INTERNET FREEDOM FOUNDATION internetfreedom.in policy@internetfreedom.in +91 011 4143 7971

By Email

To,

Anupam Mishra
Joint Secretary, Department of Consumer Affairs
Ministry of Consumer Affairs, Food and Public Distribution
Government of India
PD Krishi Bhawan, New Delhi - 110001

Email: js-ca@nic.in

Date: October 05, 2023 IFF/2023/042

Re: Comments on the draft Guidelines on Prevention and Regulation of Dark Patterns

Dear sir,

1. The Internet Freedom Foundation ("IFF") is a registered charitable trust that advances constitutional freedoms for every Indian in a digital society. We work across a wide spectrum of issues, with expertise in free speech, electronic surveillance, data protection, net neutrality, and innovation. We aim to champion privacy protections, digital security, and individual freedoms in the digital age.

2. We are writing to you to offer our inputs on the draft Guidelines on Prevention and Regulation of Dark Patterns ("Guidelines") published by you on 7 September, 2023, on which comments are invited until 5 October, 2023.[1] At the outset, we appreciate the decision of the Department of Consumer Affairs ("DoCA"), Ministry of Consumer Affairs, Food and Public Distribution ("Ministry") to regulate prevalent trade and advertising practices that trick and deceive consumers through the incumbent Guidelines.

3. We believe that the Ministry should, moving forward, be cognisant of the complex sectoral interplay in this domain and implement the Guidelines in a manner that safeguard consumer interest without overregulating the market. We also encourage the

[1] Draft Guidelines on Prevention and Regulation of Dark Patterns, J-24/34/2023-CPU Section-CPU [31763]. https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf

Ministry to take into account consumer privacy concerns posed by dark patterns, and in the future, encourage platforms and entities to minimise data collection and keep consumer-facing processes transparent. Annexure 1 of the Guidelines is a comprehensive and useful tool for consumers to identify dark patterns – the Ministry is urged to continue expanding its scope to include new patterns as they keep emerging. For this, we at IFF would be happy to keep sharing instances flagged by our community to enable the identification of emerging trends in dark patterns through our Dark Patterns Tracker (**Appendix B**), or provide our faculties and support for further strengthening the Guidelines and corresponding Consumer Protection Act and Rules. Our detailed submissions in this regard are annexed at **Appendix A**.

4. We once again extend our appreciation to the Ministry for taking up the pressing issue of regulating dark patterns in India and we hope that going forward, the Ministry considers holding public consultations involving civil society and ordinary consumers for a holistic view on the issue. We look forward to your response on this matter and remain at your disposal should you wish to discuss the issues mentioned in this submission any further.

Kind regards,

Prateek Waghre

Prateek Waghre,
Policy Director,
Internet Freedom Foundation
prateek@internetfreedom.in

IFF's comments on the draft

Guidelines on Prevention and Regulation of Dark Patterns

Internet Freedom Foundation

INTERNET FREEDOM FOUNDATION

Internet Freedom Foundation
I-1718, Third Floor, Chittaranjan Park,
New Delhi 110019

Recommended Citation: Disha Verma & Prateek Waghre, “IFF’s comments on draft Guidelines on Prevention and Regulation of Dark Patterns October 05, 2023.”

Authors:

Internet Freedom Foundation (“IFF”) is a registered charitable trust which advocates for the digital rights of Indians. Our mission is to ensure the growth of digitisation with democratic rights guaranteed under the Constitution of India..

Disha Verma is an Associate Policy Counsel at Internet Freedom Foundation. A lawyer by training, Disha spent nearly three years working in health policy with a focus on community health and disease response at the national and global level, before transitioning to tech policy. At IFF, she engages with state deployment of technologies in welfare delivery, surveillance and public administration through a critical and rights-affirming lens.

Prateek Waghre is the Policy Director at IFF. A technologist-turned-public policy professional, Prateek has spent nearly a decade in the CDN industry as a consultant and product manager. Since moving to public policy, his research work has focused on a number of areas such as internet shutdowns, information disorder in the information ecosystem, and the governance of digital communication networks/social media in India. Prateek is also an alumnus of the U.S. State Department’s International Visitor Leadership Program (IVLP) on Disinformation in the Quad.

We would like to thank Associate Policy Counsel, Tejasi Panjiar, and Digital Literacy Intern, Purvai Dwivedi for their assistance and IFF staffer Ashlesh Biradar for his design and graphic contributions. We are also grateful to our community for their support.

Appendix A

Comments on the draft Guidelines on Prevention and Regulation of Dark Patterns

The Ministry's attempt to regulate deceptive patterns on online platforms and entities is in line with the larger mandate of the Consumer Protection Act, 2019 ("Act"), which is to safeguard consumer interests. The Guidelines serve as an appropriate preliminary framework for regulating a dynamic and ever-evolving space, with which the law must also eventually evolve, and the Ministry is a suitable nodal agency to establish institutional protections against consumer manipulation. Having said that, we, at IFF, submit the following suggestions on how the Ministry may bolster the Guidelines and make them more holistic:

1. **On the regulation of dark patterns**

1.1. *Regulatory interplay*

1.1.1. Dark patterns, defined in the Guidelines as extending to "*any practices or deceptive design patterns using UI/UX interactions on any platform…*", are spread across a wide array of sectors. Instances of consumer deception are prevalent in finance, insurance, e-commerce, travel, entertainment, and so on, implicating a number of sectoral regulators and their legal frameworks. Some sectors have existing regulations penalising deceptive patterns, though in limited contexts. For instance, the Insurance and Regulatory Development Authority of India ("IRDAI") prohibits travel portals in India from covertly selling insurance as a default option.[2] The Advertising Standards Council of India ("ASCI"), a self-regulating entity also engaged with drafting the incumbent Guidelines, recently adopted the 'Guidelines for Online Deceptive Design Patterns in Advertising'.[3] In advertising, the Ministry itself also notified the 'Guidelines on Prevention of Misleading Advertisements' in 2022.[4] With a rise in prevalence of dark patterns in e-commerce, travel, and other sectors, sectoral regulators may want to likewise establish narrow legal frameworks prohibiting specific use-cases.

[2] Circular on Travel Insurance Products and operational matters, IRDAI/HLT/CIR/MISC/174/09/2019. https://irdai.gov.in/document-detail?documentId=392465#:~:text=Insurersshall%20ensure%20that%20any%20portal,not%20to%20buy%20the%20coverage.

