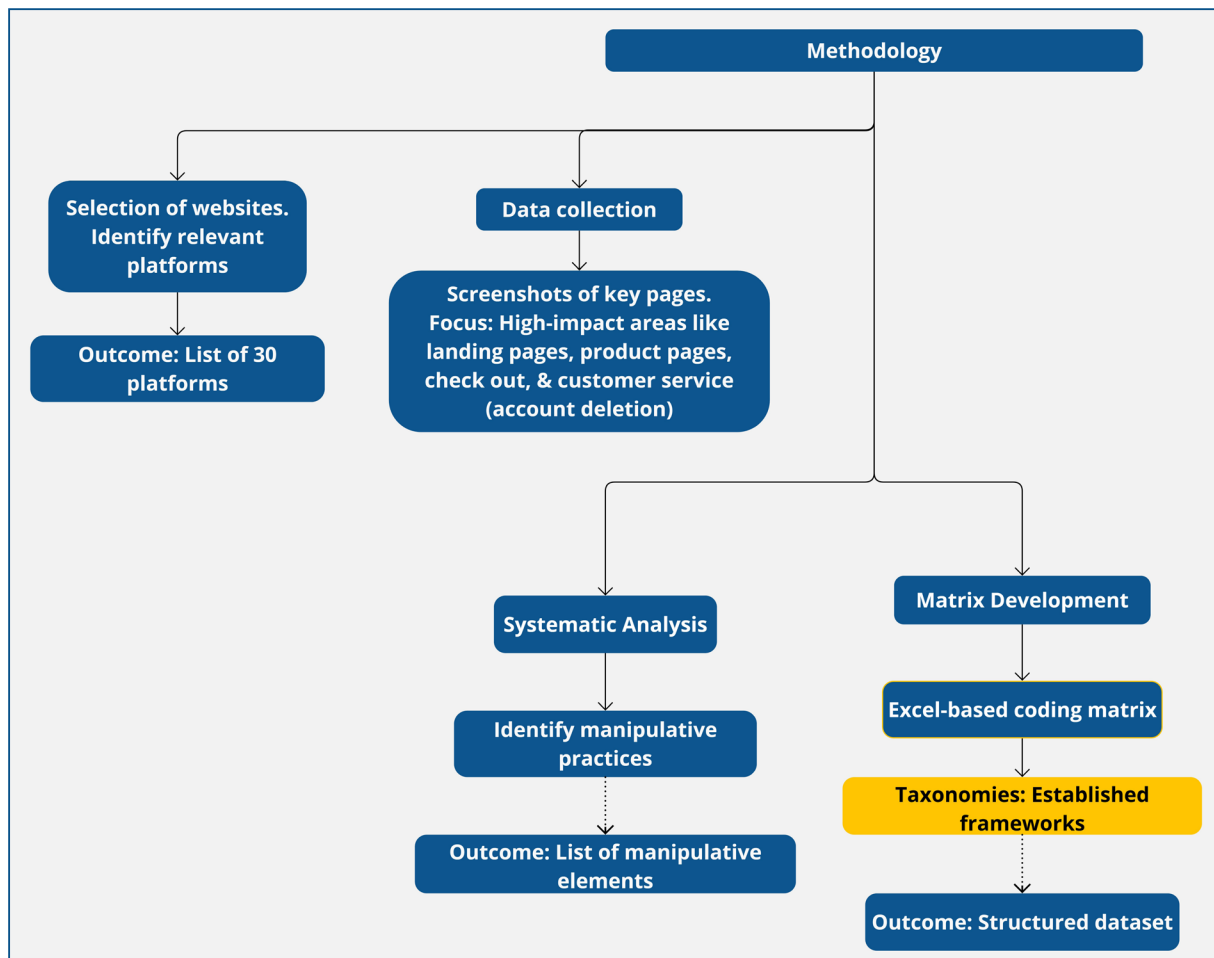
- **Scope:** The study examined 26 mobile applications, including both established e-commerce giants (e.g., Amazon, Flipkart) and emerging players across sectors such as fintech, travel, and gaming.
- **Rationale:** Platforms were selected based on their popularity during festive periods, ensuring relevance to consumer behaviour and flash sale events.

2.1 CONTENT ANALYSIS FRAMEWORK

Content analysis served as the primary method to investigate deceptive design, guided by existing literature(Gray et al., 2023). This method ensures a comprehensive examination of visual and textual elements on platforms during flash sales. The study followed a structured protocol:

- 1.**Platform Selection:** Chose platforms based on popularity during festive periods, including both established and emerging players.
- 2.**Data Collection:** Captured screenshots and recordings of interfaces during flash sales.
- 3.**Rapid Systemic Assessment:** Created a matrix based on existing taxonomy of deceptive design and categorised identified practices in the matrix. This approach mirrors academic studies that assess how visual and structural elements influence user decision-making under pressure.

