The Pranava Institute
Center for Emerging Technology and Policy

D91

The Pranava Institute and D91 Labs' Comments and Recommendations on the

Draft Guidelines for Prevention and Regulation of Dark Patterns

October 5, 2023

Authors

The Pranava Institute: Titiksha Vashist, Shyam Krishnakumar and Dhanyashri Kamalakannan

D91 Labs: Monami Dasgupta & Vinith Kurian

Table of Contents

1 Introduction: Dark Patterns and Consumer Protection....3

1.1 Defining deceptive design patterns....3

1.1.1 Global shift beyond the term ‘dark’ pattern....4

1.2 The harms of deceptive design patterns play out differently in the Indian context....5

1.2.1 Informed by Pranava Institute and D91 Labs’ research on Deceptive Design....5

2 Regulating Deceptive Design in the Indian Context....6

3 Documented instances of deceptive design across India’s digital sectors....8

4 Policy Recommendations....10

4.1 Comments on the list of dark patterns specified in the guidelines....10

4.2 Adopting a consumer harms-centred regulatory approach to tackle rapidly evolving deceptive design patterns....12

4.3 Public reporting tools and studies can deepen evidence for consumer harms emerging from dark patterns....15

4.4 Voluntary design audits for significant platforms and significant intermediaries....17

4.5 Significant Platforms and Intermediaries can be mandated to conduct annual awareness and sensitization measures to design without deception....17

4.6 Measures to incentivize the use of Ethical Design practices....18

4.7 Need for a whole-of-government approach led by the Consumer Ministry to tackle sector-specific challenges....18

1 Introduction: Dark Patterns and Consumer Protection

These comments have been prepared in response to the public call for comments issued by The Department of Consumer Affairs, Government of India on Draft Guidelines for Prevention and Regulation of Dark Patterns. The guidelines are a welcome move by the Indian government at a time when dark patterns also referred to as deceptive patterns are affecting all sectors of the digital economy, and making Indian consumers vulnerable online. This move is also in alignment with the larger global movement from governments across countries to regulate deceptive design practices and enable a safer and more trustworthy internet.

Regulating deceptive design is central to ensuring that India's most vulnerable users online are not harmed or tricked, and can safely avail of public utilities, have access to government services, and participate in the digital economy. This move is crucial to ensure consumer protection for the last digital user and is in line with the vision for India's digital economy to be beneficial for digital *nagriks*. Regulating dark patterns will also enable the empowerment of digital citizens, by ensuring that the goals of the Digital India programme[1] are met. Finally, since dark patterns impact people in tier-2 and tier-3 areas disproportionately, regulation will ensure *antyodaya* for the last digital user in line with the Prime Minister's vision for an inclusive Digital India.

The regulation of dark patterns needs to be in line with the larger principles that India sees as the foundations of its digital economy. Focusing on the consumer protection standpoint, it means that ensuring online platforms respect the rights of users including the right to privacy, are accessible and transparent, and enable information access while allowing consumers to make safe and informed decisions in the online marketplace without manipulation.

1.1 Defining deceptive design patterns

Dark patterns, also called *deceptive design*[2] or *dark commercial patterns*[3] have become a salient issue worldwide. Across the world, multifold and multidimensional consumer harms have been documented which impact users online since the term was coined in 2010. Dark patterns have also gained regulatory attention, including from the Federal Trade

[1] Vision areas of digital India. Retrieved from https://digitalindia.gov.in/vision-vision-areas/
[2] Gupta, K. (2022). Asia-Pacific IGF 2022: Takeaways on Tackling Deceptive Design Across the Asia-Pacific Region. https://webfoundation.org/2022/11/asia-pacific-igf-2022-takeaways-on-tackling-deceptive-design-across-the-asia-pacific-region/
[3] Dark commercial patterns. (2022). https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm

Commission[4] in the US, the Trade Directorate in the EU[5], the BUEC[6], and several data protection and consumer councils[7] [8] across the world.

According to the Norwegian Consumer Council[9], features of interface design are crafted to trick users into doing things that they might not want to do, but which benefit the business in question, or in short, nudges that may be against the user's own interest are called deceptive design patterns. While coercion has been used in advertising for long, dark patterns need regulatory attention owing to their scale of impact, and ubiquitousness in digital interactions. Analysis suggests that digital service providers benefit from:
(i) maximizing the sale of their product or service and/or,
(ii) maximizing the personal information they collect from the user.[10]

1.1.1 Global shift beyond the term 'dark' pattern

The term 'dark patterns' was coined back in 2010[11] at a time when conversations around coining more inclusive terminologies were limited. Subsequent scholarship has suggested that the term 'dark' in 'dark pattern' can be construed in the context of a value judgment meaning 'bad or negative'[12]. Academics also suggest that the use of the term inadvertently perpetuates racial[13] or colourist stereotypes, which is best avoided. It is suggested that the term 'dark pattern' be replaced by the more inclusive term 'deceptive pattern'/'deceptive design' - which adequately captures the intention behind the usage of these patterns[14]. It must be noted that the originator of the term Harry Brignull, as well as several large organisations, have shifted away from using the term 'dark patterns'.

