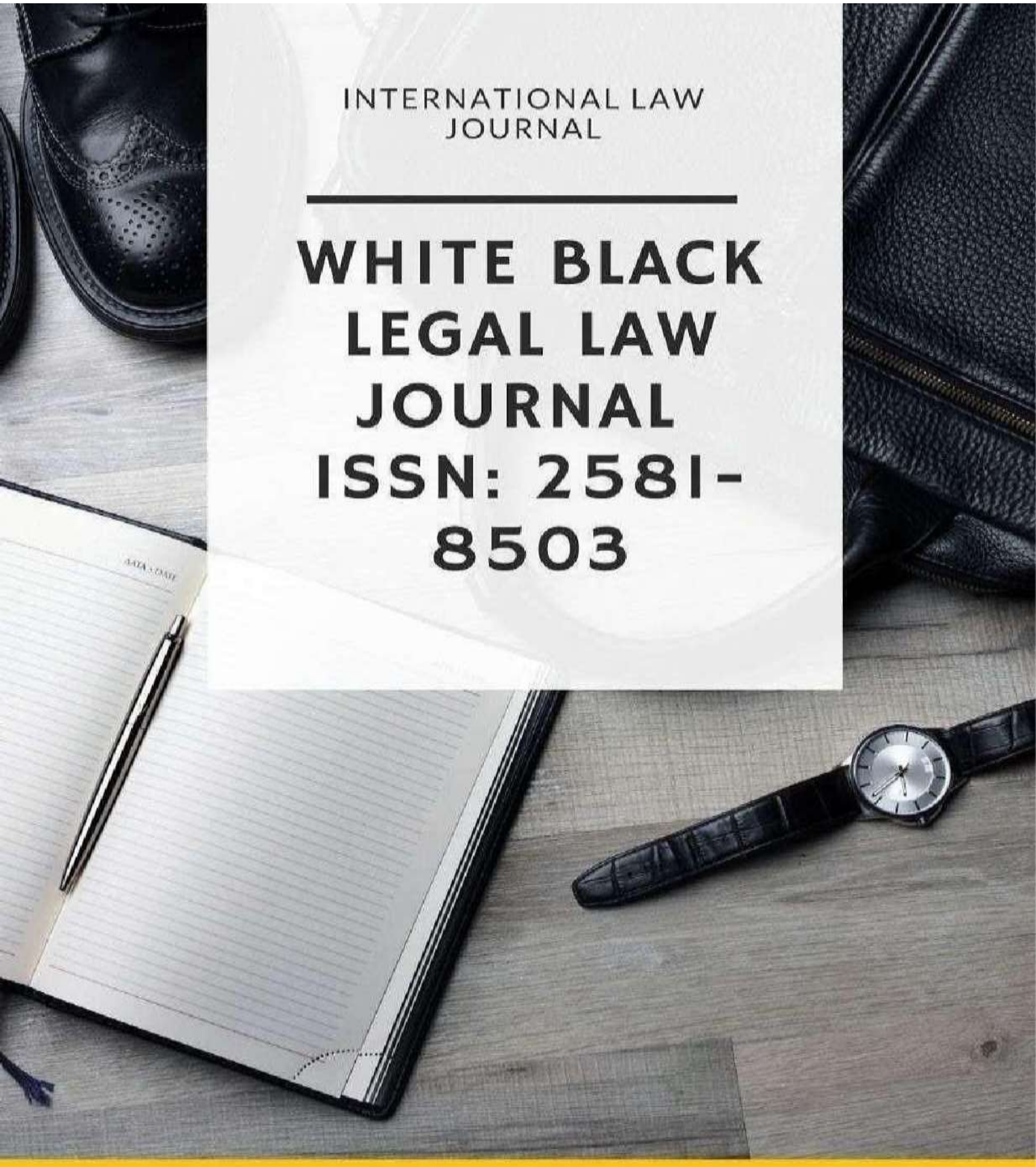

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

THE EVOLVING LIABILITY CONUNDRUM AROUND DARK PATTERNS

AUTHORED BY - TVISHA ZATAKIA

INTRODUCTION

The regulation of dark patterns is an important topic owing to the economic downturn faced by the consumers when organisations and e-commerce platforms employ faulty design architecture or dark patterns. As researched by the International Consumer Protection Enforcement Network (ICPEN) in 2019, nearly 429 websites or applications from a pool of 1760 options, that is nearly 24% could be flagged for potential 'dark pattern nudges', the top three practices being drip pricing, pressure selling and design issues revolving around obscure and obliterate terms and conditions. [1] Impactful research, conducted in 2019 by the Princeton University in the United States found almost two thousand illustrations of dark patterns being employed from an array of 11,000 websites being used by retail businesses and online marketplaces. An extensive research conducted by CSCW ultimately examined more than 11,000 e-commerce websites to conclude that more than 14% used dark patterns, the most popular one being impulse buying as used by more than two hundred e-commerce and travel websites.[2] Since consumers also tend to use mobile devices to access e-commerce platforms, a research study conducted by De Geronimo manually examined more than two hundred and forty popular mobile applications, to infer that 95% of these applications employed dark patterns with almost seven patterns being used by each application on an average.[3] A study of Northeastern University found almost 2320 instances of dark patterns across multiple services with almost eight hundred and thirty-four dark patterns found being employed for the app modality, seven hundred and fifty six for mobile browsers and

---

[1] Organization for Economic Cooperation and Development, *Dark Commercial Patterns: OECD Digital Economy Papers*, 336 OECD ILIBRARY 55 (Oct. 26, 2022), https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1707135816&id=id&accname=guest&checksum=C09AFF503D737DA4AFF8EF1F428CCA0.

[2] Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM. - COMPUT. INTERACT. 81 (2019).

