UNPACKING DARK PATTERNS: UNDERSTANDING DARK PATTERNS AND THEIR IMPLICATIONS FOR CONSUMER PROTECTION IN THE DIGITAL ECONOMY

[*]Beni Chugh & [**]Pranjal Jain

ABSTRACT

This paper examines the increasing use of dark patterns in digital interfaces and the concerns they raise for consumer protection. Dark patterns are user-interfaces that confuse, coerce, or manipulate users into making a decision that does not reflect their underlying preferences. By exploiting users' cognitive biases and reinforcing users' information asymmetry, dark patterns impair their decision-making abilities. They coerce users into disregarding their preferences and acting against their best interests. This can cause significant harm in rapidly digitizing economies and societies. Dark patterns are already being used to steer users to sign up for financial products they may not need. They are also influencing citizens' political choices and interfering with democratic processes. These incursions into users' autonomy significantly disenfranchise and disempower them in the digital economy. Further, emerging research suggests that users with lower levels of education and earning lower levels of income are more vulnerable to dark patterns. These findings are crucial for jurisdictions such as India where the use of the internet is fast expanding to rural parts, and there is a rise in first-generation users of the internet.

Here we analyze the use of dark patterns in digital interfaces and the influence they exert on users' decision making. It distinguishes dark patterns from persuasive advertisements and sets out a list of common dark patterns to examine their adverse consequences for consumers. It advocates for regulatory intervention to arrest the proliferation of dark patterns on the internet and remedy the power imbalance they have already wrought. It concludes with some open questions that India must contend with when regulating dark patterns.

[*] Beni Chugh, Research Manager, Future of Finance Initiative at Dvara Research.
[**] Pranjal Jain, Co-founder of theUXWhale, Alumnus of Dvara Research.

I. INTRODUCTION TO DARK PATTERNS

Until recently it was common for travel portals to bundle travel insurance with travel tickets. They used pre-checked boxes to default the user into buying the insurance cover, even when the user had shown no active interest in purchasing the product or understanding it. Exhibit 1 demonstrates a screenshot of a transaction, typical of travel portals in India until recently.

Exhibit 1: Use of pre-checked buttons to bundle insurance cover with travel tickets | Source: *MoneyControl*[1]

This use of pre-checked buttons to bundle travel cover with travel tickets is a classic example of a 'dark pattern'. Dark patterns are *"user interfaces that make it difficult for users to express their actual preferences or that manipulate users into taking actions that do not comport with their preferences or expectations"*.[2] The term 'dark pattern' was coined by Harry Brignull in 2010, who defined it as interface designs that *"trick users into doing things that they might not want to do, but which benefit the business in question*".[3] Dark patterns use the design of the interface to influence users to make choices they would not have made if

[1] *Explained: Here is why airlines, portals can no longer mis-sell you travel insurance from Oct 1*, Moneycontrol, available at https://www.moneycontrol.com/news/business/economy/explained-here-is-why-airlines-portals-can-no-longer-mis-sell-you-travel-insurance-from-oct-1-4492451.html, last seen on 23/12/2020.

[2] *Stigler Committee on Digital Platforms, Final Report,* Stigler Committee, available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf?la=en, last seen on 23/12/2020

[3] H, Brignull, *Dark Patterns: inside the interfaces designed to trick you*, The Verge, available at https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you, last seen on 23/12/2020.

the user interface did not distort the information presented to the user or limit the user from acting on that information.

In the example above, the use of pre-checked boxes assumes that the user's default preference will be to purchase an add-on financial service. Users are expected to expend costly time and attention to uncheck the box and opt out of the default purchase. This default setting is unfair and taps into users' cognitive limitations. Users are known to be less likely to opt-out of existing defaults as they are beset by several cognitive biases and severe cognitive inertia, that keep them from questioning default options.[4] Research from other jurisdictions suggests that when travel insurance covers travel tickets, even those users who did not intend to buy the cover, end up buying it. Even more worryingly, a sizeable proportion of buyers remains unaware that they purchased the cover, implying that they may never actually benefit from the insurance.[5]

Recognizing that pre-checked boxes disempower users by leveraging their cognitive biases, the Insurance and Regulatory Development Authority of India ("**IRDAI**") has prohibited travel portals in India from using them for selling travel insurance. IRDAI has directed travel insurance companies to "*ensure that any portal or App providing the travel insurance coverage shall not pre-select the option of buying the travel cover as a default option*".[6] The regulator further emphasized that prospective buyers of insurance products should be allowed to make an "*informed choice"* before buying them. This regulatory

[4] *General Insurance Add-Ons Market Study – Remedies: banning opt-out selling across financial services and supporting informed decision-making for add-on buyers*, Financial Conduct Authority, UK, available at https://www.fca.org.uk/publication/policy/policy-statement-15-22-general-insurance-add-ons.pdf, last seen on 23/12/2020; E.J. Johnson, S. Bellman & G.L. Lohse, *Defaults, Framing and Privacy: Why Opting In-Opting Out*, 13 Marketing Letters 5, (2002), available at https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf, last seen on 23/12/2020; *Consumer Rights Directive*, Brussels: European Commission, available at https://ec.europa.eu/info/policies/consumers/consumer-protection_en, last seen 23/12/2020.