---

[4] Staff in the Bureau of Competition & Office of Technology. (2022). FTC to ramp up enforcement against illegal dark patterns that trick or trap consumers into subscriptions. Retrieved from https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap?utm_source=govdelivery
[5] EU. (2022a). Digital services act. Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065
[6] BEUC, "Dark Patterns" and the EU Consumer Law Acquis: Recommendations for better enforcement and Reform (2022), https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf
[7] Enough Deception! Norwegian consumers' experiences with deceptive design. (2022). Retrieved from https://storage.forbrukerradet.no/media/2022/11/report-enough-deception.pdf
[8] Australian Competition and Consumer Commission. (2022). Digital Platform Services Inquiry - September 2022 interim report - regulatory reform. Retrieved from https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-september-2022-interim-report-regulatory-reform

[9] Forbrukerradet. (2018). https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf
[10] Chugh, B., & Jain, P. (2021). Unpacking dark patterns: understanding dark patterns and their implications for consumer protection in the digital economy. http://rsrr.in/wp-content/uploads/2021/04/UNPACKING-DARK-PATTERNS-UNDERSTANDING-DARK.pdf
[11] Brignull, H. (2010) Dark patterns. https://darkpatterns.org/ .
[12] Hupe, A. (2022). Why it's time to update our language about bad design patterns? Retrieved from https://amyhupe.co.uk/articles/changing-our-language-on-bad-patterns/
[13] Anti-Racist Language; Intuit Content Design. (2023, September 7). Retrieved from https://contentdesign.intuit.com/accessibility-and-inclusion/anti-racist-language/
[14] Sinders, C. (2022). What's In a Name? - Unpacking Dark Patterns versus Deceptive Design Retrieved from https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns-versus-deceptive-design-e96068627ec4

1.2 The harms of deceptive design patterns play out differently in the Indian context

It is important to note that the harms resulting from deceptive design play out differently in the Global North and the Global South contexts, varying across factors like culture, geography, language, and socio-economic parameters, occupation, etc. Given India's rich diversity of language and culture and its unique and rapid digitalisation trajectory, the harms of deceptive design play out in very different ways than what is documented in research which focuses largely on the US and the European Union. Language, digital literacy, accessibility, gender, and other factors in the Indian context influence consumer harm in the Indian context. However, the nature of deceptive design and harms as they play out in the Indian context are largely understudied academically.

1.2.1 Informed by Pranava Institute and D91 Labs' research on Deceptive Design

The Pranava Institute has been working on a multi-year project[15] to study the harms and challenges posed by deceptive design in the Indian context from 2021 onwards. The comments laid out in this document, therefore, are the outcomes of our research from the Design Beyond Deception project. Our research process[16] has included in-depth interviews with experts from fields of privacy, digital economy, human-computer interaction, design, and other related fields. We have also held three closed-door consultations with stakeholder groups including designers, civil society and public policy professionals, academics, and industry. These efforts have resulted in a research series on deceptive design and a manual for practitioners suitable for those working at the application level. **D91 Labs has been working on the nature and harms of deceptive design in India's rapidly growing fintech sector and has published an in-depth audit of deceptive design patterns found in India's fintech applications[17].**

The comments on the draft guidelines are informed by the expert interviews, stakeholder consultations, and study conducted by Pranava Institute and the research on India's fintech ecosystem conducted by D91 labs.

---

[15] Vashist, T., Krishnakumar, S., & Kamalakannan, D. (2023). Design Beyond Deception. The Pranava Institute. Retrieved from https://www.design.pranavainstitute.com/

[16] Vashist, T., Krishnakumar, S., & Kamalakannan, D (2023). Cover Note- The Design Beyond Deception Manual Project. Delhi: The Pranava Institute. https://www.design.pranavainstitute.com/_files/ugd/72dce4_cdd2b237041e4b288cc952943805e5f2.pdf

[17] Dasgupta, M., Gopalakrishnan, R., & Kurian, V. (2023). Fintech 'App'rehensions: An Assessment of Deceptive Design in Indian Fintech. Retrieved from The Pranava Institute. https://www.design.pranavainstitute.com/post/fintech-app-rehensions-an-assessment-of-deceptive-designs-in-indian-fintech.

2 Regulating Deceptive Design in the Indian Context

The Indian context includes its own unique and specific challenges pertaining to dark patterns. India is one of the fastest-growing digital markets in the world. With over 50% of the population actively online[18], and increasing internet penetration, global tech giants see Indian users as the next billion who will shape the internet. However, issues of the digital divide[19] exist across lines of divisions of rural-urban contexts, gender, literacy, and income levels. India's approach to building digital public infrastructure has also led to increased digital adoption and enabled development goals such as social services and financial inclusion. This has resulted in a fast uptake of digitization of public and private services in sectors such as finance, education, and health, as well as rapidly changing the interfaces between digital natives, the state, and the digital economy.