[3] Linda Di Geronimo et al., *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, 473 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 5 (2020).

seven hundred and thirty for the desktop browsers.[4] The following paper aims to expand on the regulation of dark patterns using the fundamental concepts of cognition and consent, ultimately leading to suggestions for consumer satisfaction. Section 1 of the paper deals with the fundamental understanding of the human cognition further exploring the different types of dark patterns, Section 2 deals with interplay between privacy and cognition, Section 3 deals with global initiatives to regulate dark patterns while Section 4 deals with the Indian guidelines exploring critiques and loopholes, ultimately ending with suggestions pertaining to effective redressal of consumer complaints by the Consumer Forum.

COGNITION AND DARK PATTERNS

The Greek equivalent of discover, 'heuristic' is "an approach to problem-solving that takes one's personal experience into account."[5] "In the digital context, companies often use dishonest design —commonly known as dark patterns— to trick or push consumers into doing thing they wouldn't have done otherwise"[6], and this heuristic becomes the rationale behind dark patterns.

Dark patterns are those illusory designs which hold the potential to influence "human psychology."[7] As defined by the Indian Consumer Protection Authority, these patterns include both "practices and deceptive design patterns using UI/UX (user interface/ user experience) interactions on any platform."[8] The Indian Ministry of Consumer Affairs' Guidelines on Dark Patterns[9] specifies thirteen such patterns. Many companies present a bogus claim that creates a "sense of urgency"[10] in the mind of the user. Herein the user comprehends such a false claim as large demand or known paucity in the near future. This is a well-known trick used by the aviation and hospitality industry. It is also used in the B2C (Business to Consumer) segment as it manipulates the consumer into making an impulsive choice on the basis of a "False Urgency"[11] created intentionally by the designer or the company.