[5] *General insurance add-ons: Provisional findings of the market study and proposed remedies*, Financial Conduct Authority, available at https://www.fca.org.uk/publication/market-studies/ms14-01.pdf.

[6] *Circular on Travel Insurance Products and operational matters*, IRDAI, available at https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo3913&fl, last seen on 23/12/2020.

intervention shines a light on the increasing use of dark patterns and the questions it raises for consumer protection in the digital economy.

II. EFFECT OF DARK PATTERNS ON USERS' DECISION-MAKING ABILITIES

Dark patterns differ from other marketing strategies in the effect they have on users' preferences. Their objective is to make consumers disregard their own preferences and act in a manner inconsistent with them. They are designed to be manipulative rather than persuasive,[7] to encourage users to make decisions they would not have made if not for their influence. This is in sharp contrast to persuasive marketing efforts that influence users to revise their preferences.[8] This is evident in the example of the bundling of travel insurance cover with the travel ticket. The travel portal does not introduce the buyers to the product or convince them of its utility to influence their preferences. Instead, it resorts to directly adding the travel cover to the buyer's purchase, regardless of their preferences.

A growing body of scholarship is investigating the effects of dark patterns on the decision-making process of users by drawing on Tversky & Kahneman's Dual Process Theory.[9]Kahneman & Tversky's research suggests that humans have two modes of thinking: *System* 1 thinking and *System 2* thinking. *System 1* thinking is prompt, unconscious, automatic, less laborious, and less rational. *System 2* thinking tends to be more conscious, rational and laborious. Researchers suggest that dark patterns appeal to *System 1* of the human brain, encouraging users to make impulsive decisions that could serve the interests of the providers better than the interests of the users.[10]

---

[7] Supra 2.

[8] J. Luguri & L. Strahilevitz, *Shining a light on Dark Patterns*, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205, last seen 23/12/2020.

[9] A. Tversky & D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases,* 185 Science 1124, 1131 (1974).

[10] C. Bösch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 2016 Proceedings on Privacy Enhancing Technologies, 237–254 (2016); J. Luguri & L. Strahilevitz, *Shining a light on Dark Patterns*, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205, last seen 23/12/2020.

Users' decisions are influenced by the way information is presented to them. Features of the design interface such as the language in which information is presented, the functional hierarchy including the placement of the information, the font type, size and color used to present the information, influence the users' decisions. Digital interfaces and accompanying choice architecture can be used to exploit users' cognitive vulnerabilities. The choice architecture is informed by a deep understanding of the users' behavioral biases, their bounded rationality, cognitive inertia and the constraints on the time and attention of users when they make decisions. As expert depositors in the Federal Trade Commission ("**FTC**") submitted, dark patterns are designed through extensive research and A-B testing. Designers experiment with interface designs and choose the ones most likely to distort the information and choices available to the users and cloud their decision-making. As a result, consumers' "*choice opportunities are just completely muddled and clouded by the little tricks that companies play*".[11]

Pre-checked boxes are one such design feature. Other design features include the careful wording of users' options and the choice of font color and the placement of buttons to close windows or to skip ads. For instance, IRDAI's ban on pre-checked boxes does not prevent the travel portal from deploying other forms of dark patterns to manipulate the consumer into buying the product. Portals pay special attention to the language used to frame users' choices. Exhibit-2 demonstrates this wordplay, where the option to refuse the purchase of the travel insurance is crafted as "*I am willing to risk my trip*". This creates a sense of fear among consumers and guilts them into revising their choices– a dark pattern identified as '*confirmshaming*'.[12]

[11] *Competition and Consumer Protection in the Twenty-First Century*, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_1_4-9-19.pdf, last seen 24/12/2020.

[12] *What are dark patterns?,* Dark Patterns, available at https://www.darkpatterns.org, last seen on 24/12/2020.