With one of the largest and fastest-growing startup ecosystems[20] In the world, India will need to address the challenges of deceptive design practices that are prevalent across sectors. Policy and regulation around deceptive practices will enable India to push innovation and entrepreneurship along with creating a safe cyberspace for all.

The following factors are relevant to understanding the specific impact of deceptive patterns in India:

a. **Digital Divide and Lower Digital Literacy**

Despite rapid growth in internet penetration, and an increase in digitization of services, India is yet to achieve its digital literacy goals. According to the National Statistical Office, while over 55 percent of Indians have access to broadband, only 20 percent have the ability to use the Internet.

b. **Vulnerable groups**

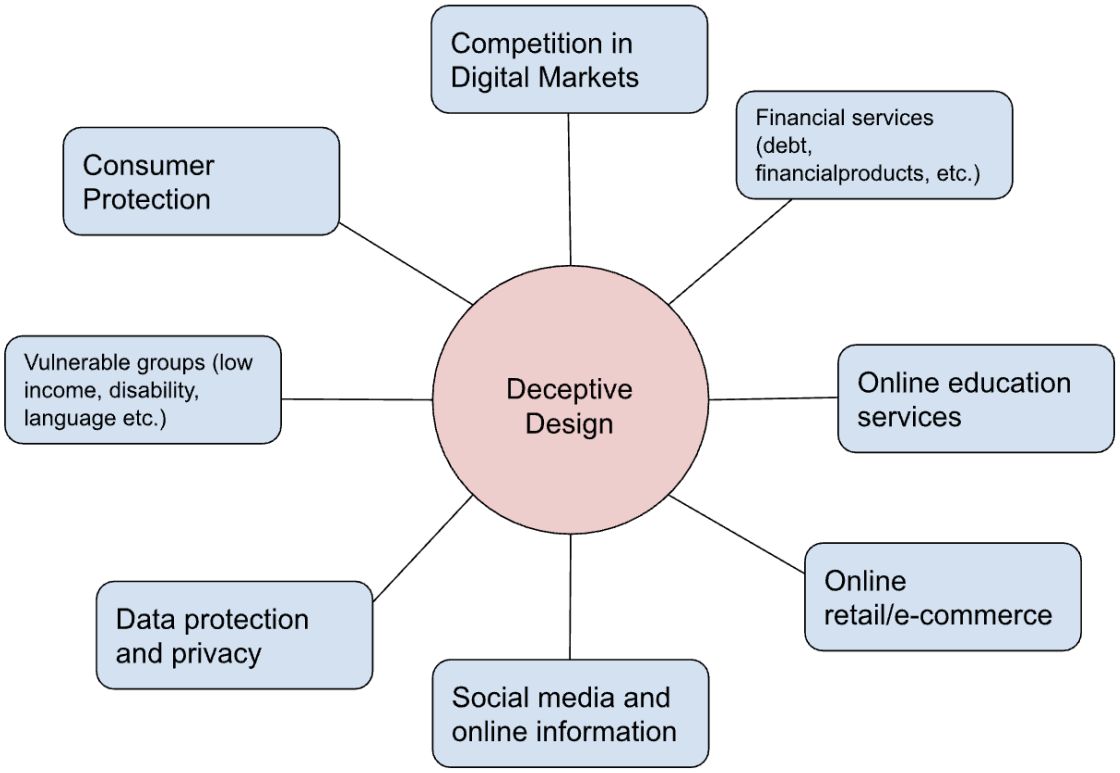
A study conducted by Dvara Research in 2021 also showed that respondents with lower levels of education, and respondents with lower levels of income were more likely to be

[18] Over 50% Indians are active internet users now; base to reach 900 million by 2025: report. (2023). The Hindu. Retrieved from https://www.thehindu.com/news/national/over-50-indians-are-active-internet-users-now-base-to-reach-900-million-by-2025-report/article66809522.ece

[19] Chandola, B. (2022). Exploring India's digital divide. Retrieved from https://www.orfonline.org/expert-speak/exploring-indias-digital-divide/#:~:text=The%20NFHS%20also%20provides%20data,females%20qualify%20for%20this%20condition.