"Basket Sneaking"[12] is another such deceptive feature where supplementary items are added to

---

[4] Johanna Gunawan et al., *A Comparative Study of Dark Patterns Across Mobile and Web Modalities*, 5 PROC. ACM HUM. - COMPUT. INTERACT. 377, 377:13 (2021).
[5] Steve Dale, *Heuristics and Biases: The Science of Decision-Making*, 32 BUS. INFO. REV. 93, 93 (2015).
[6] Alison Hung, *Keeping Consumers in the Dark*, 121 COLUM. L. REV. 2483, 2483 (2021).
[7] AGNIESZKA KITOWSKA, *THE HOWS AND WHYS OF DARK PATTERNS: CATEGORIZATIONS AND PRIVACY*, *IN* HUMAN FACTORS IN PRIVACY RESEARCH 173, 174 (Nina Gerber et al. eds., 2023).
[8] The Guidelines for Prevention and Regulation of Dark Patterns, 2023, Gazette of India, pt. lll sec. 4 (Nov. 30, 2023) § 2 (e).
[9] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1.
[10] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 1.
[11] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 1.
[12] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 2.

the cart at the time of final payment. This is nonconsensual and makes the user pay more than he intended to while purchasing the chosen product or service. However, basket sneaking does not include any additional payment included, provided a disclaimer regarding such additions is given prior to the checkout. In a recent case of *District of Columbia v. Grubhub*[13] veiled fees and unauthorized restaurant listings were claimed. The company was ordered to refund $2.7 million along with the payment of $800,000 as civil penalty.[14] Similarly, certain companies add products, services, or charity donations to the cart by shaming the consumer. Such actions leave a sense of responsibility or embarrassment in the consumer's mind and they perform the nudged action unwillingly or out of guilt. This is widely known as "Confirm Shaming."[15] Another related ruse is when the user is "forced"[16] to perform such an act he or she would not perform in the normal course of action. In this situation, the user is obligated to make an additional and "unrelated"[17] purchase to get access to his/her primary purchase. Sometimes there also exists a "Subscription Trap"[18] that makes the cancellation of any subscription nearly impossible. This includes vague cancellation instructions, hidden option or asking for payment details in the veil of providing a free subscription. This method plays with the normal consumer's intellect, which is averted by time-consuming or perplexing means of cancellation.

Designers frequently include features that are manipulative in nature to either focus on specific information or conceal important content. These "Interface interferences"[19] lead astray the user as in the case of Google LLC and Google Ireland Limited where the companies did not showcase an option to refute all the cookies in the "first layer of the cookie notice."[20] CNIL, the French regulatory body for data privacy imposed large fines on both the companies for violating the French Data Protection Act[21]. Further they were required to make necessary changes in their user interface. Sellers also promote a product and when the consumer is at the final stages of purchase, the availability is declined and similar options are presented as "alternative outcomes"[22] to trap the consumer into making a purchase with an undesired outcome. During the payment process,

---

[13] *District of Columbia v. Grubhub*, DECEPTIVE PATTERNS, https://www.deceptive.design/cases/district-of-columbia-v-grubhub.
[14] *Id.*
[15] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 3.
[16] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 3.
[17] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 3.
[18] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 5.
[19] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 6.
[20] *Deliberation of the Restricted Committee Concerning Google LLC and Google Ireland Limited*, DECEPTIVE PATTERNS, https://www.deceptive.design/cases/deliberation-of-the-restricted-committee-concerning-google-llc-and-google-ireland-limited.
[21] The Data Protection Act, No. 78-17, 1978 (France).
[22] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 7.

an element is added which charges the consumer in excess of the initially disclosed prices for further continuation.

"Disguised Advertisements,"[23] in violation of the Section 2(1)(28) of the Consumer Protection Act of 2019[24] are employed by sellers along with repeated requests to perform a certain act in the form of "Nagging"[25]. These deceptive tricks are cognitive exploitations of the users as they hinder the judgement by including biases or disrupting their original transactions. Companies and designers also use similar means to study consumer behavior and further add such dark patterns amongst their digital platforms to invite more users and rapidly increase their revenue. To prevent illicit transactions, various governments and regulatory bodies are elaborating their legal framework. It is imperative to encourage consent-based transactions and stop cheating the user with deceitful methods.