4. Validation: The findings were compared with existing literature to validate and contextualise the results.



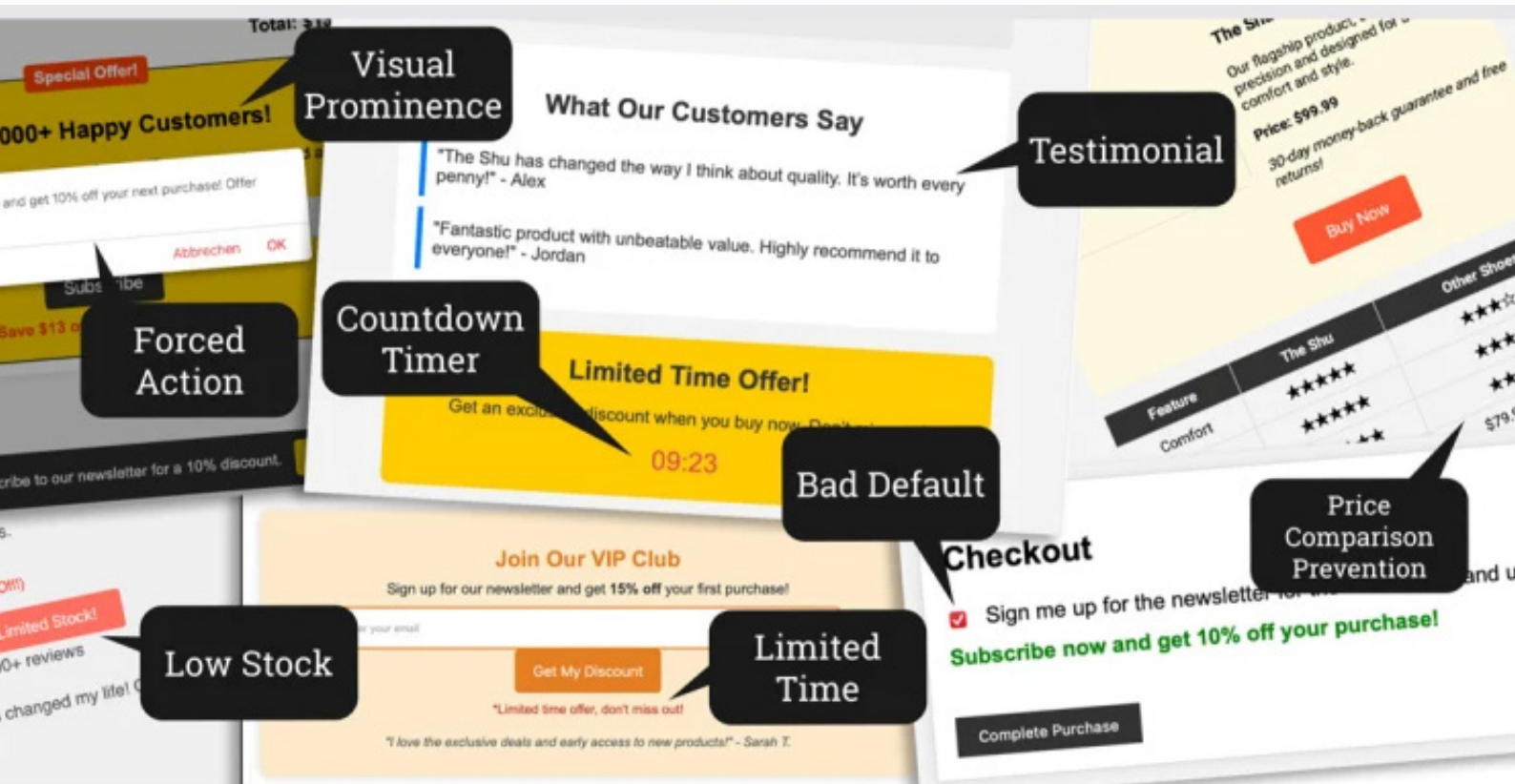
Taxonomy of Deceptive Design

Category	Variant	Description	Source
Nagging		Repeated requests to do something the firm prefers	Gray et al. (2018)
Social proof	Activity messages	False/misleading Notice that others are purchasing, contributing	Mathur et al. (2019)
	Testimonials	False/misleading positive statements from customers	Mathur et al. (2019)
Obstruction	Roach motel	Asymmetry between signing up and canceling	Gray et al. (2018) , Mathur et al. (2019)
	Price comparison prevention	Frustrates comparison shopping	Brignull (2020) , Gray et al. (2018) , Mathur et al. (2019)
	Intermediate currency	Purchases in virtual currency to obscure cost	Brignull (2020)
	Immortal accounts	Account and consumer info cannot be deleted	Bösch et al. (2016)
Sneaking	Sneak into basket	Item consumer did not add is in cart	Brignull (2020) , Gray et al. (2018) , Mathur et al. (2019)
	Hidden costs	Costs obscured/disclosed late in transaction	Brignull (2020) , Gray et al. (2018) , Mathur et al. (2019)
	Hidden subscription/forced continuity	Unanticipated/undesired automatic renewal	Brignull (2020) , Gray et al. (2018) , Mathur et al. (2019)
	Bait and switch	Customer sold something other than what's originally advertised	Gray et al. (2018)
Interface interference	Hidden information/aesthetic manipulation	Important information visually obscured	Gray et al. (2018)
	Preselection	Firm-friendly default is preselected	Bösch et al. (2016) , Gray et al. (2018)
	Toying with emotion	Emotionally manipulative framing	Gray et al. (2018)
	False hierarchy/pressured selling	Manipulation to select more expensive version	Gray et al. (2018) , Mathur et al. (2019)
	Trick questions	Intentional or obvious ambiguity	Gray et al. (2018) , Mathur et al. (2019)
	Disguised ad	Consumer induced to click on something that isn't apparent ad	Brignull (2020) , Gray et al. (2018)
	Confirmshaming	Choice framed in a way that makes it seem dishonorable, stupid	Brignull (2020) , Mathur et al. (2019)
	Cuteness	Consumers likely to trust attractive robot	Cherie & Catherine (2019)
	Friend spam/social pyramid/address book leeching	Manipulative extraction of information about other users	Brignull (2020) , Bösch et al. (2016) , Gray et al. (2018)
	Privacy Zuckering	Consumers tricked into sharing personal info	Brignull (2020) , Bösch et al. (2016) , Gray et al. (2018)
Forced action	Gamification	Features earned through repeated use	Gray et al. (2018)
	Forced Registration	Consumer tricked into thinking registration necessary	Bösch et al. (2016)
Scarcity	Low stock message	Consumer informed of limited quantities	Mathur et al. (2019)
	High demand message	Consumer informed others are buying remaining stock	Mathur et al. (2019)
Urgency	Countdown timer	Opportunity ends soon with blatant visual cue	Mathur et al. (2019)
	Limited time message	Opportunity ends soon	Mathur et al. (2019)

(Luguri & Strahilevitz, 2020)

2.2 LIMITATIONS

1. **Sample Size:** The study covers 26 mobile applications, which may not represent all e-commerce platforms or niche markets.
2. **Temporal Scope:** Data was collected during festive sales, potentially missing patterns outside this period.
3. **Subjectivity:** Identifying deceptive design involves some subjective interpretation despite using a systematic framework.
4. **Static Data:** Screenshots capture only specific moments, missing dynamic changes in design or promotions.
5. **Consumer Behaviour:** The study analyses interfaces but does not measure actual consumer responses or actions.
6. **Regional Context:** Findings are specific to India and may not generalise globally due to cultural and regulatory differences.



[Image: Krauß et al./arXiv]

3. How Platforms Use Deceptiv Design

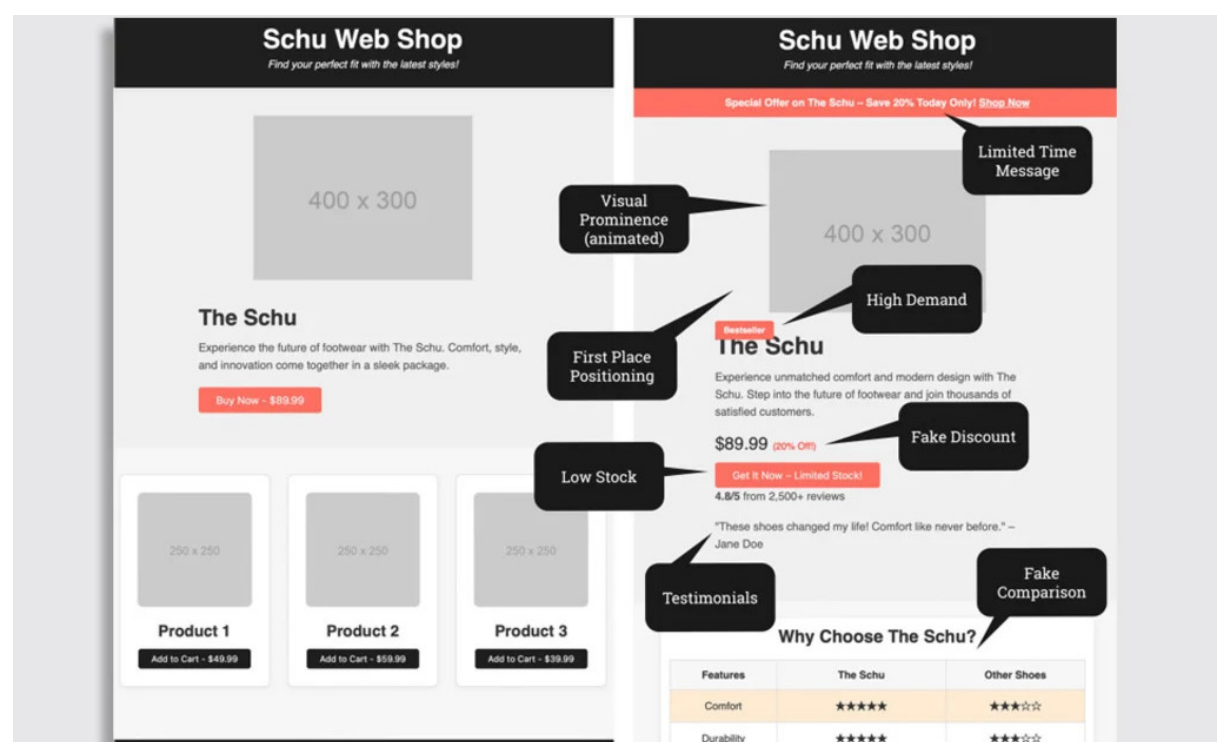
3.1 OVERVIEW

135
Instances of
Deceptive Patterns

A total of 135 deceptive patterns were identified across platforms, showcasing deliberate strategies to manipulate user decisions.

26/26
Platforms Using
Deceptive Tactics

Every one of the 26 apps we analysed employed at least one deceptive design element to influence user behaviour.



[Image: Krauß et al./arXiv]

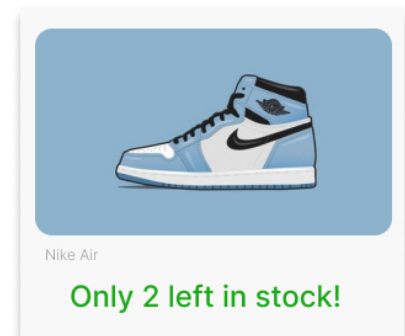
3.2 TYPES OF DECEPTIVE DESIGN OBSERVED

1. Scarcity

Scarcity refers to deceptive patterns that create a false sense of limited availability to compel users to act quickly. This category of dark patterns can manipulate user behaviour by exploiting cognitive biases related to scarcity and urgency.