[20] Patwardhan, N. (2022). Economic survey: India becomes third largest startup ecosystem in the world. Retrieved from https://www.livemint.com/economy/economic-survey-india-becomes-third-largest-startup-ecosystem-in-the-world-11643626506129.html

influenced by dark patterns.[21]



Deceptive Designs are a matter of concern across multiple digital platforms, impacting various vulnerable population cohorts, and is also a matter of public safeguards like data protection and consumer protection

c. **Language and cultural differences as vectors of deception**

Research conducted by Human-Computer Interaction (HCI) scholars in India has shown that an overwhelmingly English-language internet in India excludes the population majority in India. **India's rich language and cultural difference means that lack of linguistic representation on the internet often leaves room for confusion, lack of clarity, and low accessibility to digital services- and finally, a greater possibility of manipulation. User researchers interviewed for our study shared that owing to the highly text-first design of apps, users often confuse the purpose of the app, and what consequences its use has on the person (mistaking an investment app for a loan app, for example).** Research also shows that certain vulnerable groups in India lie at the intersection of being linguistic minorities, with often low digital literacy and economic backwardness.

These three intersections create issues of access as well as increase the potential for harm for such users. Research on HCI and designing for the vulnerable suggests adopting more culturally sensitive design practices.

[21] Chugh, B., & Jain, P. (2021). Unpacking dark patterns: understanding dark patterns and their implications for consumer protection in the digital economy. http://rsrr.in/wp-content/uploads/2021/04/UNPACKING-DARK-PATTERNS-UNDERSTANDING-DARK.pdf

In his book Cross-Cultural Design, Senongo Akpem[22] states that despite a globalized reality of technology, culture is left out and goes unaccounted for in technology dissemination. **He argues that one of the biggest mistakes seen in design today is the assumption that users all come from WEIRD (Westernised, Educated, Industrialised, Rich, Developed) cultures. "We use imagery, typography, and taxonomies familiar to us, without researching their impact in other cultures and languages. Those of us in WEIRD countries treat the web as an extension of our own lived experiences' ' Akpem says. This makes it important to use a design methodology that is culturally responsive and attuned to what diverse audiences need and want, including people in India.**

d. Fintech products penetrating tier-2 and tier-3 cities

While rapid digitalization of financial services and utilities have helped India's erstwhile unbanked population, there is also a steep rise in the use of financial products and services in tier-2 and tier-3 cities, including in lending, credit access and other financial products. While these open opportunities for growth, there is also a case to be made for increased risk, especially for vulnerable groups which are often first-time internet users. Safeguarding their finances, data and interests needs to be made a priority in regulating dark patterns.

3 Documented instances of deceptive design across India's digital sectors

a. **Fintech Apps**

India has witnessed rapid and widespread digital adoption in the fintech space in recent years. The potential risks for users which accompany the fast growth of this industry should also be examined. The fintech industry poses significant risks to users in terms of privacy and financial harm by using deceptive patterns like hidden costs, expensive surrender clauses, misleading games, and unsuitable bundled products. Research conducted by D91 Labs shows how fintech apps in India employ deceptive practices across fake loans, neo-banking, investment tech, and health insurance apps.[23] ***These deceptive practices cause multiple harms to users including financial harm, reputational harm, psychological detriment, time loss, privacy harm, and loss of trust in the market.***

b. **Fake Loan Apps**

Layoffs during the Covid-19 pandemic, increased smartphone penetration, and the lack of access to formal credit among 190 million adults in India led to the mushrooming of unsecured digital lending apps that provide quick loans without

[22] Akpem, S. (2021). Cross Cultural Design. Retrieved from https://senongo.net/cross-cultural-design
[23] Dasgupta, M., Kurian, V., & Gopalakrishnan, R. (2023). Tricked by design: Deceptive patterns in Indian fintech apps. Retrieved from https://d91labs.substack.com/p/tricked-by-design-deceptive-patterns#footnote-5-118470367

collaterals.[24] **The lending apps obtain access to the borrower's phone's location data, contacts, apps, and text messages in the name of credit risk assessment which is explicitly stated to the borrowers. Weeks after borrowing the instant loan, borrowers were faced with severe harassment from the agents who made over a thousand phone calls per day and abused the borrowers with obscene materials sent to their contact lists.** These mafia-like collection tactics and extent of abuse in some cases have even led the borrowers to contemplate suicide. In 2021, over 17 suicides were connected to such harsh recovery tactics by the Save them India Foundation.[25]

The home ministry observed that the money lending app issue impacts 'national security, economy, and citizen safety' and is an organised cybercrime executed using disposable emails, virtual numbers, mule accounts, shell companies, payment aggregators, API services, cloud hosting and cryptocurrency. The Directorate of Enforcement (ED) initiated several cases this year under the Prevention of Money Laundering Act (PMLA) where proceeds of crime of approximately Rs.2,116 crore through illegal loan apps were identified.[26] The RBI last year banned all third parties involved in the disbursal of loans and collection of repayment stating that the process should be executed only between borrowers and the entities regulated by the RBI.[27]

c. **Crypto and Virtual Digital Assets**

Cryptocurrencies and Digital assets such as NFTs became increasingly popular in 2022. Crypto companies invested in producing content in regional languages, collaborating with regional influencers, and forming local partnerships to attract young- first-time investors in tier-2 and tier-3 cities. Companies such as CoinSwitch Kuber witnessed a 135% growth in sign-ups every month from such cities in 2021.[28] **The abundance of unreliable sources, misleading information, and incomplete understanding of the crypto market risks puts the users in an unfair position**