[3] Guidelines for Online Deceptive Design Patterns in Advertising, June 2023. https://www.ascionline.in/wp-content/uploads/2023/05/Guidelines-for-Online-Deceptive-Design-Patterns-in-Advertising.pdf

[4] Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022. https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf

1.1.2. However, such overlapping regulation of dark patterns can result in regulatory uncertainty. Guideline 6 stipulates that "*where a dark pattern is regulated under any other law for the time being in force or the rules or regulations made thereunder, the provisions contained in these guidelines shall be in addition to and not in derogation of, such regulation in other laws*." This points to the possibility of a platform engaging in dark patterns being penalised under two laws simultaneously: one sectoral and specific, and the other general, such as these Guidelines. We believe that such ambiguity may have a negative impact on design innovation and creativity, or affect personalisation which may be preferred by the user.

1.1.3. Therefore, we urge the Ministry to be cognisant of regulatory interplay in this domain, and clearly delineate its jurisdiction and executive functions from sectoral regulators. While sectoral regulators can undertake *suo moto* compliance assessment on entities, the Guidelines can act as a public-facing recourse for aggrieved consumers to report dark patterns. Both can coexist harmoniously if jurisdiction is expressly divided at the outset.

1.1.4. Having said that, it is inevitable that the Ministry will run into jurisdictional deadlocks with domain regulators manifestly interested in dark patterns, such as the Competition Commission of India ("CCI"), the Data Protection Board ("DPB") or the Ministry of Electronics and Information Technology ("MeitY"). Both the Consumer Protection Act, 2019 and the Competition Act, 2002, regulate and penalise "*unfair trade practices*", which is what dark patterns are classified as under Guideline 2(e). The core difference is that the Competition Act, 2002 applies to dominant players that abuse their market position to compromise consumer interest, and the Consumer Protection Act, 2019 applies universally and more broadly.[5] However in this case, use of dark patterns by dominant marketplace entities can implicate both laws, as it will affect consumer interests as well as the market. To prevent subject-matter overlap, the Ministry is encouraged to clearly define the scope and jurisdiction of the Guidelines and delineate them from the much more strictly regulated Competition Act, 2002.

1.1.5. Regardless of overlap, we believe that the Ministry is an appropriate authority for consumers to seek redressal against the deployment of dark patterns, as the mandate of consumer protection cuts across sectors and markets. Literature also suggests that a familiar and consumer-friendly body such as the Ministry can spare consumers the anxiety of navigating new redressal mechanisms.[6]

[5] Section 4, Competition Act, 2002.

[6] Beni Chugh, Pranjal Jain, Unpacking Dark Patterns: Understanding Dark Patterns and their Implications for Consumer Protection in the Digital Economy (2021), pg. 17-18. http://rsrr.in/wp-content/uploads/2021/04/UNPACKING-DARK-PATTERNS-UNDERSTANDING-DARK.pdf

1.2. *Self-regulation*

1.2.1. While there is merit in introducing new laws to regulate emerging market trends, some experts recommend self-regulation, suggesting that market forces and competition can organically tackle and penalise dark patterns to an extent.[7] Platforms and entities can set standards for themselves, much like the ASCI, to avoid onerous regulation. Moreover, the existing ASCI 'Guidelines for Online Deceptive Design Patterns in Advertising' already discourage the use of drip pricing, bait and switch, false urgency, and deceptive advertising – four of the ten categories of dark patterns listed in Annexure 1 of the incumbent Guidelines. Advertisers expecting self-regulation under the ASCI Code may be brought under the institutional regulation of these Guidelines, which runs contrary to the spirit of the Code.[8]

1.2.2. When the Ministry recently held stakeholder consultations on dark patterns, participants seemed in agreement that industry self-regulation can play a pivotal role in addressing the issue.[9] The Press Release states, "*online platforms can establish ethical design guidelines that discourage the use of dark patterns. Encouraging responsible design practices and conducting independent audits can help identify and rectify dark pattern issues*".[10] We agree with the stakeholders to an extent – striking a balance between regulatory oversight through guidelines and a nodal regulator, and self-regulation among market players, can be an effective framework to curb the use of dark patterns. The Ministry may consider defining broad parameters of dark patterns and providing grievance redressal systems to report them, while encouraging platforms and entities to set market standards to self-regulate. As an illustration, Annexure 1 of the Guidelines can act as an indicative, and not exhaustive, list of dark patterns. Additional dark patterns/deceptive practices can be identified via consumer feedback through established feedback mechanisms under the Ministry or by various market players. The responsibility to limit or discontinue the deployment of dark patterns lies with the market participants.

1.2.3. Dark patterns as a phenomenon are generally difficult to detect and rapidly evolving in form, design, and tactics. Any attempt to create an exhaustive list, especially at this preliminary stage, might be an exercise in futility for the Ministry. Moreover, by defining exhaustive lists of categories and penalising them similarly as other contraventions in the Consumer Protection Act, 2019, the Ministry may run the risk of stifling genuine innovation and healthy market

[7] Arvind Narayanan, et. al., Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces (2020). https://queue.acm.org/detail.cfm?id=3400901

[8] ASCI, The Code for Self-Regulation of Advertising Content in India. https://www.ascionline.in/wp-content/uploads/2023/08/Code-Book_Codes_Web-ready-2.pdf

[9] Ministry of Consumer Affairs, Food & Public Distribution Department of Consumer Affairs (DoCA) and Advertising Standards Council of India (ASCI) host consultation with stakeholders on "Dark Patterns" (Press Release) (June 2023). https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1932105

[10] Ibid.

competition. The categories prescribed in Annexure 1 are undoubtedly helpful for the consumer in identifying deceptive designs, but the Guidelines should not treat them as exhaustive.

2. On the categorisation of dark patterns

2.1. In Annexure 1 of the Guidelines, the Ministry defines ten categories of dark patterns: *false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement,* and *nagging*. This is an apropos illustrative list for a preliminary framework, but does not cover the full extent of deceptive designs and practices prevalent today. Some other practices include *obstruction, social proofs, psychological pricing, growth hacking, linguistic dead-ends, roach motels, privacy zuckering,* and so on – the list is wide and ever-expanding.[11] Some examples of dark patterns in the Indian fin-tech space and their corresponding consumer harms were tabulated by researchers in a recent audit of the sector.[12] Additionally, instances of dark patterns tabulated by us in **Appendix B** reflect that many deceptive designs do not expressly fall into any of the categories provided by the Guidelines in Annexure 1.