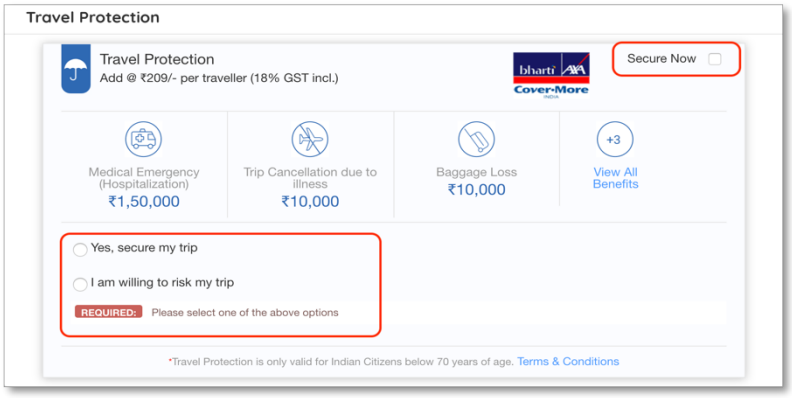

Exhibit 2: The option of not buying the insurance product is worded as "I am willing to risk my trip". This articulation creates a fear and guilt in the consumer, coercing them into compliance. This is 'confirmshaming'.

Source: Screengrab from a leading travel portal in India.

Though coercive practices in advertisements are not new, dark patterns raise concerns because of the scale and pervasiveness of their use. The prevalence of dark patterns across the web is unknown quantitatively, but a recent study[13] examined dark patterns on a set of most popular e-commerce websites. The study included 53,000 product pages across 11,000 shopping websites, and it found over 1,800 instances of dark patterns being deployed by these websites. The study suggests that these digital retailers used dark patterns to trick users into buying products they did not want. The following section discusses some typical dark patterns and the adverse outcomes they create for consumers.

III. SOME TYPICAL DARK PATTERNS AND THEIR IMPLICATIONS FOR CONSUMER OUTCOMES

Dark patterns steer users to give precedence to the providers' interests over their own. Our 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. The first objective of maximizing sales is not unique to digital service providers. The second objective of maximizing personal information has heightened relevance for

[13] A. Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 Proceedings of the ACM on Human-Computer Interaction (2019).

digital service providers. In the digital economy, it is a common practice for providers to offer products and services at zero monetary prices. Even when consumers do not pay a monetary price for the services they consume, it is well established that consumers compensate digital providers with their personal data.[14] The value of users' personal information for digital service providers can be best gauged by the fact that most Big Tech companies generate a sizeable portion of their revenues from the sale of advertising.[15] Further, the prices they command from advertisers are positively correlated with the variety and depth of personal information they have on prospective buyers.[16] Some dark patterns seek to influence the user into buying products and subscribing to services, or giving away more personal information than they would prefer. We classify these adverse effects of dark patterns into:

i. perpetuating deceptive and unsuitable selling practices, and
ii. nudging consumers to share excessive personal information.

1. Perpetuating Deceptive and Unsuitable Selling Practices

Dark patterns proliferate deceptive and unsuitable selling practices by:

1.1 Subscribing the user to a product or service she did not want

These techniques deceive the user into buying products or services that they did not intend to buy. Some typical dark patterns used to achieve deceptive sales include *sneak in the basket, forced continuity, urgency* and *scarcity*. *Sneak in the basket practices* use pre-checked boxes to trick consumers into buying products or services without some affirmative action or informed consent on part of the user. *Forced continuity* practices deceive the users into subscribing to paid subscriptions at the end of free trials. It uses credit card details taken at the time of free trial to automatically subscribe users to paid services without warning or requiring any affirmative action from them.

[14] *Quality Considerations in Zero Price Markets*, The OECD, available at https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf, last seen 24/12/2020.
[15] Ibid.
[16] D. Srinivasan, *The Antitrust Case Against Facebook*, 16 Berkeley Business Law Review Journal (2019).

Similarly, *urgency* and *scarcity* practices are used to create the impression of scarcity to make the user purchase a product or service.

1.2 Subscribing user to a product or service that is not in their best interest

These selling practices nudge the user to act against their best interests by choosing products or services that may not be beneficial to them. This is typically encouraged by using dark patterns that hide information crucial for decision-making such as the true costs of the product (a dark pattern called *hidden costs),* add irrelevant choices to distract users (*misdirection*), guilt the users into making a choice not beneficial for them (*confirmshaming*) or by asymmetric presentation of choices.

Asymmetric presentation of choices in the case of dynamic currency converter has been a burning consumer protection issue in the European Union ("**EU**"). Travelers on international trips are often confronted with a choice to make payments using their native currency or the local currency of the destination. Buyers are naturally disposed to pay in their native currency because of their comfort with it. However, payments in native currency abroad often make the transaction expensive for the buyers because they attract conversion costs. Simultaneously, providers stand to gain by the additional conversion fee. Consumer groups across the EU have underscored providers' tendency to subtly encourage the users to pay in the more expensive native currency by presenting this option in a benign 'green color' as illustrated in Exhibit 3. This reinforces consumers' cognitive bias associated with the color green and encourages users to make payments in the more expensive native currency.[17]

[17] *Dynamic Currency Conversion: When paying abroad costs you more than it should*, The European Consumer Organization, available at https://www.beuc.eu/publications/beuc-x-2017-118_dynamic_currency_conversion_position_paper.pdf, last seen 24/12/2020.