False Low Stock Messages

2.22%



2. Urgency

Urgency is a dark pattern that manipulates users by creating a sense of time pressure, making them believe they must act immediately or risk losing out. This tactic often exploits psychological triggers like loss aversion and fear of missing out (FOMO), pushing users into making decisions they might otherwise reconsider.

False High Demand messages

Fake Countdown Timers

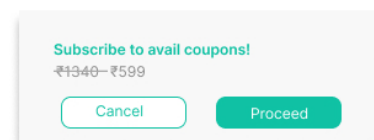
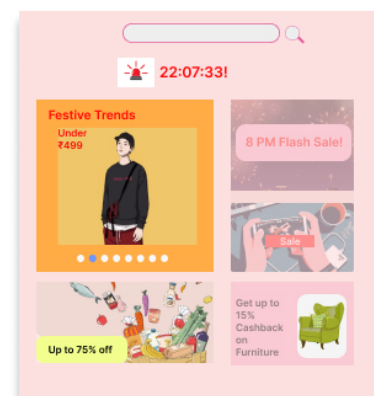
Fear Of Missing Out

Loss Aversion

Limited Time Deals

Coupon Incentives

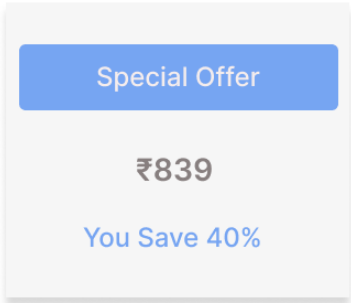
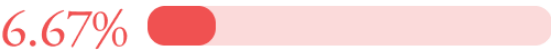
39.26%



3. Obstruction

Obstruction as a dark pattern complicates user actions intentionally. Examples include the "Roach Motel," where signing up is easy but cancelling is difficult, and "Immortal Accounts," which prevent permanent account deletion. Price comparison prevention hides unit prices, while the "Privacy Maze" buries data settings deep in menus, discouraging user adjustments.

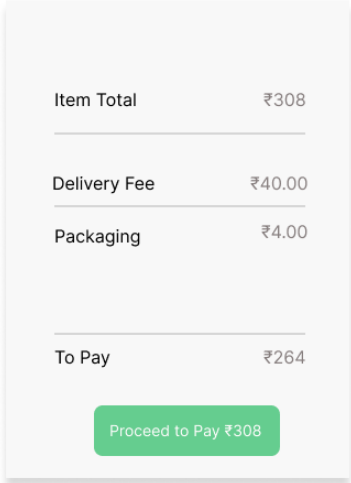
- Roach Motel
- Immortal Accounts
- Privacy Maze



4. Sneaking or Information Hiding

Sneaking as a dark pattern involves deceptive practices that mislead users during transactions. Examples include sneakily adding items to the cart that the consumer did not select, revealing hidden costs late in the purchase process, or using hidden subscriptions where automatic renewals occur without clear consent. Another tactic is bait and switch, where customers are offered one product but end up with something different than originally advertised.

- Price Comparison Prevention
- Hidden Costs/ Hidden Subscription
- Bait & Switch
- Drip Pricing

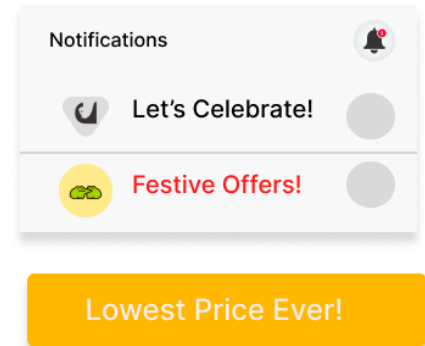


5. Interface Interference

Interface interference manipulates users by design tricks like disguised ads posing as content, pre-selected options nudging unwanted choices, confusing toggles for opt-outs, and misdirection hiding alternatives to favour preferred actions.

Misdirection
False Hierarchy
Visual Interface
Nagging

20.74% 

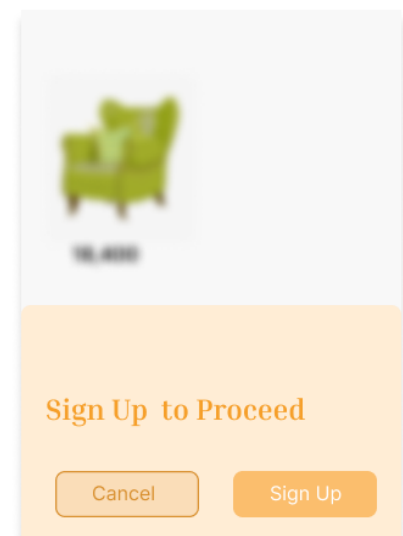


6. Forced Action

Forced action compels users to perform undesired tasks to proceed. Examples include mandatory account creation before checkout, requiring consent to excessive permissions for app use, or forcing users to complete surveys before accessing content.

Unauthorised Transactions
Forced Registration

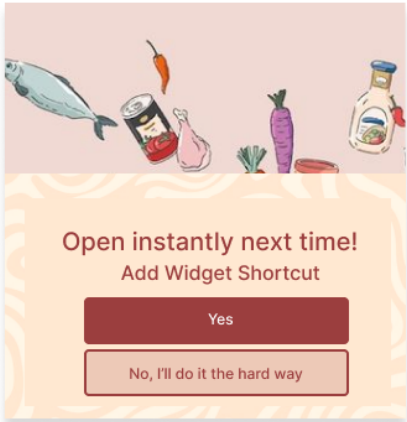
4.44% 



7. Asymmetric Choice

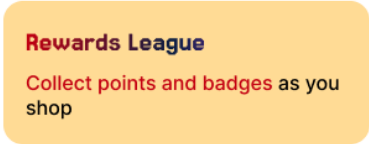
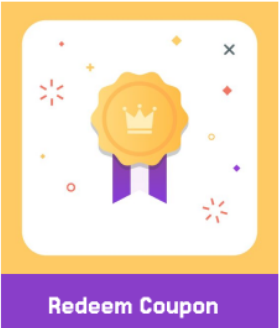
Asymmetric choice refers to deceptive strategies that manipulate decision-making processes by presenting options in a manner that triggers shame/discomfort or selecting the action by default for the user. This category of dark patterns can significantly influence user choices by manipulating the way options are displayed and presented.

Confirm Shaming
Pre-selection



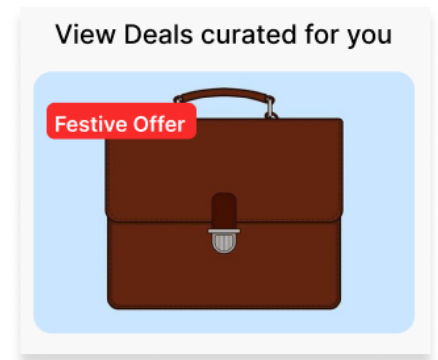
8. Gamification

Gamification involves incorporating game-like elements into non-game contexts to encourage user engagement and behavior. While gamification can enhance user experience, it can also be manipulated as a deceptive pattern that exploits users' motivations and biases.



9. Personalisation

Personalisation tailors user experiences using individual data, but it becomes a dark pattern when it misleads or exploits users without transparency. Examples include manipulative product recommendations during flash sales, re targeted ads, or tailored emails and texts with deceptive limited-time deals.