2.2. We reserve that the Ministry should not prescribe exhaustive categories for dark patterns, but also acknowledge that new and emerging dark patterns need to be tracked. Considering our proposal that Annexure 1 should be an illustrative tool for consumers to identify and avoid dark patterns, we encourage the Ministry to proactively update it to reflect emerging trends of the time. This can be done by inviting consumers and civil society to report sightings of new dark patterns through a specified portal, or by encouraging them to write to the Ministry or DoCA. Community responses can be a vital resource for policymaking in this regard. Based on survey responses from our community, and media reports, we have collated many instances of the usage of dark patterns that the Ministry may refer to. (**Appendix B**)

[11] See: (for obstruction, social proof) OECD, Dark Commercial Patterns (2022), pg. 53. https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1696486865&id=id&accname=guest&checksum=8B6203C4A92234A4DC40A36EF8571F5A; (for psychological pricing, growth hacking) Arvind Narayanan, Dark Patterns: Past, Present, and Future: the evolution of tricky user interfaces (2020). https://queue.acm.org/detail.cfm?id=3400901; (for linguistic dead-ends) Shun Hidaka, et. al., Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps (2023). https://dl.acm.org/doi/pdf/10.1145/3544548.3580942; Deceptive Patterns, 'Hard to Cancel' https://www.deceptive.design/types/hard-to-cancel; (for privacy zuckering) Wired, How Facebook and Other Sites Manipulate Your Privacy Choices (2020). https://www.wired.com/story/facebook-social-media-privacy-dark-patterns/

[12] Monami Dasgupta, et. al., Tricked by Design: Deceptive Patterns in Indian Fintech Apps, Tales of Bharat (May 2023). https://d91labs.substack.com/p/tricked-by-design-deceptive-patterns

3. On contraventions

3.1. As said above, dark patterns are difficult to detect and rapidly evolving. To apply the Guidelines justifiably in the domain and equitably for small and big entities, we encourage the Ministry to set clear parameters for penalising dark patterns. In our recommendation, the Guidelines could establish an 'intention to deceive' to assess the gravity of consumer harm and extent of penalisation. Owing to their deceptive nature, it may be tricky to see if a dark pattern was employed by an entity with the intention to deceive. But a case-by-case assessment on merits can establish intent, and the entity can be penalised accordingly.

3.2. We do not agree with the argument that only the entities above a certain user base or monetary threshold should be penalised, as small/medium sized entities can also be deceptive. The magnitude of the penalties, however, can take into consideration the size of the firm. We also do not believe that all cases or categories of dark patterns should be subject to the same penalties, as some designs can lead to greater consumer harm than others. For instance, fin-tech and investment entities like PayTM Money and Groww use a combination of nagging, confirm shaming and false urgency to influence personal finance decisions, which can have grave long-term effects on consumer well-being. Entities grievously or repeatedly undermining consumer interests can be assessed and penalised as per the provisions of the Consumer Protection Act, 2019, as provided by Guideline 8.[13]

4. On addressing privacy concerns

4.1. As stated by the Hon'ble Secretary during the Guidelines consultation, "*consent by deceit is not express consent*".[14] Though comprehensive in other regards, the Guidelines do not address the plethora of privacy risks associated with dark patterns. Collection of excessive and unnecessary personal data without informed consent of consumers is a grave threat dark patterns pose to consumer interest. This risk may exist even after the notification of the requisite rules under the Digital Personal Data Protection Act, 2023 ("DPDPA, 2023"), as the Act does not govern interfaces or designs through which personal data is collected. So, there is an urgent need to address this lacuna, and the incumbent Guidelines may be an appropriate medium to do so.

[13] Section 89 of the Consumer Protection Act, 2019 states that "*any manufacturer or service provider who causes a false or misleading advertisement to be made which is prejudicial to the interest of consumers shall be punished with imprisonment for a term which may extend to two years and with fine which may extend to ten lakh rupees; and for every subsequent offence, be punished with imprisonment for a term which may extend to five years and with fine which may extend to fifty lakh rupees.*"

[14] Stakeholder consultation (Press Release), supra.

4.2. We agree with the Ministry and stakeholders, that consumer's personal data collected through manipulation or deception is not collected with consent. We believe that the Guidelines can play a dual role in regulating consumer data collection through dark patterns, in two ways.

4.2.1. First, it could include additional categories of dark patterns that compromise consumer privacy, and provide illustrations of such patterns (such as *privacy zuckering, nagging, privacy maze, bait and switch* and *linguistic dead-ends)* in Annexure 1 to make consumers aware of the data risks associated with them.

4.2.2. Second, the Ministry could suggest standards and principles for platforms or entities engaging in data collection, guiding them on how to minimise the data they collect from consumers, and process it in a transparent manner. Establishing principles like 'privacy by design', which encourage data protection through inherent technology design, has proven to help meet this objective and mitigate consumer data risks.[15] Literature suggests that institutionalising privacy by design significantly contributes to fostering a rights-based approach among entities and implementing privacy law principles in a legal framework.[16] Moreover, we have seen that when consumers are given the option by the entity to minimise the sharing of their data, they will exercise it. Apple launched an App Tracking Transparency feature in 2021, mandating apps to request permission from users to track their activity. A majority of Apple's consumer base started to prefer declining app permissions.[17]

4.3. In other jurisdictions, there are protections in place specifically against collection or use of consumer data obtained through dark patterns. The Colorado Privacy Act, 2021 does not recognise consent obtained through dark patterns.[18] It defines dark patterns as UI designed or manipulated with the substantial effect of subverting or impairing user autonomy or decision making. The California Consumer Privacy Act, 2018 prohibits companies from preventing consumers from opting out, or complicating the language of their privacy policies.[19] EU Guidelines on deceptive design patterns in social media platform interfaces also mandate data protection by design and by default, placing privacy considerations of the consumer at the

[15] European Union, General Data Protection Regulation, Privacy by Design. https://gdpr-info.eu/issues/privacy-by-design/
[16] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564791
[17] Fast Company, Most people are embracing iOS 14.5's new anti-tracking features (2021). https://www.fastcompany.com/90633965/ios-14-5-tracking-opt-out-rate#:~:text=Compared%20to%20the%20average%2037,%2C%20and%20entertainment%20(31%25).
[18] Colorado Privacy Act, 2021. https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf
[19] California Consumer Privacy Act, 2018. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

fore.[20] Similar regulatory standards can be considered for in the Indian context, after due consideration and diligence on their applicability.