Exhibit 3: ATMs in EU Countries.

1.3 Making it harder for the consumer to discontinue or opt-out of existing purchases and subscriptions

Dark patterns are also used to retain consumers in ongoing services by making it harder for them to discontinue or opt-out of existing subscriptions. The 'Roach Motel' dark pattern is used to keep users subscribed to services by requiring them to go through several pages before they can opt-out. It resembles the classic maze in which entering a maze is easy but finding the right path out is much more difficult.[18] 'Roach Motel' is used while designing interfaces for cancelling subscriptions, deactivating accounts or unsubscribing from a mailing list.

2. Nudging Consumers to Share Excessive Personal Information

In a rapidly digitizing economy, users' data is an important economic input[19] and providers seek to maximize the data collected from users. Dark patterns such as 'Privacy Zuckering' (encouraging users to share more personal information publicly) and 'Trick Questions' (tricking users into giving answers they did not intend to) sway users into sharing more personal data than they intended to. A recently concluded study shows that

[18] Supra 12.
[19] *The economic value of data: discussion paper*, Government of United Kingdom, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf, last seen on 24/12/2020.

dark patterns can set back the effectiveness of consent management platforms. Removing the opt-out button from the first page of the notice increases instances of users giving consent by over 22 percent.[20]

In concluding this discussion on typology, the table below summarizes the most prevalent dark patterns found in our review of literature and their effects on consumers' outcomes.

Dark Pattern	Description	Intended effect on users
Sneak in the basket	Tricks users into buying products without their informed consent.	Subscribes users to unwanted products or services.
Forced continuity	Deceives users into subscribing to paid subscriptions via free trials.	Subscribes users to unwanted products or services.
Expensive autorenewals	They renew subscriptions to the most expensive business models.	Subscribes users to services that are not in their best interest.
Urgency	Makes users believe that purchases are urgent.	Manipulates users to subscribe to products or services.
Scarcity	Makes users believe that products are scarce.	Manipulates users to subscribe to products or services.

[20] *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence,* Honolulu: Association for Computing Machinery, available at https://arxiv.org/pdf/2001.02479.pdf.

Hidden costs	Hides true costs of products.	Subscribes users to services that are not in their best interest.
Misdirection	Adds irrelevant choices to confuse users.	Subscribes users to services that are not in their best interest.
Confirm shaming	Guilts users into buying products.	Subscribes users to services that are not in their best interest.
Asymmetric presentation of competing choices	Represents competing choices asymmetrically, making one look more appealing than the other.	Manipulating the user to make a choice that may not be in their best interest.
Roach motel design	Makes it hard to unsubscribe a product or service or abort transactions.	Subscribes users to unwanted products or services.
Privacy Zuckering	Encourages users to share more personal information publicly.	Encourages users to share excessive personal information.
Trick Questions	Tricks users into giving answers they did not intend to.	Encourages users to share excessive personal information.

Table 1: Some common dark patterns and their effect on consumers' outcomes.

Source: Compiled by the authors based on their review of the literature.

IV. DARK PATTERNS: A CALL FOR ACTION TO REGULATORS?

The decision to regulate dark patterns rests on at least two important considerations- (i) the inability of users to safeguard themselves from dark patterns, and (ii) the inability of market competition to penalize the use of dark patterns.

1. The Inability of Users to Safeguard Themselves from Dark Patterns

Although empirical research on the effect of dark patterns on consumers is still quite young, a recently concluded American study examines the efficacy of a bait and switch dark pattern that persuaded users to buy an identity theft protection plan.[21] The experiment, conducted on a group of over 1900 respondents, found that the respondents' willingness to enroll into identity theft protection plan was significantly and positively related to their exposure to dark patterns. The respondents' enrolment rates in the identity theft protection program more than doubled when they were exposed to mild dark patterns, while it quadrupled for those exposed to aggressive dark patterns.

More worryingly, the findings of this study also show that respondents with lower levels of education are more vulnerable to dark patterns. In the control group (i.e., in the absence of dark patterns) level of education of respondents did not affect their decision to enroll in the program. However, in the presence of dark patterns, respondents with lower levels of education exhibited higher rates of enrolment. The study also found that respondents with low levels of income are likely to be more influenced by dark patterns. These findings emphasize that individuals belonging to disadvantaged and marginalized groups are more vulnerable to dark patterns.