[24] Chandran, R. (2021). Your data for cash: Indian lending apps force tough choice. Retrieved from https://economictimes.indiatimes.com/tech/tech-bytes/your-data-for-cash-indian-lending-apps-force-tough-choice/articleshow/80583018.cms

[25] Makol, M. K. (2022). India's digital loan sharks face crackdown as complaints Mount. Retrieved from https://economictimes.indiatimes.com/industry/banking/finance/indias-digital-loan-sharks-face-crackdown-as-complaints-mount/articleshow/88683649.cms

[26] Mukul, P., & Bhalla, T. (2023).IT, Home Ministries and RBI to decide on steps post loan app ban; fintech firms seek clarity. Retrieved from https://economictimes.indiatimes.com/tech/technology/it-mha-officials-to-talk-to-rbi-to-decide-on-next-app-ban-steps/articleshow/97703079.cms

[27] Tripathi, R. (2022). Illegal digital lending apps driving citizens to suicide, says Ministry of Home Affairs. Retrieved from https://economictimes.indiatimes.com/industry/banking/finance/banking/illegal-digital-lending-apps-driving-citizens-to-suicide-says-ministry-of-home-affairs/articleshow/95188059.cms

[28] Mittal, A. (2021). Investors from non- metro cities flock to online brokerages, crypto platforms. Retrieved from https://economictimes.indiatimes.com/tech/technology/small-towns-investors-flock-to-online-brokerages-crypto-platforms/articleshow/85573250.cms
https://economictimes.indiatimes.com/tech/technology/small-towns-investors-flock-to-online-brokerages-crypto-platforms/articleshow/85573250.cms

and leads to several potential harms including financial loss, loss of time and effort, privacy loss, and even psychological harm. Some platforms often misrepresent information about the security and returns associated with investments in cryptocurrency using the words usually associated with regulated entities by people such as ‘currency’, ‘securities’, ‘custodian’ and ‘depositories’ and create a sense of familiarity. The ASCI[29] advised the VDA product advertisements which talk about cost or profitability to contain clear, sufficient, updated information about the same with a disclaimer regarding the risks associated. Furthermore, ads for virtual digital assets cannot include comparisons with other regulated assets, promise guaranteed profits or showcase crypto as a solution for money problems.

d. **E-commerce**

In a global report of a survey of 4800 small businesses all over the world, 63% of small businesses in India have been selling online in the last 1-5 years which was higher than the global average of 55%.[30] Although e-commerce started as a boon to small-scale businesses, small sellers have complained of increased challenges caused by the platformisation by e-commerce giants. Studies have shown how e-commerce platforms incorporate deceptive design patterns to manipulate consumer choice and harm them through search engine manipulation, preferential listing, exclusive partnerships (fostering close relations with alpha sellers, providing higher discounts, and entering into vertical agreements with them), targeted ads and abuse of dominance affecting the competition[31]. **In such cases, considering the harm caused to the end consumer alone would not be a good measure of deception. Harms caused by deceptive design to the stakeholders i.e. sellers on the platform by affecting the competition in the market results in significant loss to the MSME and other businesses.**

4 Policy Recommendations

4.1 Comments on the list of dark patterns specified in the guidelines

[29] Kaul, A. (2022). ASCI releases guidelines for ads, promotion of crypto assets, services. Retrieved from https://www.livemint.com/market/cryptocurrency/asci-releases-guidelines-for-ads-promotion-of-crypto-assets-services-11645599224619.html

[30] Khurana, G. (2023). Over 60% of Indian small businesses use website, e-store or e-commerce to grow; above global average: Report. Retrieved from https://www.financialexpress.com/industry/sme/msme-tech-over-60-of-indian-small-businesses-use-website-e-store-or-e-commerce-to-grow-above-global-average-report/3106238/

[31] Kalra, A., & Stecklow, S. (2021). Amazon copied products and rigged search and rigged search results to promote its own brands, documents show. Retrieved from https://www.reuters.com/investigates/special-report/amazon-india-rigging/

The deceptive patterns listed in draft guidelines presented by the Department of Consumer Affairs and Advertising Standards Council of India are specific and non-exhaustive. Although most of the broader categories of deceptive patterns are covered, we recommend that the guidelines consider incorporating the following specific sub-categories of deceptive patterns as well.