4.4. When it comes to dark patterns, privacy-respecting standards are a popular means of governance in self-regulating environments. The Network for Advertising Initiative (NAI) in the United States, a self-regulating advertisers' network comparable to the Indian ASCI, released 'Best Practices for User Choice and Transparency' in 2022.[21] These standards address dark patterns involving collection of consumer data, and provide specific recommendations encouraging companies to maximise transparency, consent, and choice for consumers when it comes to the collection and use of their data. The Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) of the Advertising Standards Authority, a similar body in the UK, contains principles addressing certain dark patterns such as drip pricing, disguised advertisements and subscription traps.[22] In keeping with our recommendations to strike a balance between regulatory oversight and self-regulation, the Ministry along with ASCI may encourage standard-setting in the domain, while providing broad oversight and guidance.

4.5. Additionally, in the stakeholder consultation, the Ministry considered equipping users with tools and resources (like browser extensions, apps or plugins) that allow them to make informed choices online to protect them from privacy risks and dark patterns. While consumer empowerment is crucial, the onus of preventing harms caused by dark patterns should not be shifted to the consumer. We believe that features such as accessible privacy policies, customisable settings, default opt-outs, etc. must be built into the design of the platform or entity. This can be enforced in law through these Guidelines or other future frameworks by the Ministry in tandem with MeitY and the DPB.

5. On grievance redressal systems

We believe that through these Guidelines, the Ministry has an opportunity to strengthen existing enforcement mechanisms and grievance redress channels established by the Consumer Protection Act, 2019. To better implement the Guidelines on Misleading Advertising, DoCA along with ASCI launched the Grievances Against Misleading Advertisements (GAMA) portal.[23]

[20] EU Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them (2023). https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[21] NAI, Best Practices for User Choice and Transparency (2022). https://thenai.org/best-practices-for-user-choice-and-transparency/

[22] ASA, Shedding some light on "dark patterns" and advertising regulation (2022). https://www.asa.org.uk/news/shedding-some-light-on-dark-patterns-and-advertising-regulation.html

[23] DoCA, GAMA Portal. https://gama.gov.in/Default.aspx

The portal's usage may be expanded in this instance and aggrieved consumers can be directed to the portal for expedited and easy redressal, instead of creating a parallel mechanism. Notwithstanding the portal, the Guidelines should clearly set out all the recourses available to an aggrieved consumer to file complaints against dark patterns, including the general route under the Act of approaching the District Consumer Disputes Redressal Commission as well as DoCA's National Consumer Helpline (NCH 1915).

Appendix B

IFF's Dark Patterns Tracker

We, at IFF, conducted a community survey asking ordinary consumers to recognise and describe dark patterns they come across in their daily lives (**B.1.**). Additionally, we undertook a sweep of media reports flagging various instances of dark patterns, to identify recent trends in the domain (**B.2.**). In our preliminary assessment, we observe the following:

1. The scope and modalities of what can constitute a 'dark pattern' is almost indefinite – it is already vast, and continues to evolve rapidly. The ten categories prescribed by the Ministry in Annexure 1 of the Guidelines are adequate as illustrations, but cannot be an exhaustive list.
2. The highest instances of dark patterns were reported in payment related actions across platforms, and the second highest were noted to be subscription traps.
3. Not only private platforms, but there was one instance of a government platform engaging in alleged dark patterns, a domain that may be a blindspot in these Guidelines.

B.1. Community Survey Responses

Below is an anonymised tabulation of responses we received through our survey. The columns correspond to the platform or entity identified by the responder, a broad categorisation of the dark pattern by us based on the ten categories provided in the Guidelines at Annexure 1, and a brief description of the dark pattern, as submitted by the responder, with minor edits from us.

	Entity	Dark pattern	Dark pattern description
1	Adobe Creative Cloud	Subscription trap	Cancelling a subscription, or even signing up for one month is extremely deceptive - with very high cancellation charges. This is already on top of very complicated cancellation process where you have to go through multiple screens of them offering you lower prices/free products just to keep you in the loop
2	Air Asia	Bait and switch	Airasia on ticket booking told I can do 1 check in, 1 carry on and 1 hand luggage and at the airport told me carryon which was within wt limit/size limit can not be taken as carry on and I had to pay for extra baggage and extra weight to put that bag in checkin and all the extra hassle of moving my electronics while the weight was within the limits.

3	Airtel	Subscription trap	Airtel doesn't let us cancel broadband connection despite many requests online and visits to shops.
4	Airtel Thanks	Forced action	A user needs to download this application if they want to know who called you while your phone was unreachable. Earlier this information used to get delivered over an SMS. Now the SMS asks you to download this app if you need this information.
5	Airtel Thanks	Subscription trap	Does not give you an option to cancel or end your broadband package early. They let you pause it or change its address but you cannot end it without calling customer care. Even the customer care is mostly automated and doesn't give you an option to cancel. You need to *somehow* know the correct digits to enter to get to speak to a human agent and then ask them (repeatedly) to end your plan. Extremely frustrating, led to me paying for an extra month.
6	Airtel Thanks	Subscription trap	App has no method to cancel a subscription. They only list a complaint and have a 4-7 day call back which comes from a spam number. They charge for this interim period. The app has no faq for disconnect. Their own field team cannot connect to IVRS. They charge a full fees and have no method to move refund amount. No method to request a refund.
7	Ajio		Charging convenience fee of ₹99. These are arbitrarily imposed and there is no clarity regarding what services we are paying extra for. Terms like "convenience fee" or "fulfilment fee" are vague as can be.
8	Ajio		Most platforms like Ajio, Myntra, Swiggy, Smytten, etc are charging extra "convenience fees". Sometimes it goes as high as 299 Rs for some people based on returns. Some platforms charge % of the total cart value as convenience fee. Even if it is based on returns, there are platforms that avail products (skincare, etc) that have no returns.
9	Ajio		Ajio had 80₹ delivery charges and even still has 20₹ convenience charges. And promising free delivery.
10	Amazon	Subscription trap	Hard to cancel prime. On buying prime it sets up recurring autopay