This has significant implications for India, which is characterized by low income, low levels of digital literacy and a sizeable proportion of first-time users of the internet. Journalistic reports suggest that individuals with lower levels of education and in urgent need of money make for easy targets for financial service providers. Often users also sign-up for financial products unintentionally and unknowingly. Notably, an ed-tech company, Byju, 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 examined in

[21] Supra 8.

this report in 'The Ken', 50 percent had no information that they had purchased a loan in the guise of a free trial.[22]

Similarly, it is also common for users to face significant deterioration in their financial condition because they signed-up for financial services without fully knowing their terms and conditions.[23] Though these are instances of mis-selling of products in traditional finance, these are likely to get worse when first-generation digital users are influenced by dark patterns while accessing digital finance.

2. The Inability of Market Competition to Penalize the use of Dark Patterns

Competition in markets is a powerful tool to uphold consumer protection.[24] Competition in markets enables consumers to choose from a wide variety of providers and reject providers that offer inferior products. This incentivizes providers to compete on the quality of the product. However, market failures that arise when providers' incentives are not aligned with the consumers' best interest are unlikely to be redeemed by competition. This appears to be true of dark patterns. Although the empirical research is still quite new and limited, it is beginning to show the limitations of market competition to address dark patterns.

In their ground-breaking study, researchers from Princeton found that shopping websites that were more popular as per Amazon's Alexa rankings were more likely to deploy dark patterns.[25] Similarly, the American study discussed earlier found that the use of mild dark patterns by digital providers is likely to go unpunished.[26]

---

[22] *The making of a loan crisis at Byju's*, The Ken, available at https://the-ken.com/story/the-loan-crisis-at-byjus/, last seen on 24/12/2020.
[23] *Selling to those who can't pay: human cost of modern banking*, The Ken, available at https://the-ken.com/story/human-cost-of-modern-banking/?utm_source=daily_story&utm_medium=email&utm_campaign=daily_newsletter, last seen 24/12/2020.
[24] *Indian Financial Code*, Financial Sector Legislative Reforms Commission, available at https://dea.gov.in/sites/default/files/fslrc_report_vol2_1.pdf, last seen 25/12/2020; *Report of the Financial Sector Legislative Reforms Commission*, Government of India, available at https://www.prsindia.org/report-summaries/financial-sector-legislative-reforms-commission, last seen 25/12/2020.
[25] Supra 13.
[26] Supra 2; Supra 8.

In summary, emerging evidence suggests that dark patterns are fast becoming an instrument of competition rather than competition being a restraint on the use of dark patterns. The market mechanism *per se* may be inadequate to address the consumer protection concerns raised by dark patterns. Simple, subtle dark patterns that are effective in manipulating the consumer attract little or no backlash from the consumers. Consequently, they appear to be increasingly prevalent among popular service providers. Moreover, though dark patterns diminish users' autonomy and welfare across the board, their effects are more pronounced for the already disadvantaged groups such as those with lower levels of education.[27]

V. CONCLUSION: OPEN QUESTIONS FOR REGULATORS WHEN REGULATING DARK PATTERNS

Discussions so far indicates that the use of dark patterns warrants regulatory intervention. However, regulatory approaches to dark patterns must contend with a few frontier questions:

1. Distinguishing between Personalization and Manipulation

The distinction between personalization and manipulation has been at the heart of policy issues that stem from the use of personal information in the supply of services. Moreover, the distinction between personalization and manipulation is subject to the social-cultural context of the users, their own privacy preferences and the outcome of the interface design. As an example, using behavioral data to understand users' preferred payment methods and modifying the interface to present the most-used payment method upfront may reduce friction in users' payment experience and increase convenience. However, if that preferred-payment mode attracts an additional transaction fee then many would argue that the interface's design amounts to dark patterns. The line between personalization and manipulation is not only thin but it is also murky because it is fraught with subjective assessments of the designer's intentions, implications for consumer welfare and the consumer's own value system.

[27] Supra 2.

An exclusively objective standard of distinguishing personalization from manipulation may not be feasible or even warranted. Scholarship from behavioral economics can lend some ideas on creating a framework to distinguish manipulative dark patterns from benign nudges. Thaler and Sunstein define nudges as "*any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives*".[28] Their emphasis on the effect of a nudge being predictable and not changing users' economic incentives could serve as important indicators for identifying dark patterns which are likely to fail on one or both counts.