Deceptive patterns as per draft guidelines	**Additional deceptive patterns**
Forced action	Under the deceptive pattern of Forced action, there are 2 more patterns that should be considered 1. **Forced disclosure** - Users tricked or forced into sharing more personal information than necessary for the product. For eg - Some fintech apps ask for information linked with Aadhar and credit bureau records, even when it is not a credit product. 2. **Friends Spam/ Address book leeching**- Manipulative extraction of information about a user's contacts and social networks. For eg - Lending apps ask for phone numbers of the user's immediate network to "follow up" in case of loan defaults. The borrower may not have a complete understanding of this process.
Subscription Trap/immortal account	Under the deceptive pattern of subscription pattern, one more pattern should be considered 1. **Lack of transparency** For eg - Reluctance to offer explanations or control options to users when it is favorable to the business
Interface Interference	Under the deceptive pattern of Interface interference, there are 3 more patterns that should be considered 1. **False Hierarchy** - Visual prominence given to the firm's preferred setting or version of a product For eg - Highlighting the most expensive products over the cheaper options, influencing a user's buying decision (regardless of their need). 2. **Misleading reference pricing**- False or misleading reference price is

	displayed For eg - Using outdated information on the rate of returns to attract users to invest in products that are more favorable to the business. 3. **Preselection** - Firm-friendly default is preselected (e.g. more expensive or less privacy-protecting option) For eg - Assuming consent for privacy-intrusive settings such as default opt-in for scraping SMS data and communication over WhatsApp.
(Additional Deceptive Pattern category) *Social proof -* *These dark patterns attempt to trigger a decision by the user based on observations of other users' behaviour, and can thus exploit social proof bias that makes people conform to what others are doing.*	1. Testimonials - For eg - Statements from other users regarding a product, which may be misleading or false

4.2 Adopting a consumer harms-centered regulatory approach to tackle rapidly evolving deceptive design patterns

Academics have found the sheer number and range of deceptive design patterns are growing and evolving beyond the accepted taxonomies and categories of deceptive design. With the advent of generative AI solutions for designing user interfaces, the problem is likely to grow exponentially. Since banning a type of pattern may not effectively remove the harm caused by it (since new patterns can cause the same harm and types of dark patterns are proliferating rapidly), research and emerging global regulatory approaches suggest that approaching regulation from a harm-centered approach will be more effective. A principles-based approach which serves as the foundation on which India's digital economy and its rules rest, can be reflected in the regulation on deceptive design. These principles, including privacy, enabling access and inclusion, and fair competition and transparency need to be central in digital regulations, including those on deceptive design.

Each deceptive pattern can be mapped to one or more harms that it may cause. Deceptive patterns often lead to harm such as invasion of privacy, intended financial loss, psychological burden, loss of societal reputation, and erosion of trust in the market. While creating a list of harms caused by deceptive patterns, we could also consider ranking them in their order of magnitude which will help the industry to tackle and reduce the prevalence of the patterns accordingly.

Harms caused by deceptive patterns would include -

- Financial harm

- Privacy harm
- Reputational harm
- Loss of trust in the market
- Psychological detriment and time loss

We have provided a description of each harm along with examples for explanation. These are not an exhaustive list of harms and with the increase in types of deceptive patterns, the list of harms will also increase.

Harm #1
Psychological Detriment and Time Loss

The experience of frustration or increased cognitive burden that result from deceptive design. These designs exploit a user's inertia, limited attention span or time. These cognitive elements are exploited to create addictive behaviours by sufficiently capturing a user's time and attention.

Examples
Psychological Detriment

- Overloading information to confuse the user into agreeing to T&C that are favourable to the business. (Obfuscation)
- Pushing a user to complete a process or draw attention towards a new product that you were not looking for. (Nagging)

Examples
Time Loss

- Making it difficult for users to sign-out or unsubscribe from a service or receive communication (Roach Motel)
- Forming addictive engagement habits by employing elements of 'gambling' such as slot machines or wheels of fortune to keep the user coming back daily. (Gamblification)

Harm #2
Financial Harm

The experience of financial loss incurred directly (by paying a higher monetary price due to hidden costs) or indirectly (by completing actions that may lead to future financial loss). Deceptive designs are employed to get user's to buy something that they may not have required or to get them to spend more than they intended to spend.

Examples

- Interfaces that profit from adding (bundling) products at check-out point without the user's consent (Sneaking into basket)
- Mislead users into thinking they are signing up for one-time offers but instead creating a recurring fee (Hidden subscription)
- The headline price advertised at the beginning of anoffer differing from the final offer due to additional fees, taxes, and other charges (Drip Pricing)

Harm #3
Reputational Harm

The resultant negative impact on a user's reputation or social standing by creating designs that use access to personal information to interact with or influence the user's social network.

Examples

- Apps requesting contact details from your immediate network with the implicit understanding of reaching out to them in case of a loan repayment default (Address Book Leaching / Friend Spamming)
- Assumed consent for accessing communication channels like WhatsApp through pre-selected checkboxes. (Preselection)

Harm #4
Privacy Harm

The loss of user's privacy by divulging more personal data than intended, potentially exposing them to further risks. Deceptive designs exploit user bias by offering a trade-off between the tangible and immediate short-term benefit of using the service and the costs of potential long-term privacy loss.