11	Amazon	Bait and switch, drip pricing	Flash sales where you strike of the original price and give offer price but in reality it's the normal sale price
12	Amazon	Bait and switch, drip pricing	I was browsing amazon.in in incognito mode with the first search being related to laptops. Then I came to the home page and visited a flash sale. Then I saw a banner with women in revealing clothes. they are using images of women to drive in more sale and engage audience
13	Amazon	Bait and switch, drip pricing	Fake Discounts - amazon is showing the kindle edition price (£12.99) compared to the print list price (£19.99 crossed out). The kindle list price is actually £12.99 and has not changed since launched
14	Amazon	Disguised advertisement	why many listings from its brands were marked “sponsored” in the source code but not to the public. The company told us those were not search results or ads but “merchandising,” labelled “featured from our brands.” Ads from the platform should be labelled as such.
15	Amazon	Various	Lightning deals, adding prime membership to the cart directly when it’s due to expire, audible subscription, if not renewed, cancels free credits given to the user every month, flashing "only 1 left" signs in carts
16	Amazon		I will get random email from Amazon and on first glance it looks legit but those are not from ex ad@amazon.com but from Amazon...@somerandomcompany.com. And unsubscribing is literally used by these scammers to confirm your email id.
17	Amazon		The concept of false rebates in Amazon and other eshopping website. For example, product values are shown as high as 10000 rs, but offer ridiculous discounts of 70-90%. It’s obvious that the value if the products are near to the discounted price. This is an unnecessary rebate system used by many companies selling below par or basic items. There is nothing wrong with being cheap, but its marketed under massive discounts. A very bad and misleading practice where people get mislead to buy products they expect to be a higher quality.

18	Artistry Goa	Subscription trap	Booked a concert ticket once from Artistry Goa's website. Received regular promotional emails from Artistry Goa (via events@wearenocturnal.com) without subscribing. The email had no unsubscribe button (unethical/illegal?). Eventually had to resort to writing a threatening email to get unsubscribed.
19	Axis Mutual Fund		In order to redeem your units from your portfolio, you have to go through this maze of confirmation buttons. You have to confirm at least thrice before it lets you redeem your units. The "skip" or "cancel" buttons are brightly coloured, whereas the "confirm" button is either greyed out or less colourful. Even after you successfully finish the process, it will ask you to "click here" with a bright coloured button, but next to it, greyed out is the text saying "If you wish to cancel your redemption".
20	Bajaj Finance	Bait and switch, false urgency	My mother never applied for this card but she is getting messages like this which claim she has applied but actually redirects to a sign up flow. This should be illegal. Counts as a Dark Pattern as per FTC: Some dark patterns manipulate consumer choice by inducing false beliefs. For example, a company may make an outright false claim or employ design elements that create a misleading impression to spur a consumer into making a purchase they would not otherwise make.
21	Bigbasket		Scamming people to add money into their account wallet and then redeeming the money without notifying the user or providing any services.
22	Blinkit	Bait and switch, interface interference	Push notifications should not have the same copy as system functions. I also had not ordered anything. I saw this and thought someone was trying to call me and then realised it's just a random notification.
23	Blinkit	Basket sneaking	Putting random things that we searched for in our cart. Often seen that they swap certain similar items when the original product is not in stock.
24	BluSmart		"Pay without saving card" option is less visually inviting, coloured in gray, while "Pay and save card" is displayed prominently in blue.
25	BoAt	False urgency	Ending In:<time> this message is there daily.

26	BookMyShow	Basket sneaking	Book My Show’s ₹1 donation is turned on by default? The FTC says it is a Dark Pattern. FTC report “Bringing Dark Patterns to Light”. Appendix A, Page 22 says: SNEAKING OR INFORMATION HIDING Sneak-into-Basket. Automatically adding items to the shopping cart without a shopper’s permission OR Tricking a shopper into buying unwanted items by using a pre-checked box.
27	BookMyShow	Subscription trap	The URL link provided for unsubscribing to emails (to which I have not subscribed to begin with) doesn’t work.
28	Bumble		I cancelled the subscription but the amount gets debited from my account anyway.
29	Bumble	Subscription trap	There is no visible unsubscribe button. There is no unlink payment method option in settings,which says subscription won't be cancelled by unlinking.
30	ChatGPT		By default, ChatGPT users allow OpenAI to use their data for model training, exposing them to memorization risks. The opt-out interfaces unnecessarily link privacy with reduced functionality, and the more flexible control is hard to find and use.
31	CRED	Basket sneaking	In the Cred app, when you try to withdraw CredCash, in the last step they automatically and discreetly add ₹499 for insurance. The design makes it such that it's very tough to identify the toggle button to unselect the insurance option. In the end, users end up buying insurance too. That was very sneaky from Cred's side. Their design is good but the UI uses a dark pattern and this is my hands-on experience.
32	Croma	Drip pricing, deceptive advertising	Listing products for sale for unbelievably low price and then blocking check out. They claim it is an error but don't update the price to increase website traffic. It's like free advertisement but all lies.
33	Duolingo	Interface interference	The app has advertising for free users. There is a mute button which they keep moving around and is blended with the advertisement. Unable to mute the ad or end up clicking on it.

34	Facebook	Bait and switch	facebook gives you fake notifications to make you engage in the app. For example even if you don't use the marketplace app you will have a notification bubble in the marketplace tab to make you see the marketplace. even if you don't follow someone you get notification. you will get content from things you don't even follow. there is no way to disable this.
35	Financial Express	Deceptive advertising	Publishing articles on celebrities (especially Bollywood actors/actresses) paid by their PR in news paper's Entertainment section. These are technically ads but nowhere in the article they mention it as a paid article.
36	Flipkart	Nagging, forced action	Notifications Configuration being clubbed such that you can only subscribe to transactional updates if you also subscribe to sales notifications.
37	Flipkart	Bait and switch, drip pricing	Different prices shown to logged in customers, on the same pincode and from the same seller.
38	Flipkart	Forced action	Sneaky marketing with Byju’s. The Byju's demo is added as mandatory. You remove that and the main product is removed as well.
39	Flipkart	False urgency	Spam emails with subjects that are phrased for urgency. It is a dark pattern that really misleads the recipient
40	Flipkart		Delete your account permanently. There is an option to delete, but you cannot delete the account.
41	Flipkart		Secured Packaging Fee on products such as mobile phones. Basically delivery charge without the label, all while marking it as 'Free Delivery'. They are charging between 50-100 rs depending on product value.
42	Flipkart	Drip pricing	Flipkart that charges ₹60-100 as secure packaging charges and charging ₹10 extra on some deals
43	Furlenco	Bait and switch, subscription trap	Home page and the payment page shows there will be a discount for one year subscription plan. But the disclaimer of no refund when the product is returned in the one year subscription plan is mentioned nowhere except in the support section . After you return the product the customer executive only informs you on the phone about the policy. You will be left with no product and no refund.