It is crucial that a framework to identify dark patterns incorporates and reflects society's expectations, value-system, and cultural context. The community's engagement is essential to determine choices that cannot be squarely addressed by the law and where the trade-offs are more intricate. For instance, in our small but deeply qualitative study in 2017, respondents unequivocally expressed their reservations against providers using their location data.[29] These findings were also corroborated by other primary studies, such as those undertaken by Consumer Unity and Trust Society[30] ("**CUTS**"). Any default settings that permit providers to collect users' location data when it is not strictly necessary to provide a service will be adjudged as a dark pattern. Any determination of dark patterns cannot be made in isolation from the socio-cultural context and with disregard for the community's perceptions. To achieve this, regulators must crowd-in opinions from the community, engage in inclusive public consultations, conduct primary studies to gauge users' privacy preferences and be transparent about their decision-making processes.

2. Appointing Appropriate Regulatory Body to Regulate Dark Patterns

[28] R. Thaler & C. Sunstein, *Nudge - Improving Decisions About Health, Wealth, and Happiness*, 6 (2008).
[29] *Privacy on the Line*, Dvara Trust, available at https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf, last seen 25/12/2020.
[30] *Is privacy an elitist concern? Not so, says new survey*, The Scroll, available at https://scroll.in/article/899168/is-privacy-an-elitist-concern-not-so-says-new-survey, last seen 25/12/2020.

Appointing a relevant regulator to oversee dark patterns is not straightforward. Dark patterns could attract several regulators' jurisdictions simultaneously. Regulators with direct jurisdiction over dark patterns include a data protection authority, the consumer protection authority and the sectoral regulator(s) that has jurisdiction over the provider using dark patterns. Simultaneous jurisdiction can lead to duplication of regulation or regulatory arbitrage.

The IRDAI did not have jurisdiction over travel portals, in the example of travel portals using prechecked boxes to sell insurance cover. It had to rely on regulated entities i.e. travel insurance providers to enforce the ban, as also reflected in its language, "*Insurers shall ensure that any portal or App providing the travel insurance coverage shall not pre-select the option of buying the travel cover as a default option"*.[31] While the regulator was able to achieve its objectives in this case, it does highlight the problem that sectoral regulators may not have jurisdiction over e-commerce entities or social networking platforms. This can create a patchy regulatory framework and may not protect users effectively from the use of dark patterns.

The existing consumer protection authority is emerging as a strong contender to regulate dark patterns due to its economy-wide jurisdiction. In the United States, the Federal Trade Commission ("**FTC**") which is the federal body in charge of consumer protection in the economy has been regulating dark patterns and penalizing service providers by using its power to punish "*unfair and deceptive practices"*.[32] The case of *Federal Trade Commission* v. *AMG Capital Management*[33] is an important ruling on dark patterns. AMG Capital Management, a payday lender, deployed dark patterns to auto-renew (instead of close) expensive payday loans to borrowers. Borrowers were deceived into believing that their loans would be closed after withdrawing the principal amount and the interest rate in one instalment from their bank account. The interface, however, was not designed to close the loan. Prechecked boxes in the loan agreement ensured that the default

[31] Supra 6, S. 3(iii).
[32] 15 U.S.C. S. 5 (United States).
[33] Federal Trade Commission v. AMG Capital Management, 19-503 (2021, United States Court of Appeals for the 9th Circuit).

option was set to auto-renewal of the loan. Auto-renewals directed users to more expensive subscription models, and, Roach Motel models ensured that users could not change the extortionist default settings easily.[34] The FTC found AMG Capital Management guilty of unfair and deceptive practices under Section 5 of the FTC Act. The Court of the Appeals of the Ninth Circuit also upheld the FTC ruling, and the amount of penalty (USD 1.3 bn) levied on the provider.[35]

The language of the FTC Act and its interpretation of deceptive practices allowed the FTC to book the offender and punish them for their misconduct. The success of existing consumer protection authorities in regulating dark patterns will depend on the language of the existing regulation and its ability to include dark patterns in the cause of action. In India, some dark patterns such as *hidden costs* could fall under the remit of the Consumer Protection Act, 2019 and the Central Consumer Protection Authority ("**CCPA**") that the Act creates to redress such issues. Section 11(ii) of that Act considers the deliberate withholding of important information as a deficiency in service that is punishable under the Act. Similarly, Section 28(iv) of the Act considers it as 'misleading advertisement'. Other dark patterns such as *confirmshaming*, however, are harder to fit into this consumer protection framework. The inability to qualify these dark patterns as offences under the consumer protection framework could significantly constrain the regulator's effectiveness in regulating their use.

To overcome these issues, existing consumer protection frameworks could be amended to equip them to deal with dark patterns. American senators introduced the 'Deceptive Experiences to Online Users Reduction ("**DETOUR**") Act'. This Bill aims to curb the use of dark patterns by banning interface features that intentionally diminish consumers' autonomy, ability to make decisions and choices. It also gives the FTC more authority to regulate such practices and provide guidelines to

[34] Supra 8.
[35] Supra 33.

platforms on design practices.[36] Consumer protection bodies with amended legislations that allow them to regulate for dark patterns could help in creating a consistent consumer protection framework. It could also spare consumers the anxiety of navigating a new regulatory body with a new set of mechanisms.