Examples

- Apps requesting excess information without clarity of purpose and duration of data pull or third-party data sharing (Privacy Zuckering)
- Clubbing multiple consents without no choice to opt-out. This could be detrimental to user's attention span (Obfuscation of consent framing)
- Creating accounts that remain active indefinitely (Immortal accounts)

Harm #5
Loss of Trust in the Market

The erosion of a user's trust towards a product or platform as well as the broader industry, potentially hampering future innovations. The deceptive designs used here manipulate, mislead or hide important information from the user, leading to a negative or sub-optimal user experience. Loss of trust may result from repeated exposure to most deceptive design.

Examples

- Not disclosing the credit underwriting process after the loan is disbursed or proving unclear terms of credit at the point of sale (Lack of transparency)
- Indefinite access to transaction data through SMS scrapping with unclear purpose of use. (Obstruction)
- Fabricated user reviews and testimonials. (Social Proof)
- Using language that makes a user feel that they might miss out on an offer. (Creating Urgency)

4.3 Public reporting tools and studies can deepen evidence for consumer harms emerging from dark patterns

Global precedents by consumer protection agencies show that evidence collection can create a substantial impact on ensuring other sectoral regulators take proactive measures to prevent deceptive design-based harms. Therefore the regulatory body can consider setting up public reporting tools and commission studies to deepen the understanding of specific harms of deceptive design in the Indian context that could lead to proactive measures under a whole-of-government approach for consumer protection.

A. Creation of a Consumer Portal for Voluntary Reporting of 'Deceptive Patterns'

Deceptive design practices and elements are constantly evolving. They are inherently elusive and can be quickly modified to circumvent existing and less flexible regulatory frameworks, making them a moving target for regulators as evidenced by regulatory experience in the United States[32]. To tackle this issue comprehensively, we propose the establishment of a centralized consumer portal for voluntary reporting of deceptive design patterns observed in usage. An indicative framework[33] for a voluntary crowd-sourcing tool of this kind has been shared by the Tech Policy Design Lab (An initiative of the World Wide Web Foundation). This consumer portal allowing for voluntary reporting of these tactics serves as a real-time, adaptive mechanism to counter this evasive nature. ***By crowdsourcing insights into emerging and evolving dark patterns, the portal can provide regulators and policymakers with timely data, thereby enabling them to adapt and update guidelines more responsively.*** Similar consumer-driven approaches have been particularly effective in the domain of mapping and GIS-centric solutions[34].

The key objectives of the portal should include

1. To **identify, document, and categorize** deceptive design patterns in digital interfaces through crowd-sourcing such ideas.
2. To **facilitate public awareness** and knowledge sharing of the prevalent deceptive patterns.
3. To provide a **structured dataset for regulators, policymakers, and consumer advocacy groups** on the nature and extent of deceptive design practices being employed across parameters such as industries, user groups, and product categories.
4. To aid in the formulation and implementation of **better regulations against such practices.**

---

[32] Slater, F. (2023) The Future of Manipulative Design Regulation - Future of Privacy Forum. Retrieved from https://fpf.org/blog/the-future-of-manipulative-design-regulation/#:~:text=The%20breadth%20and%20nuance%20of,under%20a%20single%20regulatory%20framework

[33] Tech policy design lab. Retrieved from https://techlab.webfoundation.org/strategies-for-change/crowdsourced-reporting-tool

[34] Crowdsource Reporting Apps – GIS For Citizen-Driven Planning (2020). Retrieved from https://www.msa-ps.com/crowdsource-reporting-apps-gis-for-citizen-driven-planning/#:~:text=A%20crowdsource%20reporting%20app%20is,for%20development%20within%20that%20map.

Designing the consumer portal for voluntary reporting of deceptive design patterns is the first step. We are cognizant of the need for a comprehensive framework around the operationalizing of such a portal. This would require more multi-stakeholder consultations. Some indicative points of discussion may include:

1. **Ensuring Data Validation:** There is a need to devise a mechanism for authorities to investigate, validate, and act upon the reported issues.
2. **Ensuring User Privacy and Data Security:** Protecting the identities of individuals reporting dark patterns and ensuring data security will be important
3. **Resource Allocation:** Adequate staffing, technical infrastructure, and budget need to be allocated to ensure the proper functioning of the portal.
4. **Creating Public Awareness:** For the portal to be effective, people need to know about it. Strategies to ensure public awareness and ease of access must be thought of.
5. **Creating a Feedback Loop:** For businesses to respond to accusations of using deceptive design practices and make corrective actions, under regulatory oversight.

B. Sponsor investigations to document harms in the Indian context: Consumer protection agencies and regulators across the world, including those in Norway, Australia, the US, the EU, and the Netherlands, have taken up investigations and work on deceptive design as central to consumer protection in a digital world[35]. Several of these bodies have issued studies in order to understand the full range of harms that result from dark patterns. These studies have then been used to provide evidence for sector-specific regulatory bodies to levy fines, issue new codes and directives, and create laws for the digital economy[36].