UNBOXING THE INTERPLAY WITH PRIVACY

Based on intellectual barriers like anchoring, framing, hyperbolic discounting and over choice[26], dark patterns are often privacy breachers. Anchoring occurs when the decision made is on the immediate or "first available" information, which can manipulate the choice according to only partial disclosure.[27] Whereas framing entails a black and white image being drawn in the minds of the consumer in the form of good or bad to influence the perception.[28] Frequently exploited by the tech industry, framing becomes a barrier to "free" and "specific" consent, especially under the Section 6 of the Digital Personal Data Protection Act, 2023.[29] In a similar violation, an over choice is given to the user which prevents him/her from giving specific consent which is "unambiguous"[30]. The user in such a scenario is presented with multitudes of options which deceitfully lead the consumer to make uninformed or partly informed choices, which further result in violations of the law on behalf of the company. Hyperbolic discounting is when the company presents excess value of a choice that the user would make in the present setting, while this excess dilutes the future consequences that might occur.[31] This can count as unfair trade practices as such actions are done with a hidden motive and are manipulative to the user.

---

[23] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 9.
[24] The Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019), § 2 (1) (28).
[25] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1 § 10.
[26] Ari E. Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'* 31 CURRENT OPINION IN PSYCHOL. 105, 107-108 (2020).
[27] *Id.* at 107.
[28] *Id.* at 107.
[29] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023), § 6.
[30] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023), § 6.
[31] Ari, *supra* note 25, at 107.

Awareness and preference to maintain privacy is often misdirected by "cognitive limitations"[32] which in turn can be regarded as a privacy breach. Digital platforms' designs make it tough for consumers to make balanced decisions. It is often seen that confirm shaming is used to seek consent for certain things which the user would not consent to as a rational and free choice. In the case between the Federal Trade Commission and LendingClub Corporation[33], the US District Court of California found the latter guilty of sneaking and including hidden costs in transactions. A settlement worth $18 million was reached along with an agreement to adhere new guidelines. The corporation violated the Gramm-Leach-Bliley Act[34] and which requires financial institutions to provide customers with "a clear and conspicuous"[35] privacy notice that precisely defines the financial institution's privacy "policies and practices."[36] The company also violated the FTC Act[37] which forbids "unfair or deceptive acts or practices in or affecting commerce."[38] The company was required to disclose all charges and fees upfront which it failed to do. This case is an appropriate example of privacy violations and dark patterns used by companies to increase their earnings and misleading their customers. In a Supreme Court of India case[39], WhatsApp was directed to make its users aware that accepting their privacy policy does not stand as a requirement to use the app.[40] Further no disruptions in regular use of the app would be there in case of no provision of consent. This highlights how disruptions in normal use of any digital platform can be employed by companies to nudge users to accept their terms and conditions which can be violative of privacy norms.

Used to maneuver the consumer according to their wishes, such dark patterns are illegal in many countries and they coincide with various laws. Often secret techniques used to seek consent by nudging or misleading a user is violative of privacy laws. Laws require companies to make full

---

[32] Ari, *supra* note 25, at 109.

[33] *LendingClub Agrees to Pay $18 Million to Settle FTC Charges,* FEDERAL TRADE COMMISSION (Jul. 14, 2021) https://www.ftc.gov/news-events/news/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges#:~:text=Online%20lender%20LendingClub%20Corporation%20agreed%20to%20pay%20%2418,and%20about%20whether%20their%20loan%20applications%20were%20approved.

[34] THE GRAMM-LEACH-BLILEY ACT § 503, 15 U.S.C. §§ 6801-6821 (1999).

[35] THE GRAMM-LEACH-BLILEY ACT § 503 (a), 15 U.S.C. §§ 6801-6821 (1999).

[36] THE GRAMM-LEACH-BLILEY ACT § 503 (b) (1), 15 U.S.C. §§ 6801-6821 (1999).

[37] Federal Trade Commission Act § 5, 15 U.S.C. §§ 41-58.

[38] Federal Trade Commission Act § 5 (a) (1), 15 U.S.C. §§ 41-58.