3. Designing Effective Regulatory Tools to Regulate Dark Patterns

Designing appropriate regulatory tools is crucial to the success of regulators. Considering that regulating dark patterns is a recent regulatory preoccupation, there is limited research on the tools that regulators could use to address it. Some tools that appear useful from the preliminary analyses of issues and emerging research include:

3.1 Auditing of organization's design practices

Regulators can periodically audit digital interfaces to gauge the effect of the interfaces on users' decision-making capacity and agency. Audits could look for designs that foster deceptive and unsuitable selling or nudge users to share excessive personal information. Lessons can be drawn from the audits designed to prevent algorithmic bias as a way to promote compliance in the automated systems.[37] As algorithms become more embedded in decision-making in the economy, providers are leaning on researchers and journalists to examine their algorithms for discrimination.[38] Similar collaborations could be explored to audit digital interfaces for dark patterns. In addition to audits, regulators could also lay out model

---

[36] *Senators Introduce Bipartisan Legislation to Ban Manipulative 'Dark Patterns'*, Mark R. Warner, US Senator from the Commonwealth of Virginia Website, available at https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns, last seen on 26/12/2020.

[37] B. Casey, A. Farhangi & R. Vogl, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, 34 Berkeley Technology Law Journal 143 (2018), available at https://ddl.stanford.edu/sites/g/files/sbiybj9456/f/Rethinking%20Explainable%20Machines.pdf, last seen on 25/12/2020.

[38] *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms*, University of Michigan, available at http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf, last seen on 25/12/2020.

interfaces or guidelines to help providers design user-friendly interfaces, such as those set out by the IRDAI or the FTC. Regulators could also mandate a design practice where the opt-in and opt-out choices presented to the users are equal in hierarchy and comprehensible for all users. These guidelines may be especially relevant when regulators rely on digital interfaces for enforcing laws. For instance, the effectiveness of the German law to regulate hate speech online- the 'Netzwerkdurchsetzungsgesetz' ("**NetzDG**" or the "**Network Enforcement Act**"), was significantly compromised because of dark patterns. The law mandated social networks to offer users a form to report unlawful content online. In some cases, significant providers with millions of users made the pathway to reporting hate speech lengthy, convoluted, and requiring multiple clicks from users. This reduced reporting incidents and considerably reduced the effectiveness of the Act.[39]

3.2 Developing bright-line rules to detect dark patterns

Creating bright-line rules, i.e., objective standards to detect dark patterns can help regulators remove ambiguity around what is permissible. These standards can be a crucial benchmark against which user interfaces can be measured to assess if they exert undue influence over users' autonomy. Further, bright-line rules should reflect the users' ideal expectations of the providers. A-B testing of interfaces should not only be conducted to maximize providers' interests[40] providers could also solicit users' feedback on the design interface to make it user friendly.

Dark patterns can enable the economic exploitation of users and their disenfranchisement by limiting users' ability to exercise their rights on digital interfaces and vitiates regulation. Together, these possibilities highlight the need and urgency to regulate dark patterns. The urgency is warranted by the disproportionate effect that dark patterns are likely to wield on users from disadvantaged and marginalized groups. This is especially relevant for demographics such as rural internet users in India,

[39] S. Reigers & C. Sanders, *Dark Patterns: Regulating Digital Design* (Berlin: Stiftung Neue Verantwortung 2020); *Dark Patterns and Policy*, Data and Society Points, available at https://points.datasociety.net/dark-patterns-and-design-policy-75d1a71fbda, last seen on 25/12/2020.

[40] Supra 11.

who have started to outnumber urban users.[41] With significantly less exposure to the internet, lower levels of literacy and potentially lower levels of awareness about dark patterns, these users are more vulnerable to their deployment by providers.

The government's push for digitization in the last decade will lack legitimacy if digital interfaces cannot be safe for users. Rural respondents in our primary study, Privacy on the Line*,* emphasized their inability to comprehend or audit providers' practices on digital interfaces and the lack of agency and means to demand recourse from them. The respondents in our study unanimously emphasized the need for a guarantee that the providers' activities will not harm them and the need for the government to intervene should harm occur.[42] Given the expansion of the internet to first-time users, the policy push for digitization and the users' demand for more safeguards in the digital economy, the call for action to regulators cannot be stronger.

References:

Justice Srikrishna committee submits report on data protection. Here're its top 10 suggestions, Econmic Times, available at https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms.