44	Google	Bait and switch	The search query that you put into the search box (Google or any other search engine) is replicated word by word into the title of a link on the results page, in order to lure you into clicking on it, and then you realise the page is nowhere related to your query, and you were just baited into clicking on it thinking it was exactly what you were looking for.
45	Google		When signed in to Google with multiple email accounts, there is currently no option available to sign out of individual accounts individually. As illustrated in the attached screenshot, the only available option is to sign out of all accounts simultaneously.
46	Google Chrome		Chrome is trying to trick you into believing that enabling their security feature gives you more privacy.
47	Google Location Services		GLS repeatedly prompts users to permit the usage of location. It only displays the “don’t show me again” option and does not provide an actual decline option. In both cases users can decline, but not permanently.
48	Hathway	Nagging	Hathway provides broadband service in Bangalore. It has been spam calling for the past 7 months to get a new connection after I disconnected it. I have requested them to stop calling me several times but they don't listen and continue calling me to this day at odd hours.
49	Hotstar Mobile App		When using the Hotstar mobile app to watch live matches of the ICC Cricket 2023 World Cup, while the ads that appear in between the overs are not a concern, there is an issue with the screen brightness when viewing in full-screen mode during ads. The screen brightness automatically increases to max ONLY during ads irrespective of your screen brightness settings.
50	Indigo	Drip pricing, forced action	Dark Patterns of forcing users to PAY for seats, only to perform a simple web check-in. Consider giving an option to Auto check-in, rather than only "Select Paid Seats?" Also common with other airlines as well. Limiting auto-checkin to a specific time frame without clear indication of it on the ticket itself is a dark pattern.

51	Instagram		Instagram uses gaslighting to make content more and more engaging. For example, Instagram will show you things you love first for eg: cars in between the reels they test you with things you may like like women. they use this info to subconsciously give you more edgy content and ads. you will never know what they know about you since you will be in the midst of something you like.
52	Instagram		While using the website on your mobile browser, it has gotten really hard to use it unless you download the app. Same with Facebook. Also, uploading a same ‘picture/video’ file on Instagram from your iphone has better quality than from android.
53	Instagram		Almost impossible to deactivate account, especially if you select “taking a break” upon deactivation. They also have a 7 day limit before which you can’t deactivate again!
54	Instagram		Steps to follow: 1. Open the Instagram app. 2. Navigate to the "Reels" section. 3. Begin scrolling through the Reels feed. 4. Occasionally, Reels from certain accounts, such as 'abc' (for example, content related to hospitals, medical procedures, or sensitive subjects), appear, which may not be suitable to view. 5. To address this, tap on the three dots located at the bottom right corner of the Reel, then select "Not Interested," followed by "Don't suggest posts from 'abc' account." After taking these steps, the next Reel should start playing. 6. The issue arises when a message appears stating, "Thanks, we won't suggest Reels from this account," and this message remains active for at least 6 seconds. This is problematic because it covers the bottom three dots on the right side of the screen. Consequently, if the following Reel also contains content that the user finds inappropriate, they are compelled to watch it for the entire 6-second duration, including audio and video. There is no option to skip it, except for scrolling, which might lead to a repeated recommendation of similar content.
55	Ixigo		When booking they'll automatically select their 100% refund plan for a sum of extra rupees, even if we uncheck and continue they'll ask a yes or no confirmation but it's asked in such a way that we'll unknowingly accept it again ...

56	Jio Set top box		The jio STB plays its own ads in place of YouTube ads. I think this violates
57	JioCinema	Nagging	Regular request for turning on notifications,when consciously wanting no such push notifications. Asking so on every opening of the app
58	Just Pay	Interface interference	Opt-out button is grey and super unhighlighted, making it seem like it is not an available option
59	Justdial.com		When you try to cancel your Justdial's monthly subscription, they ask you to submit a request with the support team, and they say once it's approved then the plan will be cancelled after 3 months! So basically if you find their service useless and want to cancel it, you still have to pay for next 3+ months (taking into account the time they would take additionally to approve your cancellation request)
60	Ketto	Nagging	Once donated to Ketto organisation and was mandatorily required to share a phone number. Despite promising that the number will not be used to send messages, ppl from Ketto organisation have called on multiple occasions to donate for a fundraiser. They kept pushing to donate and it was uncomfortable. Randomly got a call from an unknown number and upon receiving, there was some caller from some NGO asking for donation. On asking where they got my number, they said they have "purchased my number from a vendor".
61	Kotak Securities		had to liquidate my holdings because the bank made it hard to transfer the stocks.
62	Lenskart	Basket sneaking, drip pricing	Lenskart adds a Convenience Fee on a purchase of their membership, inflating the price of the product.
63	MakeMyTrip	Bait and switch, drip pricing	Fraudulent advertisement of high discount amounts, when they are not available. The MMTSUPER discount T&C page (Grab Up to Rs. 2000 OFF* on Domestic Flights.) is archived at, and says upto 2000 rupees off on domestic flights. However, on trying to book the costliest flights I could find (Srinagar - Kochi, return flight worth 1.75 Lac), the discount still maxes out at 400 rupees.

64	MakeMyTrip	Basket sneaking	Makemytrip by default enables "Donate ₹5 to relief fund" on their payment pages. These are usually amounts less than ₹10, but when compounded can go into Crores — you only need 20L transactions where customers didn't mind that ₹5 extra amount during payment to reach ₹1 Cr, giving them that small validation.
65	MakeMyTrip	Basket sneaking	Insurance and charity donation boxes are checked by default.
66	MakeMyTrip		Mmt takes convenience fee for booking and for cancellation as well.
67	Meta		Facebook has made it complicated to delete the Facebook account.
68	Mobile games	Interface interference	Very small close button. When I press the close button it automatically redirects to an ad site
69	MyGate	Interface interference	App has ads that appear a bit later or update a few microseconds so you accidentally click on the advertisement.
70	MyGate	Interface interference	The app has advertisements on top. They resize the ad after it appears so you accidentally click on it. It resizes to be above the main useful buttons. Forcing accidental clicks etc. They do the same with banner ads too.
71	Myntra	False urgency	only x items left
72	Myntra		Charging convenience fee of ₹99. These are arbitrarily imposed and there is no clarity regarding what services we are paying extra for. Terms like "convenience fee" or "fulfilment fee" are vague as can be.
73	Myntra		Most platforms like Ajio, Myntra, Swiggy, Smytten, etc are charging extra "convenience fees". Sometimes it goes as high as 299Rs for some people based on returns. Some platforms charge % of the total cart value as convenience fee. Even if it is based on returns, there are platforms that avail products (skincare, etc) that have no returns. So it doesn't make sense to charge additional fees.
74	Nykaa	Confirm shaming	Sad emojis with the description “I don’t want freebies” when unchecking something from the cart. Repeated hounding with messages on WhatsApp from multiple accounts even after blocking them