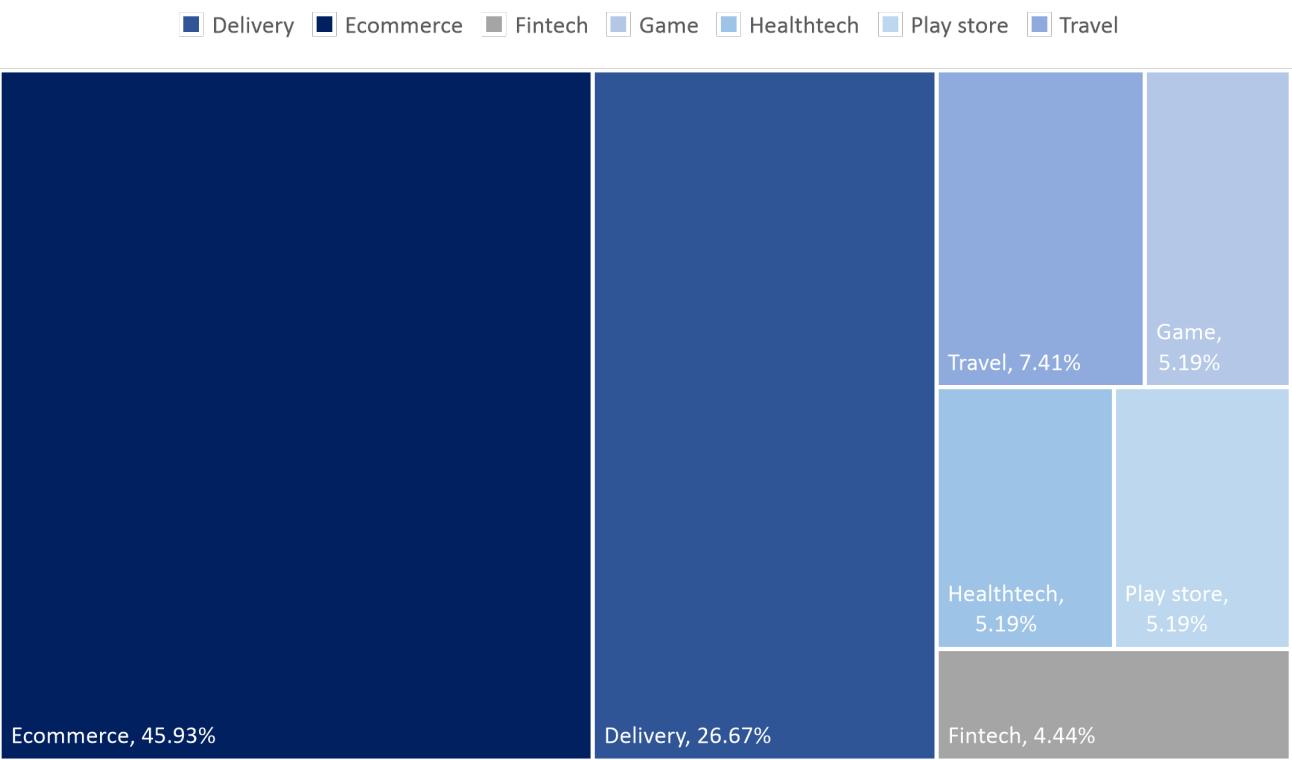
3.70%

- Inbox caro, let's reunite. Come back for unlimited entertainment. - Now on **Netflix** More TV
- Inbox caro, we have a plan for every budget—as low as \$6.99 a month - Now on **Netflix** Enjoy
- Inbox caro, Love Is Blind Season 4 is now on **Netflix** - Now on **Netflix** Season 4 <https://www.netflix.com/title/80057281>
- Inbox 😞 caro, give us another chance? We've got thousands of new TV shows and movies
- Inbox caro, Shadow and Bone Season 2 is now on **Netflix** - Now on **Netflix** | Shadow and Bone
- Inbox caro, we have a plan for every budget—as low as \$6.99 a month - Now on **Netflix** Enjoy
- Inbox We're ready when you are, caro. Come back to your favorite shows and movies. - Netflix

A cancelled Netflix account flooded with emails urging a return, spotlighting invasive and questionable data practices. Image credit: Thepudding.cool

3.3 INDUSTRY WISE DECEPTIVE DESIGN

Prevalance of Deceptive Patterns per Category

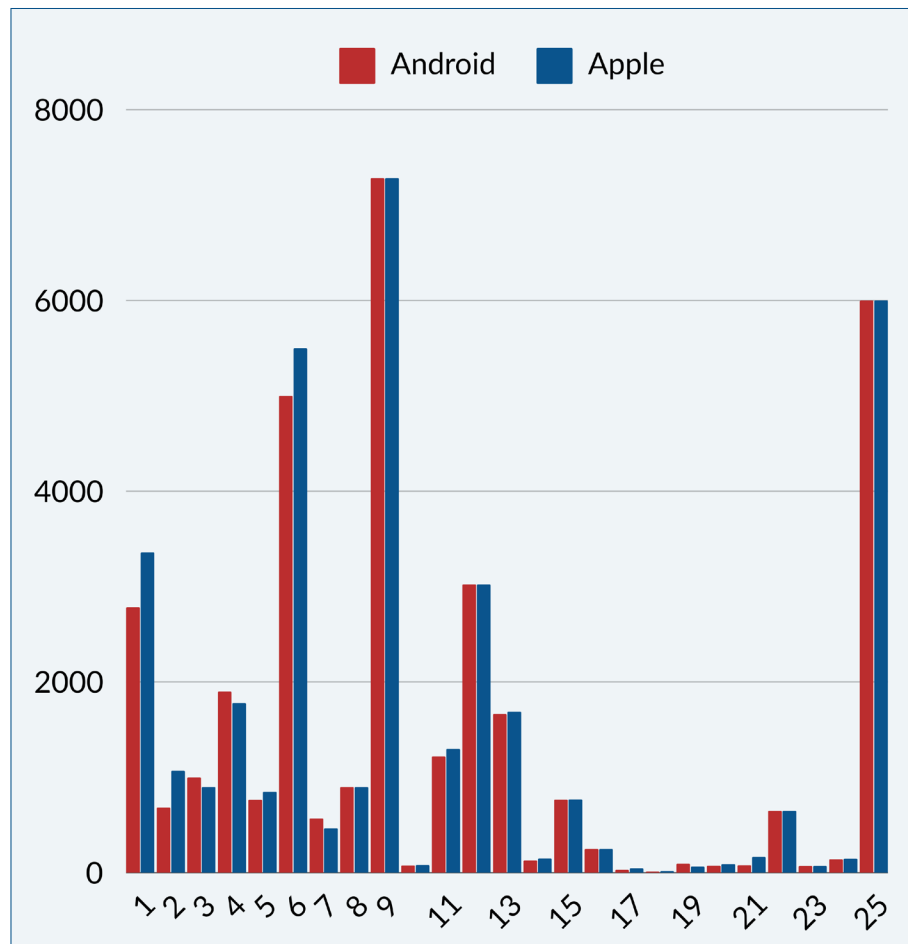


Our analysis of dark pattern prevalence across different app categories reveals significant variation, with certain sectors more prone to employing these manipulative design tactics. E-commerce apps lead the chart, constituting 45.93% of observed deceptive design. This high percentage underscores the sector’s emphasis on tactics that drive consumer urgency and impulsive purchasing decisions, such as countdown timers, limited stock notifications, and deceptive discount claims. Following e-commerce, delivery apps account for 26.67% of dark pattern instances, often using prompts and notifications to encourage continuous use and quick transactions. Travel apps make up 7.41%, frequently deploying strategies like fluctuating prices to create a false sense of urgency for bookings. Smaller percentages were observed in fintech (4.44%), gaming (5.19%), healthtech (5.19%), and the Play Store category (5.19%), which also feature design elements aimed at user retention, subscription enrolment, and micro-transactions.