India's Personal Data Protection Bill: What we know so far, MoneyControl, available at https://www.moneycontrol.com/news/technology/indias-personal-data-protection-bill-what-we-know-so-far-4297331.html.

Dark patterns in UX: how designers should be responsible for their actions, UX Collective, available at https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c.

Johnson, E. J., Bellman, S., & Lohse, G. L, *Defaults, Framing and Privacy: Why Opting In-Opting Out,* 15 Columbia University Faculty Research, 5, 15

[41] *India has more internet users in rural areas than urban: IAMAI report*, The Hindustan Times, available at https://tech.hindustantimes.com/tech/news/india-has-more-internet-users-in-rural-areas-than-urban-iamai-report-story-1EsbphWTBM5wZzjtNFXXyJ.html, last seen on 25/12/2020.

[42] Supra 28.

(2001), available at https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf.

The economic value of data, Government of UK, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf.

Personal Data: The Emergence of a New Asset Class, World Economic Forum, available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

How Businesses Are Collecting Data (And What They're Doing With It), Business News Daily, available at https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

Cooper, J, *Personalization: The Key to Monetizing Your Content*, Adobe Blog, available at https://theblog.adobe.com/personalization-key-monetizing-content/.

Wilson, S, *Every Cognitive Bias Put Into a Single Diagram*, Clinically Relevant Insights BLOG, available at https://www.shawnwilsonphd.com/post/2017/10/06/every-cognitive-bias-put-into-a-single-diagram.

Should Restaurants Offer Healthy Menu Options?, The Balance Small Business, available at https://www.thebalancesmb.com/should-restaurants-offer-healthy-menu-options-4147177.

Lai, Y.-L., & Hui, K.-L, *Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns*, SIGMIS CPR '06: Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research, 253, 263 (2006).

Hanson, J. D., & Kysar, D. A. (1999), *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 Harvard Law Review 149 (1999).

Luo, S., Gu, B., Wang, X., & Zhou, Z., *Online Compulsive Buying Behavior: The Mediating Role of Self-control and Negative Emotions*, ICIEB '18: Proceedings of the 2018 International Conference on Internet and e-Business. Singapore: Association for Computing Machinery (2018).

Zhang, F., Yuan, N. J., Zheng, K., Lian, D., Xie, X., & Rui, Y., *Mining consumer impulsivity from offline and online behavior,* UbiComp '15: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing Osaka Japan: Association for Computing Machinery (2015).

Luo, X., *How Does Shopping with Others Influence Impulsive Purchasing?* 15 Journal of Consumer Psychology 288-294 (2005).

Calo, R., *Digital Market Manipulation*, 82 George Washington Law Review 57 (2019).

Google Location Services: Spam, UXP2 - Dark Patterns, available at https://darkpatterns.uxp2.com/pattern/google-location-services-spam/.

Unfair and Deceptive Trade Practices, Mass Legal Help, available at https://www.masslegalhelp.org/consumer/unfair-deceptive-trade-practices.

User-Centered Design Basics, Usability.gov, available at https://www.usability.gov/what-and-why/user-centered-design.html.

Frederick, S., Loewenstein, G., & O'Donoghue, T., *Time Discounting and Time Preference: A Critical Review*, 40 Journal of Economic Literature 351, 401 (2001).

Confirmation bias, Science Daily, available at https://www.sciencedaily.com/terms/confirmation_bias.htm.

Prasad, S., *Defining "Harm" in the digital ecosystem,* Dvara Research, available at https://www.dvara.com/blog/2019/05/06/defining-harm-in-the-digital-ecosystem/.

Calo, R., *The Boundaries of Privacy Harm*, 86 Indiana Law Journal (2011).

Why is data important for business, Grow, available at https://www.grow.com/blog/data-important-business.

Akerlof, G. A., *The market for "lemons": Quality uncertainty and the market mechanism. In Uncertainty in economics*, 84 The Quarterly Journal of Economics, 488, 500 (1970).

How to Monetize Your Customer Data, Gartner, available at https://www.gartner.com/smarterwithgartner/how-to-monetize-your-customer-data/.

The Data Brokers: Selling your personal information, CBS News, available at https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

Filing complaint against Grindr's sharing users' HIV-status and sexual preferences, Forbrukerrådet, available at https://www.forbrukerradet.no/side/filing-complaint-against-grindrs-sharing-users-hiv-status-and-sexual-preferences/.

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower. Politico, available at https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/.

The Role of Advertising and Advertising Regulation in the Free Market, Federal Trade Commission, available at https://www.ftc.gov/public-statements/1997/04/role-advertising-and-advertising-regulation-free-market.

Hanson, J. D., & Kysar, D. A., *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 Harvard Law Review 1420 (1999).

Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, Cornell University, available at https://arxiv.org/abs/2001.024795.