75	Nykaa Fashion		Charging of convenience fee on every order placed.
76	Ola		The app will charge a random surge fee if a destination is added, even if its on the way and does not add any kilometres or proportionate waiting time for additional stop. For example a 8km ride at 150rs can become 500rs if the distance is 8km. They have a random default policy of only one refund even if drivers refuse trip. The ui forces you in circles without a resolution.
77	PayTM		Charging extra for every transaction under the title "platform fee".
78	PayTM		The UI advertises cashback points. When you redeem the cashback it tends to have rs1 offers but ridiculous shipping of 199 or 299 for even the smallest items, this is mentioned in legal terms, hard to catch. Deceptive practice. The coupons they provide are easy to accidentally click which is an ad coupon. Mostly for gambling websites.
79	PayTM		The concept of cash back points in PayTM as it translates to nothing. The points appear so high but actually offer discounts on unheard products. Also, the unfair malpractice tempting people to use those points to enter into lottery systems to win desirable products.
80	PayU India Payments Flow	Interface interference	A greyed out, but lightly checked checkbox for saving cards. This makes the checkbox appear disabled, and tricks users into thinking they don't have a choice.
81	Phonepe		Stops from making a payment saying that it's for my safety. Other UPI apps let me make the payment. The real dark pattern is that there is no way of reaching customer service by chat or call in their help section. They just have different questions and answers but nowhere to submit queries that aren't solved by those questions.
82	Plantum	Interface interference	Popups do not have a prominent close button. It is almost invisible.

83	PolicyBazaar	Nagging	Policy Bazaar harasses users with cold calls when the policy expires. In my case I answered the first call and let them know that I am not renewing as I'm leaving the country for good and to please take me off their call list. They said okay. And then every single day I got atleast one call (multiple calls when I didn't answer) for the same renewal. I got tired of telling 5-6 executives what my reason for not renewing was and asking them to please stop contacting me. The insurance company (Star health) did the same thing. So for one cause, I had two companies hounding me to renew after communicating on the phone. It's mentally taxing to deal with these. In my case since it wasn't a discontinuation of the policy, it was simply non renewal, I had no way to really "opt out" of this menace.
84	RTI website Indian govt	Interface interference	The captcha system does not work, it takes dozens of attempts and refresh pages to get a captcha that matches the correct answer.
85	Redmi		The issue pertains to an app that comes pre-installed on every Redmi device, known as 'Security.' This app is part of the default software and cannot be removed from the device's settings by any user. The cause for concern lies in the permissions granted to this app, which include access to 'call logs, contacts, phone functions, SMS, and even additional permissions related to BLE settings'. Importantly, these permissions cannot be revoked by the user.
86	Smytten		Most platforms like Ajio, Myntra, Swiggy, Smytten, etc are charging extra "convenience fees". Sometimes it goes as high as 299Rs for some people based on returns. Some platforms charge % of the total cart value as convenience fee. Even if it is based on returns, there are platforms that avail products (skincare, etc) that have no returns. So it doesn't make sense to charge additional fee.

87	SonyLiv		When you access the sonyliv.com website with an adblocker enabled (example in Google Chrome), you'll encounter a message that reads, "Ad Blocker Detected!" This message presents two options: "I have disabled Ad blocker, Reload" and "No Thanks!" However, there is an issue with the latter option. Instead of being a functional button, it is presented as plain text. This discrepancy in the design should be rectified to make the "No Thanks!" option an actual button for better user experience.
88	Spotify		Cancelling spotify premium membership is not possible through phone apps. They don't have any direct button to cancel premium membership.
89	Swiggy	Drip pricing	Numbers in invoices are rounded up or down to make up for the maximum profit. Swiggy claimed this was a invoicing bug, but needs to be investigated further for real confirmation.
90	Swiggy		Charging extra on every order as platform fee even when I have signed up for their extra one subscription.
91	Swiggy		In the final bill, instead of rounding up to the next number it adds an extra 2-3 rupees. eg: if total comes to 285.6, instead of adding 0.4 to make it whole they add 3.4 make it 289.
92	Swiggy		Platform fees. Emotional manipulation to tip the riders
93	Swiggy		Swiggy charges "platform fee", they make it seem as if they're giving us a discount by striking off ₹5 and showing ₹3, telling that they're giving us a discount of ₹2 on the platform fee. This fee is just nonsense.
94	Swiggy		Most platforms like Ajio, Myntra, Swiggy, Smytten, etc are charging extra "convenience fees". Sometimes it goes as high as 299Rs for some people based on returns. Some platforms charge % of the total cart value as convenience fee. Even if it is based on returns, there are platforms that avail products (skincare, etc) that have no returns. So it doesn't make sense to charge additional fees.

95	Swiggy		Charging extra delivery charges for rain even if its not raining. This has happened so many times in different cities. I remember once I literally shared the pic of the sky as it was bright sunlight and there were no clouds. They made an excuse that the restaurant area has rainfall. The restaurant was nearby (I could see the area from my terrace). There was no rainfall.
96	Swiggy		Swiggy in Bangalore, too many times the restaurant will not send all the items and customer care gave no refund. Have lost thousands in their fault.
97	Truecaller	Forced action	Truecaller makes a list of all the people that see my profile. It gives me a notification which doesn't say anything about additional fees and once I click on the notification, it asks me to buy a premium membership to see who has seen my profile. Basically, advertising features as free but then asking a fee.
98	Twitter	Disguised advertisement	Twitter is not marking all ads as ads any more.
99	Twitter	Forced action	Twitter suspends all new accounts that are created without a phone number. As soon as you try to use your new account, created with an email address, it gets suspended, and twitter requires a phone number to verify and unsuspend your account. As a result, Twitter's dark pattern forces users to part with their mobile number which twitter uses for advertising and tracking purposes. Twitter also has a history of using phone numbers provided for one purpose (2FA) for ad targeting, for which they were fined.
100	Twitter		Automatic enrollment into data tracking and ad personalization without an opt-out.
101	Uber/Ola	Drip pricing	Their surge pricing is an algorithm that uses demand from an individual i.e. need of individual to vary their prices. This is against competition law, the ideal calculation for demand is an aggregate, from a certain group of people. Ideally this group should be geographical, or demographic for the definition to come into play. This individualistic pricing mechanism is borderline and feels like its taking advantage of individual circumstances.