3.4 DECEPTIVE PRICE STRATEGIES

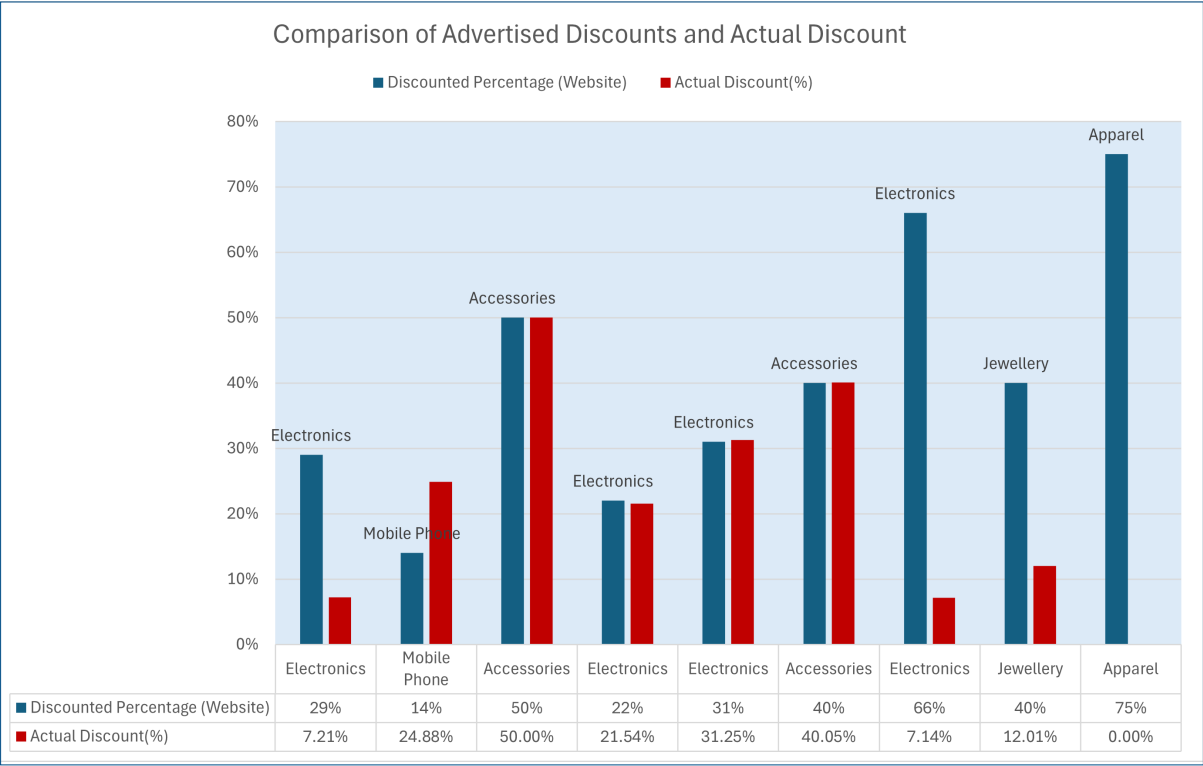
Based on our analysis, Apple app users pay approximately 12% more than Android users for the same products.

This finding aligns with research indicating that platform differences, such as Apple's higher-income user base and perceived brand premium, can lead to significant price disparities (Smith & Telang, 2018; Gefen & Straub, 2020). Studies show that pricing strategies may target Apple users differently, attributing higher willingness to pay due to Apple's distinct market positioning (Zeng et al., 2022).



For each product, we checked the highest price it had been sold for before and compared it to the advertised and actual discounts. Here's what we found: the real discounts were small, only 6.27% lower than the usual prices. But the advertised discounts were hugely inflated—on average, they were exaggerated by 111.34% to make the deals look better than they

actually were. For example: A product claimed a 40% discount, but when we checked, the actual price reduction was only about 12%. This kind of overstatement happened across the products we studied.



These findings suggest the importance of monitoring platform-based pricing strategies to avoid deceptive practices. For regulators and consumer advocates, addressing differential pricing mechanisms becomes essential to ensure that all users are aware of and understand pricing decisions, fostering a fairer and more transparent e-commerce environment.

3.5 WHEN PERSUASION BECOMES MANIPULATION

In recent years, India’s festive season has transitioned from traditional in-store shopping to a predominantly digital experience. This transformation is driven by increased digital adoption, widespread smartphone use, and aggressive marketing strategies by e-commerce platforms that have embedded the concept of “flash sales” into consumer culture. The result is not merely a rise in online sales but a fundamental change in consumer behavior, characterised by urgency, emotional intensity, and a higher willingness to spend. For instance, during the 2024 festive season,

urban India is projected to spend approximately ₹1.85 lakh crore (around \$22 billion), highlighting the massive surge in digital transactions and consumer engagement during this period (Forbes India, 2024).

Against this backdrop, this report's findings reveal a concerning issue:

“All 26 shopping apps analysed exhibited some form of deceptive design”.

As per our analysis, homepages are noisier during flash sales. Typically, landing pages and screens are kept simple and streamlined to encourage target users to take specific actions that drive conversions. However, during flash sale events, these landing pages often adopt more cluttered and chaotic interfaces, which can be overwhelming and challenging for users to navigate. The interface employs an extensive use of warm colours, strategically intended to draw users' attention to key visual elements, particularly the call-to-action (CTA) to buy. However, this approach inadvertently creates cognitive overload due to the lack of a clear visual hierarchy, resulting in an overstimulation of the user. Consequently, the overuse of warm tones leads to a disorganised experience that undermines the intended focus on critical actions. While not inherently deceptive, these practices raise ethical concerns about their potential impact on user autonomy and the ability to make informed choices.

These design strategies exploit cognitive biases and user vulnerabilities, manipulating individuals into actions they might not have taken if fully informed. While persuasive design is generally aimed at guiding users towards making informed decisions, flash sales cross a critical line from persuasion to manipulation. Persuasion leverages cognitive biases to nudge users gently, maintaining their autonomy. Manipulation, however, uses the same biases to coerce users into choices that may be against their best interests. During flash sales, the stakes are higher, both emotionally and culturally, making users more prone to coercive tactics masked as deals and limited-time offers. This manipulative approach taps into consumers' emotional investment in securing “exclusive” deals, leading to reactive decisions rather than informed choices. The pressure to seize “unmissable”

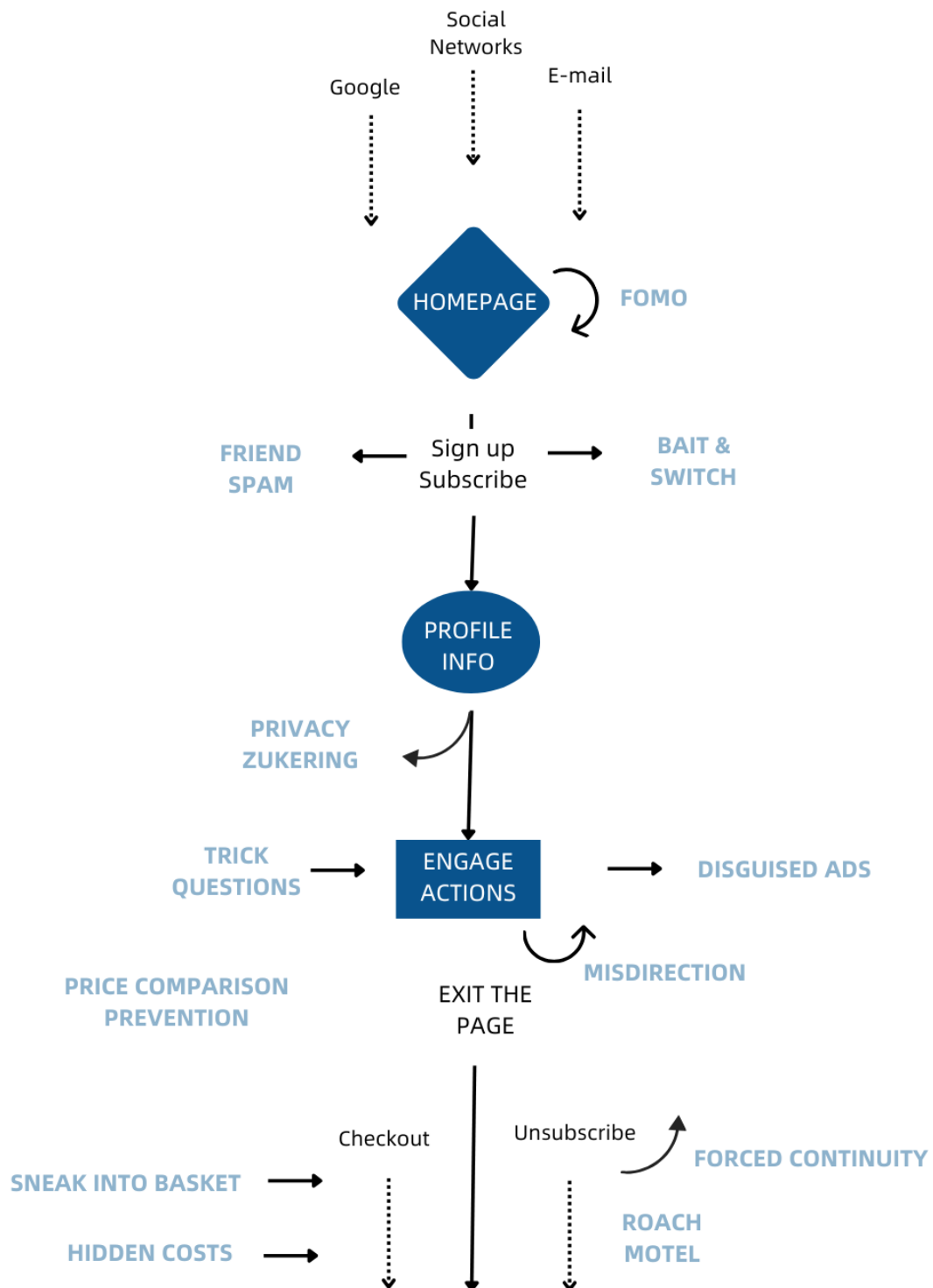
discounts and participate in cultural celebrations reduces critical thinking and decision-making time. This creates fertile ground for deceptive design to thrive, driving impulsive decisions that often result in financial overextension.