[39] Karmanya Singh Sareen & Anr. v. Union of India & Ors., (2019) 17 SCC 689.

[40] *WhatsApp v Right to Privacy: Supreme Court Directs WhatsApp to Publicize its May 2021 Undertaking; to Hear Petition in April 2023,* SCC ONLINE BLOG (Feb. 3, 2024), https://www.scconline.com/blog/post/2023/02/03/directed-whatsapp-to-widely-publicise-stand-that-its-users-in-india-do-not-have-to-accept-its-2021-privacy-policy-in-order-to-use-mobile-application/.

and complete disclosure of their data usage and privacy policies along with seeking free consent from users regarding their policies.

THE EUROPEAN UNION REGIME

The regulation of dark patterns, as approached by the European Union revolves around an amalgamation of multiple legislations including the General Data Protection Regulation (GDPR)[41], the Digital Services Act (DSA)[42], the Digital Markets Act (DMA)[43] and the Unfair Commercial Practices Directive (UCPD)[44] along with the proposed regulations like the AI Act and the Data Act [45]. However, the DSA and the DMA account for the dark-pattern specific laws as opposed to the other existing regulations [46]. Focussing on the regulation of online intermediaries, the DSA, as a legislative instrument cracks down on internet access providers, search engines and hosting services, thereby promoting transparency and innovation [47]. The key provision in the DSA Act which deals with dark patterns is Article 25 pertaining to the prohibition of usage of dark patterns [48]. Furthermore, Article 25(1) of the DSA only restrains platforms from "designing, organising or operating online interfaces[49] in a way that deceives or manipulates users or materially distorts or impairs their ability to make free and informed decisions" [50]. However, it is to be noted that this article only extends to "online platforms," thereby eliminating entities which employ dark patterns but do not classify as "online platforms" as defined under Article 2 of the DSA [51]. DSA tends to protect the decisional space of the users by implementing the concept of autonomous informed based choices[52]. Moreover, expansion around the concepts of autonomy, choice and decision has been done under Recital 67[53], while also providing further clarifications

[41] General Data Protection Regulation, 2016, 216/679, European Parliament, 2016 (European Union).
[42] Digital Services Act, 2022, 2022/2065, European Parliament, 2022 (European Union).
[43] Digital Markets Act,2022, 2022/1925, European Parliament, 2022 (European Union).
[44] Unfair Commercial Practices Directive, 2019, 2019/2161, European Parliament, 2019 (European Union).
[45] Dan Cooper et al., *EU Stance on Dark Patterns*, INSIDER PRIVACY, https://www.insideprivacy.com/eu-data-protection/the-eu-stance-on-dark-patterns/.
[46] Mark R. Leiser & Cristiana Santos, *Dark Patterns, Enforcement, and the emerging Digital Design Acquis -- Manipulation beneath the Interface*, SSRN ELIBRARY (2023) https:/Mark, %20Cristiana%20-%20Dark%20Patterns%20Article%20Outline.pdf.
[47] European Commission, *Digital Services Act Package (Digital Strategy)* https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.
[48] Digital Services Act, 2022, § 25 ,2022/2065, European Parliament, 2022 (European Union).
[49] Mark, *supra* note 49, at 20.
[50] Mark, *supra* note 49, at 20.
[51] Digital Services Act, 2022, § 2,2022/2065, European Parliament, 2022 (European Union).
[52] Digital Services Act, 2022, § 45 ,2022/2065, European Parliament, 2022 (European Union).
[53] Digital Services Act, 2022, § 67 ,2022/2065, European Parliament, 2022 (European Union).