4.4 Voluntary design audits for significant platforms and significant intermediaries

In the case of significant platforms and intermediaries, we recommend **annual design audits by independent third-party experts to identify the use of deceptive design practices and assess the ethical considerations integrated into digital platforms**, along the lines of data audits recommended in the Digital Data Protection Bill. These audits could be initially made on a voluntary Code of Conduct basis or through industry self-regulation. In the medium term, **mandatory annual design audits could also be considered for significant intermediaries.**

[35] Such as the ACCC in Australia, the Norwegian Consumer Council in Norway, and the BEUC in the European Union.
[36] For instance, the BEUC's work on "DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS" laid out recommendations for enforcement and reform, which also influenced the Digital Services Act which prohibits deceptive or nudging techniques.

4.5 Significant Platforms and Intermediaries can be mandated to conduct annual awareness and sensitization measures to design without deception

The guidelines can mandate that **significant platforms and intermediaries, as defined by their user base, the volume of transactions, data collected, systemic importance and other factors, across various digital sectors including fintech, e-commerce, social media and tech to conduct annual measures to educate product teams on the impacts of deceptive design on consumers and conduct decisions on designing beyond deception.** These are crucial since product teams play a crucial role in creating digital interfaces, setting metrics to evaluate success, and designing the UI/UX which users interface with. The government can consider certifications for industry professionals on the theme of responsible and ethical design that goes beyond deception.

4.6 Measures to incentivize the use of Ethical Design practices

When the evolving nature of the problem, preventing and regulating deceptive design practices may not always be an enforceable position. In this regard, it is suggested to include mechanisms that incentivize employing ethical design practices. To encourage ethical design practices, similar to how car crash safety ratings[37] have made safety features more desirable for both consumers and car manufacturers, various mechanisms can be implemented. These measures can include both market-driven incentives and formal regulatory frameworks. Some indicative metrics for making the use of ethical design more desirable include:

1. **Play Store/App Store Ratings:** App stores could include a specific rating for ethical design, alongside the usual metrics for performance and user interface. Users would be more inclined to download an app with a high ethical rating, creating a competitive advantage for companies that invest in ethical design.
2. **Certifications from Industry bodies/ Self-Regulatory Organizations (SROs):** Independent bodies can be authorised to issue certifications to companies that meet predefined ethical design guidelines. This could be similar to a 'Fair Trade' or ‘sustainability’ certification but for digital products/ interfaces. A framework outlining an accreditation approach has been provided by the Tech Policy Design Lab (An initiative of the World Wide Web Foundation)[38]

4.7 Need for a whole-of-government approach led by the Consumer Ministry to tackle sector-specific challenges

Experiments in innovation and regulation across the world have shown that dark patterns need to be regulated by multiple bodies which seek to protect different aspects of a citizen’s online experience. Deceptive design is pervasive across sectors of the digital economy.

---

[37] Teoh, E. R., & Monfort, S. S. (2023). IIHS small overlap frontal crash test ratings and real-world driver death risk. https://www.tandfonline.com/doi/full/10.1080/15389588.2023.2199342
[38] Tech policy design lab. Retrieved from https://techlab.webfoundation.org/strategies-for-change/evaluation-accreditation

While the Consumer Protection Ministry has taken a welcome lead in regulating deceptive design practices, the problem requires a whole-of-government approach with interventions from sector-specific regulators to create codes and guidelines that prevent consumer harms which are most important (e.g. Financial loss in the case of fintech applications). Similarly, data protection and privacy issues resulting from deception need to be addressed by India's forthcoming Data Protection Authority (DPA) as per the Digital Personal Data Protection Bill, 2023. Sector-specific regulators can also levy fines and penalties for large players who set the norms for the UI/UX in their domains. This will increase the cost of using deceptive design, and ensure that players adopt consumer-focussed, ethical practices.

This requires multiple regulatory bodies to develop an approach that regulates deceptive design at multiple levels in order to safeguard the interests of citizens, as well as use regulatory tools to ensure that the digital economy is based on fairness, privacy, and transparency.

About The Pranava Institute

The Pranava Institute is an Indian think-tank that works at the intersection of Emerging Technology, Public Policy, and Society from an India-first perspective. Our work focuses on original research on digital issues in the Indian context including trust and safety, responsible AI and youth and emerging technology. The Pranava Institute believes in developing emic approaches to technology regulation to shape sustainable digital futures.

About D91 Labs

D91 Labs is a research entity within Setu dedicated to fostering fintech innovation in India by conducting cutting-edge research and developing fintech ideas that could address the unique challenges and opportunities of the Indian market. Through our research, we bridge the knowledge and empathy gap among stakeholders to improve digital financial services.