Moreover, flash sales often result in unplanned spending, which may cause missed payments, delayed EMIs, and debt accumulation. As per the Disney+ Hotstar Festive Shopping Sentiment Survey, consumer spending is expected to increase by 47% during such periods, putting more pressure on personal finances (Hotstar, 2024). This surge in spending, coupled with the manipulative design of shopping apps, can lead consumers to overextend financially, resulting in increased debt and economic vulnerability.

In short, the convergence of heightened consumer engagement during flash sales and the pervasive use of deceptive design by shopping apps creates an environment where consumers are more likely to make impulsive and financially detrimental decisions.

“The shift from persuasion to manipulation during this period is not just about increasing sales but actively exploiting consumer vulnerabilities at a time of heightened spending. This highlights the need for greater awareness and regulatory oversight to protect consumers from manipulative design practices, especially during periods of increased spending and vulnerability.”



3.6 WHERE DO THESE DECEPTIVE DESIGN APPEAR?

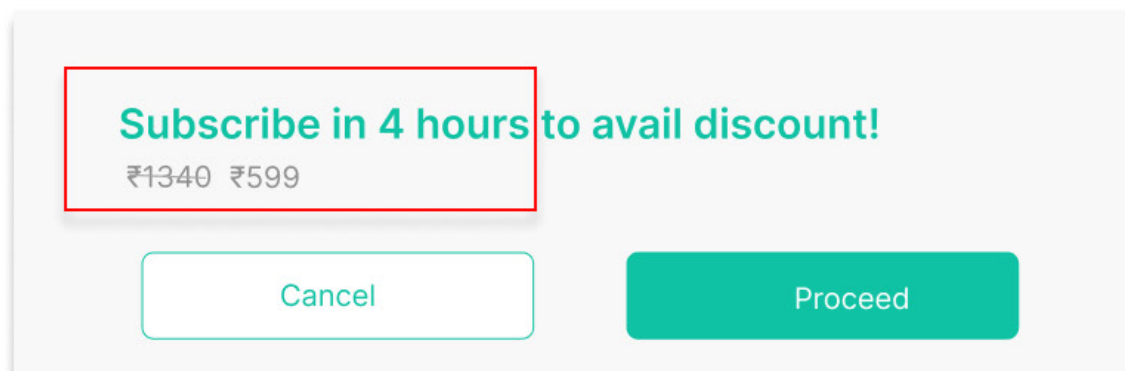
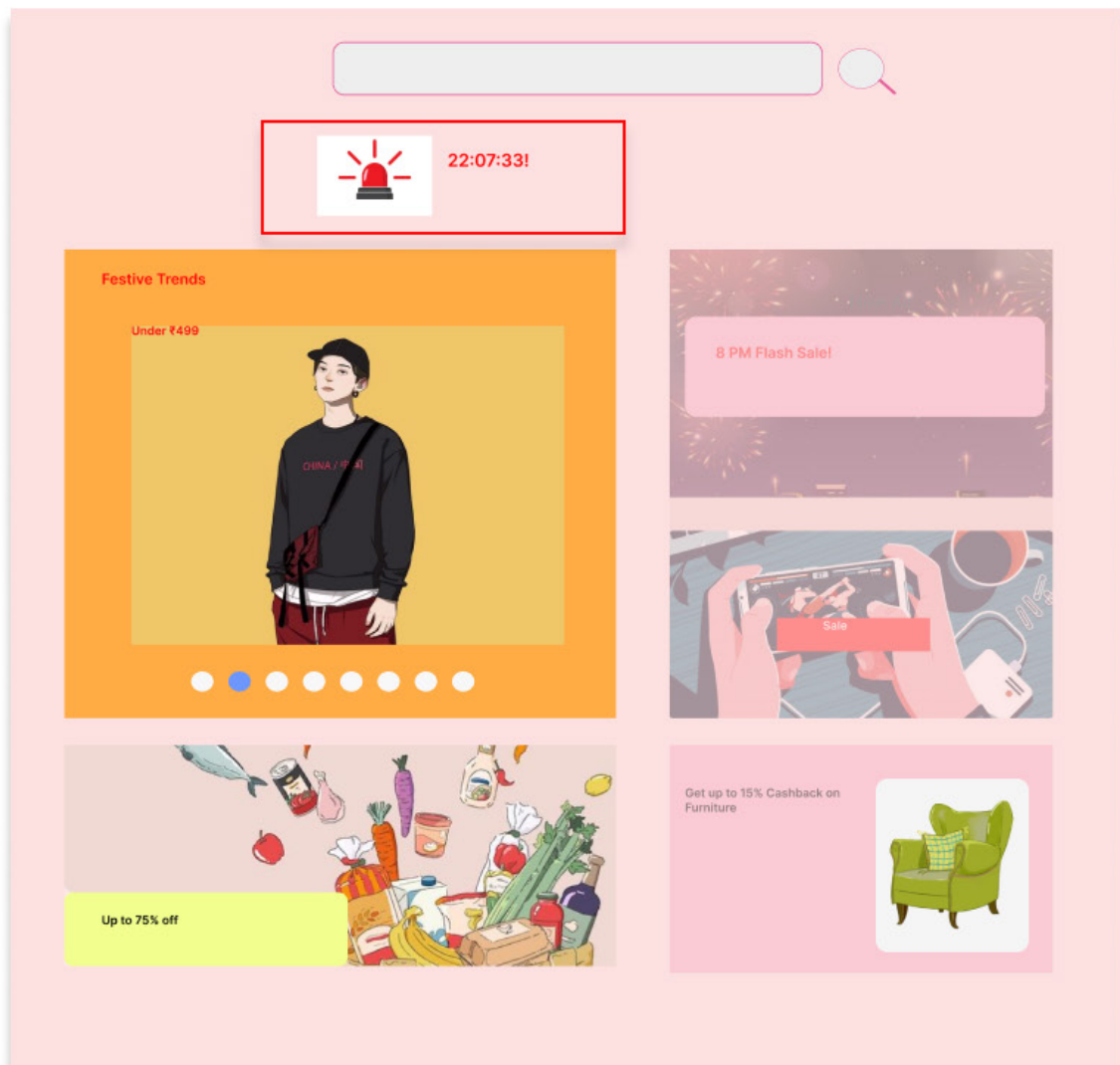


Recreated based on Ana Valjak's Design (Infinum)

3.7 IMPACT ON THE USER

The following table summarises the key psychological principles underlying major deceptive design observed in UX design and their impact on user behaviour during the festive season. It highlights how these patterns exploit cognitive biases to drive manipulative outcomes.