102	Uber/Ola/Rapido/Namma Yatri	Nagging	Extremely difficult to cancel rides. The app takes you through multiple steps just to cancel. Promotional ads come back even though notifications for the same have been blocked around a month ago
103	Upstox (Angel Broking)	Nagging, false urgency	All through the process applications make frequent use of urgency in completing sign-up as fast as possible. During the setup and installation, the default options selected allow the applications to reach consumers through push notifications, alerts, email, and text (sometimes WhatsApp) messages. This allows the apps to ensure their regular presence through frequent notifications. During sign-up behaviourally-framed messages often emphasise on riskier trade options such as intraday trading. For instance, during sign-up, the Angel Broking application sent in notifications of free vouchers, brokerage, but also how users can begin trading in under an hour with an accompanying stop-watch. There were also calls for users who left the registration halfway through, to encourage them to complete documentation.
104	Urban Company	Subscription trap, confirm shaming	Subscription trap for 6 months membership before the checkout page - the option to decline is worded "I want to pay full price" and the page shows up after checkout, right before completing the purchase, which could make a user think that they're paying for their cart
105	Various		Notifications say “This is your salary day, order food now”

106	Various		Fake close buttons on ads. Buttons too small to accurately close. Overlays blocking close buttons. Influencers traveling to other countries where disclosure of promotion is not required, posting a video, then returning to the US. Sometimes on Non-Amazon websites they will give you a coupon to get a small percentage off your total, but not disclose upfront that it switches your products in cart to a subscription. Spotify more than once has “given” me free months after I cancelled a subscription, only for me to find they never cancelled my subscription when I requested it and I was going to be charged the next month, so I have to re-request cancellation. They didn't charge me for the "free" months, I had no say in whether or not I wanted that service short of uninstalling the app. But they definitely did not honor my cancellation request despite receiving the confirmation email that my subscription was cancelled at my initial request. More common, but used a lot, I see companies that have a free version of their product (I usually grab the free version first to try it out). But immediately on opening the website or app, you're presented with payment options and the skip/close/no thanks is so small and barely readable or clickable.
107	Various	Nagging	Constant messages on WhatsApp from business accounts of Airtel, Reliance, Jio, Tata Croma etc. I never signed up for WhatsApp updates in the first place. Even after replying STOP/NO for further communications, they keep sending the messages.
108	Youtube		Youtube gives you topics like your religion to trick you into watching content. for example they will use religious videos inbetween shorts to make you engage more in shorts. youtube fingerprints browser and geolocation. for example, if you use youtube in firefox in incognito mode they will store the fingerprint of your browser and location. next time you watch a specific content you get content from the same channels you watched. for example if you watch content from techlore and then watch print and the next day if you watch techlore you get print content next. this happens in firefox using incognito mode with cookies cleared

109	Zomato	Basket sneaking	Zomato used to have its donation enabled by default, seems like they do not any longer, regardless if there is a checkbox asking for your donation. But because their customers have given their money to these companies, they count this donation amount towards *their* CSR contribution for the year. It is mandated by law for companies with net worth of ₹500Cr+, or a turnover of ₹1000Cr+, or a net profit of ₹5Cr+ to spend at least 2% of their net profits on Corporate Social Responsibility projects, i.e., donations to relief funds or charities / NGOs. So essentially their customers end up paying the legally required money instead of the corporation paying from their own pockets by using this loophole. This law only applies to big corporations, which ironically can make good use of this loophole because of their huge customer base, which would mean a higher turnover from enabling small donations by default on payments page. As a cherry on top of the shitpile, corporates aren't required to spend all their CSR funds on charities & NGOs, a majority of this CSR fund is spent on advertising the company being the saviour of the unprivileged by donating so charitably :)
110	Zomato		Zomato has some platform fee too.
111	Zomato		One incident with Zomato where they try to resolve this issue when the restaurant didn't send the food and they told we feel your pain but can't do anything as the mobile given by the restaurant to Zomato is wrong. No refund and this was a big part of the order missing. I had to Google search restaurant no and send them the details so they can talk with them and still Zomato didn't refund. They gave my no to Restaurant and I had to resolve it. Still no refund. Food was hours late at that point.
112	Zomato		Zomato charges an extra 3 rupees per order.

B.2. Media tracker

Below is a tabulation of media reports on dark patterns prevalent in or affecting Indian markets.

	Entity	Dark pattern	Source
1.	Byju’s	Byju’s offered loans to hundreds of unsuspecting parents at the time of enrolling their children for online coaching classes. The parents’ biometric impressions taken at the time of enrolment were used to give them loans that they had not sought. Of the small sample of the parents, 50% had no information that they had purchased a loan in the guise of a free trial.	Journal article
2.	Meta	In 2020, Instagram updated its direct messaging services to create vanish mode. Upon clicking the vanish mode, an update dialogue appears that does not explicitly tell the users that they are about to link their Instagram account to Facebook Messenger. Post-this-exercise, Facebook reported that more than 60% of users adopted interoperability between Instagram and Messenger. The design of the apps downplays key information and uses confusing language to deceive or manipulate users to bypass consent.	Journal article
3.	Telcos (various)	Adding free OTT subscriptions with WIFI/mobile connections which auto-renew after 3-6 months without user consent, sometimes adding the OTT sub fee to the user's phone bill.	Blog
4.	Google	Testimony during Google’s antitrust case revealed that the company may be altering billions of queries a day to generate results that will get you to buy more products.	Report
5.	Groww, Upstox, PayTM	Right after enrolling into the popular app Groww, users see behaviourally framed messages which build an urgency to invest. “Didn’t Invest yet? It’s a good day to start investing”. Upstox uses a similar design element – users will see a sad emoji if there are no orders placed. Another example of attention prompts is when cues within the apps leverage social proofing to nudge investments. Paytm Money makes use of socially framed nudges on its home screen such as, “11,12,649 investors have already invested via Paytm Money”. Such an instance is classified as a dark pattern that makes use of social proofing, leveraging people’s fear of missing out.	Report

6.	Twitter	Twitter prompted users to provide their telephone numbers or email addresses for security purposes, such as to enable multi-factor authentication, secure their accounts, etc. But behind the scenes, this data was being used to serve people targeted ads.	FTC Blog
7.	Various	An FTC Report outlining various instances of dark patterns in the United States.	Report

INTERNET
FREEDOM
FOUNDATION

Internet Freedom Foundation
I-1718, Third Floor, Chittaranjan Park,
New Delhi 110019

policy@internetfreedom.in
internetfreedom.in