	<p>1. Unintended Consumption</p> <p>Dark patterns manipulate users into making unplanned purchases through tactics like confirmshaming or scarcity messages. Additionally, they waste users' time with deliberately convoluted processes.</p>
	<p>2. Psychological Impact</p> <p>Dark patterns cause psychological stress by exploiting cognitive biases, creating a sense of urgency, or introducing decision fatigue. This erodes user confidence, leading to frustration and dissatisfaction with the platform.</p>
	<p>3. Privacy Implications</p> <p>Dark patterns manipulate users into sharing personal information through misleading consent mechanisms or pre-checked options, often without clear awareness of the implications.</p>
	<p>4. Behavioural Market Failures</p> <p>By manipulating user behaviour, dark patterns disrupt efficient decision-making, pushing users into choices that are not in their best interest and distorting market dynamics.</p>
	<p>5. Market Trust Erosion</p> <p>Repeated exposure to deceptive practices erodes user trust in platforms, fostering scepticism and reducing long-term user engagement with digital services.</p>



Urgency: Creates time pressure to exploit FOMO and loss aversion, pushing users into hasty decisions.

4. Current Regulation

4.1 OVERVIEW OF THE EXISTING LEGAL FRAMEWORK ON DECEPTIVE DESIGN

Globally, only a few countries have introduced specific guidelines to regulate deceptive design. Leading the way are the Central Consumer Protection Authority (CCPA) in India, the Federal Trade Commission (FTC) in the USA, the European Data Protection Board (EDPB) in the European Union, and the Korean Fair-Trade Commission (KFTC) in South Korea. While these authorities all focus on online consumer protection, the FTC and EDPB also address issues related to data protection and consumer consent.

The guidelines issued by each authority have different scopes and structures:

- The FTC and EDPB function as broad regulatory bodies that set guidelines but depend on state or national authorities for enforcement.
- The CCPA and KFTC, on the other hand, play a dual role, both issuing and enforcing guidelines, indicating a more direct approach to regulating deceptive design.
- With the USA and EU showing more proactive cases like the FTC's \$245 million fine against Epic Games and a EUR 300k penalty in Italy based on EDPB guidelines. In contrast, the CCPA and KFTC have yet to showcase major enforcements, as their guidelines are relatively new and evolving.

The focus of prohibited practices also varies across these guidelines:

- The CCPA primarily targets consumer-centric manipulations such as basket sneaking and false urgency.
- The EDPB emphasises data transparency and user consent, addressing patterns like language discontinuity and conflicting information.

- The FTC and EDPB have specific transparency requirements related to consent and privacy, while the CCPA and KFTC currently lack explicit transparency provisions.

Table: Guidelines Across the World on Deceptive design

Country	India	European Union	Korea	USA
Regulatory Body	Central Consumer Protection Authority	European Data Protection Board	Korean Fair-Trade Commission	Federal Trade Commission
Publishing Date	November 2023	March 2022	September 2023	September 2022
Applicable Laws	Section 18, Consumer Protection Act, 2019	Chapter 2&3, General Data Protection Regulation (2016)	Personal Information Protection Act (PIPA), 2011 & e-commerce Act, 2019	Section 5, FTC Act, 2004
Enforcement Mechanism	Imprisonment of 6 months or a fine of up to INR 2 million (USD 24k) or both	Administrative fine up to EUR 20million (USD 21.5 million) or up to 4% of the total worldwide turnover of the preceding financial year, whichever is higher	Administrative fines up to 3% of total sales	Fines, Injunctions & Legal actions
Transparency Requirements	No specific requirements, but emphasis on disclosure	Detailed transparency requirements regarding data processing and rights of data subjects, under Article 5, 7, 12, 13 & 14	No specific requirements, but emphasis on disclosure	Clear and conspicuous of material terms and conditions
Updates & Amendments	No recent amendments or updates	Periodic revisions & amendments based on the evolving technology	Amendments & Updates through legislative process	Periodic updates & revisions based on upcoming issues

Table based on a Mamidwar et al. (2024) analysis

All four regulatory authorities incorporate a range of enforcement mechanisms, including administrative fines, legal actions, and injunctions. However, only the CCPA includes imprisonment as a possible penalty, highlighting a stricter punitive measure (Mamidwar et al., 2024). Approaches to updates also differ: the FTC mandates regular updates to address emerging issues, while the EDPB relies on periodic reviews of technological advancements. The CCPA and KFTC have not revised their guidelines, as they were recently introduced (Mamidwar et al., 2024).

Overall, while there is significant overlap, each authority's guidelines reflect specific regulatory priorities—such as data protection in the EU or consumer transparency in India and South Korea. The absence of comprehensive dark pattern guidelines in many other countries highlights the need for a more unified international approach that covers high-level patterns as well as complex, context-specific manipulations in digital interfaces.

Table 2: Comparison among National Guidelines on basis of Types of Deceptive design

High-Level Pattern	Meso-Level Pattern	Low-Level Pattern
Obstruction D: FTC CCPA KFTC I: EDPB	Roach Motel (D: FTC)	Immortal Accounts (D: FTC)
	Creating Barriers	Dead End (D: EDPB)
	Adding Steps (I: EDPB)	Price Comparison Prevention (D: FTC KFTC)
Sneaking I: FTC EDPB CCPA KFTC	Bait and Switch (D: FTC EDPB CCPA)	Privacy Maze (D: EDPB)
	Hidden Information	Disguised Ad (D: FTC CCPA KFTC)
		Sneak into Basket (D: FTC EDPB CCPA)
		Drip Pricing, Hidden Cost (D: FTC EDPB CCPA)
	(De)contextualizing Cues	I: KFTC
		Conflicting Information (D: EDPB I: CCPA)
Interface Interference D: CCPA KFTC I: FTC EDPB	Manipulating Choice Architecture	False Hierarchy (D: KFTC I: EDPB)
		Pressured Selling (I: FTC CCPA)
	Emotional or Sensory Manipulation (D: CCPA KFTC)	Positive or Negative Framing (I: EDPB CCPA KFTC)
	Trick Questions (D: FTC EDPB CCPA KFTC)	-
	Choice Overload (D: KFTC I: EDPB)	-
	Hidden Information (D: FTC KFTC I: EDPB)	-
Forced Action D: CCPA I: FTC KFTC	Language Inaccessibility Nagging (D: FTC CCPA)	Wrong Language (I: EDPB)
	I: EDPB KFTC	-
	Forced Continuity (I: FTC EDPB)	-
Social Engineering	Scarcity and Popularity Claims (I: FTC KFTC)	High Demand (D: FTC I: KFTC)
	Social Proof	Low Stock (D: FTC I: KFTC)
	Urgency (D: FTC KFTC)	Activity Message (D: FTC CCPA I: KFTC)
		Countdown Timer (D: FTC CCPA I: KFTC)
		Limited Time Message (D: FTC CCPA I: KFTC)
		Confirmshaming (D: FTC CCPA I: EDPB)
	Shaming	

Table 2: Sources indicated in green is for FTC, turquoise is for EDPB, red is for CCPA and pink is for KFTC as abbreviated. "D" indicates a direct use of the pattern in the original source of the document and "I" indicates an inferred similarity between different terminology used in the document.

Mamidwar et al. (2024)

4.2 REGULATORY CHALLENGES IN ADDRESSING DECEPTIVE DESIGN

Despite the increasing recognition of deceptive design as a threat to consumer autonomy, existing regulatory frameworks exhibit significant gaps that undermine their effectiveness in addressing the full spectrum of manipulative practices. While regulations like the European Digital Services Act (DSA) and the Central Consumer Protection Authority (CCPA) guidelines represent important steps, their focus remains narrow, leaving several critical aspects of deceptive design unregulated.

One major gap lies in the oversight of data-driven personalisation and behavioural exploitation. Platforms increasingly leverage detailed user data to craft interfaces that target individual susceptibilities. By analysing browsing history, purchase behaviour, or even time spent on specific pages, platforms can deploy highly personalised urgency cues, scarcity messages, or default settings that subtly coerce users into making impulsive decisions. Current frameworks rarely address how the misuse of such behavioural data amplifies the manipulative power of deceptive design.

Another oversight is the absence of transparency requirements for algorithmic design and functionality. Algorithms that sort search results, prioritise pricing options, or filter offers often manipulate consumer choices in ways that are opaque to users. These mechanisms escape regulatory scrutiny as there are no mandates for platforms to disclose how algorithmic decisions influence user interfaces or behavioural outcomes.

The regulatory focus on isolated transactions also limits the ability to capture the cumulative impact of deceptive design on consumer trust and decision-making. Deceptive design are often assessed as singular manipulations, but their repeated exposure can create long-term psychological and financial vulnerabilities, normalising unethical practices in digital marketplaces.

Additionally, while regulators have emphasised the importance of informed consent, they fail to consider cognitive overload.

Consumers frequently encounter dense, technical disclosures that overwhelm them, leading to “consent fatigue.”

This undermines the principle of autonomy, as users are compelled to accept terms without fully understanding their implications.

Emerging technologies, particularly AI-driven interactions such as chatbots and virtual assistants, present a further regulatory blind spot. These tools, often designed to appear neutral or supportive, can subtly nudge users into decisions benefiting the platform, bypassing traditional definitions of deceptive design.

These gaps highlight the need for a comprehensive and forward-looking regulatory framework. Addressing behavioural data exploitation, mandating algorithmic transparency, and recognising the cumulative effects of manipulative practices are essential to closing these loopholes. Without such measures, existing regulations risk being outpaced by the rapid evolution of deceptive design in the digital economy.

A hand is pointing at a 'Sign Up' button on a website. The button is a dark red rectangle with the text 'Sign Up' in white. Below the button, there is a pink rectangle with the word 'Subscribe' in white, followed by the text 'to our newsletter' in black. Below this, there is a light gray rectangle with the text 'Sign up today for free and get the latest information'. At the bottom of this section, there is a light gray rectangle with an envelope icon and the text 'Enter your email address'. The background of the image shows a blurred website with a navigation bar containing links like 'ME', 'BRAND', 'STYLE', 'NEWS', 'BLOG', and 'SHOP'.

Sign Up

Subscribe to our newsletter

Sign up today for free and get the latest information



Enter your email address

Forced Action: Compels users to take specific steps, often irrelevant to their intent, to access services or complete tasks.

5. Conclusion

The findings of this report highlight a pressing global challenge: the pervasive use of deceptive design on digital platforms, especially during high-pressure contexts like festive flash sales. While only four countries—the USA, EU, South Korea, and India—have introduced regulations targeting these manipulative practices, significant gaps remain in addressing emerging tactics such as data-driven personalisation, algorithmic manipulation, and cumulative consumer impact. Deceptive design not only exploits consumer vulnerabilities but also erode trust in digital platforms, amplifying financial and emotional risks during culturally significant periods. For example, a study found that 68% of users who didn't know about deceptive design chose a more expensive subscription plan when confirmshaming was used, compared to only 35% of users who were aware of it (Naheyen & Oyibo et.al, 2024). This shows how important it is to create awareness so that consumers can identify and avoid manipulative tactics, helping them make better decisions for themselves. To safeguard consumer autonomy, the digital ecosystem must prioritise transparency, ethical design, and robust oversight.

Without these interventions, the unchecked proliferation of deceptive design risks normalising manipulation, leaving consumers increasingly vulnerable in an evolving digital marketplace. To build on these findings, several critical questions and gaps demand immediate attention.

Future Questions

1. REGULATION AND POLICY

Global Cooperation: How can international organisations (e.g., UN, WTO) help standardise ethical design practices across borders?

Regulatory Frameworks: What best practices can countries adopt to address evolving digital dark patterns?

Enforcement Mechanisms: How can regulatory bodies ensure compliance in a rapidly evolving digital ecosystem?

2. CONSUMER IMPACT AND AWARENESS

Education: How can digital literacy programs empower users to identify and avoid manipulation?

Impact Analysis: What are the financial and emotional costs of dark patterns, especially for vulnerable populations?

3. TECHNOLOGY AND ETHICS

Emerging Technologies: How do AI, blockchain, and IoT expand the scope of dark patterns?

Platform Accountability: How can platforms balance personalisation and persuasion with ethical design practices?

6. References

1. Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark patterns and privacy behaviors. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2016, No. 4, pp. 237-254).
2. Regulation of Dark Patterns in India. Ministry of Consumer Affairs, Government of India. 35
3. Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 165-175).
4. European Data Protection Board (EDPB). (2022). Guidelines on Deceptive Design Patterns in Digital Services. European Union.
5. Gerber, N., Gerber, P., & Volkamer, M. (2023). From nudging to dark patterns: Understanding and measuring deceptive practices in the digital marketplace. *Information Technology & People*, 36(2), 205-230.
6. Gray, D., Crofts, N., Morgan, J., & Martin, B. (2023). Systematic Review Principles for Content Analysis in Digital Environments. *Journal of Digital Consumer Studies*, 12(3), 159-178.
7. Kahneman, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux.
8. Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Studies*, 50, 51-84.
9. Mamidwar, A., Bhutkar, G., & Vishwakarma Institute of Technology, Pune, India. (2024). An Overview of Guidelines on Dark Patterns. In *CEUR Workshop Proceedings* (p. 1).
10. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
11. Nilsson, T. (2022). Impulse buying in digital marketplaces: The role of dark patterns. *Journal of Consumer Psychology*, 32(1), 50-62.
12. Spencer, S. (2020). Persuasion vs. manipulation: A conceptual framework for ethical design. *Ethics in Digital Marketing*, 17(4), 205-220.
13. Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, 23(5), 645-726.
14. Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.
15. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
16. Forbes India. (2024). Urban Indian households likely to spend close to Rs 2 lakh crore in shopping for this festive season: Survey. Retrieved from <https://www.forbesindia.com/article/news/urban-indian-households-likely-to-spend-close-to-rs-2-lakh-crore-in-shopping-for-this-festive-season-survey/94262/1>

17. Hotstar (2024). Disney+ Hotstar Festive Sentiment Survey 2024. Retrieved from 34 Flash Sale and Deceptive Buying: Manipulated to Buy Festive Report 2024 - Insights & Solutions for smarter , effective , marketing
18. Shane Frederick, Nathan Novemsky, Jing Wang, Ravi Dhar, Stephen Nowlis, Opportunity Cost Neglect, *Journal of Consumer Research*, Volume 36, Issue 4, December 2009, Pages 553–561, <https://doi.org/10.1086/599764> .
19. ASCI Academy, Parallel, Bachani, N., Dhanwani, R., Kapoor, M., Nasscom, & Department of Consumer Affairs. (2024, August 1). 52 out of 53 of top apps in India use deceptive patterns- reveals study by ASCI Academy & Parallel [Press release]. <https://www.ascionline.in/wp-content/uploads/2024/07/Press-Release.-Conscious-Patterns-25.07.24.docx.pdf>
20. ICUBE. (2023). Internet in India 2023. In ICUBE India 2023. https://uat.indiadigitalsummit.in/sites/default/files/thought-leadership/pdf/Kantar_iamai_Report_20_Page_V3_FINAL_web_0.pdf
21. India E-Commerce Market Size. (2024). Mordor Intelligence. Retrieved December 2, 2024, from <https://www.mordorintelligence.com/industry-reports/india-ecommerce-market>? Luguri, J., & Strahilevitz, L. J. (2020).
22. Shining a Light on Dark Patterns. *The Journal of Legal Analysis*, 13(1), 43–109. <https://doi.org/10.1093/jla/laaa006> Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019).
23. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Lirias* (KU Leuven), 3, 81. <https://lirias.kuleuven.be/handle/123456789/659030>
24. National Payment Corporation of India. (2024, October). National Payment Corporation of India. <https://www.npci.org.in/what-we-do/upi/product-statistics>
25. Press Information Bureau. (2024, August). [Press release]. Retrieved December 2, 2024, from https://pib.gov.in/PressReleasePage.aspx?PRID=2040566&utm_source=chatgpt.com
26. Report on Currency and Finance 2023-24. (2024). In Reserve Bank of India. Delhi. Retrieved November 28, 2024, from <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RCF29072024D5F1960668724737AD152F783DB63F10.PDF>



Farheen is a Policy and Trust Analyst at the Advanced Study Institute of Asia. She is an alumna of Osmania University and Nizam College. Her areas of interest includes political economy, digital economy, behavioural and experimental economics.

Annayah is a Research Assistant at ASIA. She holds a Bachelor's degree in Economics from Ethiraj College for Women and is currently pursuing a Master's in Psychology at Indira Gandhi National Open University. Her area of interests includes psychology, behavioural science, and UX design.