and context around the terms "structure, design or functionalities"[54], primarily the characteristics of dark patterns. However, the most critical aspect of the Act is the fact that not all dark patterns can be regulated through this Act, including infinite scroll, auto play, and nagging practices to name a few[55], since dark patterns involving personal data are regulated through the GDPR those pertaining to B2C transactions, are scrutinised under the UCPD [56]. The Digital Markets Act (DMA)[57], further extends to scrutinise dark patterns employed by online platforms classifying as "gatekeepers"[58] like search engines, video sharing platforms, operating systems, cloud computing services and advertising platforms [59]. The language used is like the DETOUR Act[60] in the US, thereby defining dark patterns as "mechanisms subverting end users' autonomy, decision making or free choice" [61]. A similar definition has been adopted by the California Privacy Rights Act (CPRA)[62] and the Colorado Privacy Act (12)[63]. Recital 70[64] of the DMA further highlights the practices to be followed which revolve around the design, structure, function, and the manner of operation as employed by a neutral user interface, falling in line with Recital 69 which concedes the negative impact of dark patterns and the importance of transparency and trust[65]. The Data Act[66], which is yet to become a formalised legal instrument, builds up on GDPR and other existing regulations, thereby covering a wide range of dark patterns that cause hindrances to the users from exercising their data rights including rights pertaining to data access, data mobility and data elimination[67]. To provide an illustration, the Data Act will actively work towards curbing dark patterns which make it rather difficult or complex for the users to delete, block or force stop their accounts or even transfer the data to new devices by introducing multiple steps or procedures to complete such actions[68]. However, it is crucial to understand that a mechanism which does not classify as a dark pattern under the GDPR or has a strong legal standing to avoid scrutiny under the GDPR, might as well classify as one under the Data Act in case it violates regulations

[54] Mark, *supra* note 49, at 21.
[55] Mark, *supra* note 49, at 21.
[56] Mark, *supra* note 49, at 21.
[57] Digital Markets Act,2022, 2022/1925, European Parliament, 2022 (European Union).
[58] Digital Services Act, 2022, § 3 ,2022/2065, European Parliament, 2022 (European Union).
[59] Mark, *supra* note 49, at 23.
[60] DETOUR Act, 2019, 2019/1084, European Parliament, 2019 (European Union).
[61] DETOUR Act, 2019, § 3(a)(1) 2019/1084, European Parliament, 2019 (European Union).
[62] California Privacy Rights Act, 2020.
[63] Colorado Privacy Act, 2021, 2021/190, General Assembly, 2021 (State of Colorado).
[64] Mark, supra note 49, at 23
[65] Mark, supra note 49, at 23
[66] Data Act (Proposal), 2022, 2022/0047, European Parliament, 2022 (European Union).
[67] Data Act (Proposal), 2022, 2022/0047, European Parliament, 2022 (European Union).
[68] Data Act (Proposal), 2022, § 37,2022/0047, European Parliament, 2022 (European Union).

pertaining to storage, deletion, or transfer of data[69]. Recital 34 also highlights the disadvantages and penalties of the usage of dark patterns by third party entities thereby directing them to avoid taking coercive methods which might lead to hindrance in the digital interface used by the user[70].

INDIAN GUIDELINES AND THE WAY FORWARD

The Guidelines for Prevention and Regulation of Dark Patterns have been notified by the Central Consumer Protection Authority (CCPA) under the Section 18 of the Consumer Protection Act, 2019[71]. The Guidelines lay the foundation for the scrutiny of online entities employing dark patterns, thereby defining 'dark patterns' as "practices or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights".[72] As opposed to the global standard limiting the scope of a dark pattern to subversion of autonomy, the Indian Guidelines go the extra mile thereby expanding the scope to misleading advertisements, unfair trade practices or violation of consumer rights as well[73]. However, many contradictions can be observed within the Guidelines. For example, although the Guidelines sought to extend only to advertisers and sellers, the operative restrictions further mentioned in the Guidelines include all "persons and platforms"[74]. Similarly, although Annexure 1 contains an indicative list of illustrations pertaining to mechanisms amounting to dark patterns, Guideline 5 states that any entity employing those mechanisms specified in Annexure 1 will be considered engaging in coercive actions and dark patterns[75]. Furthermore, many redundancies and overlapping with other legislations can also be observed. For example, the guidelines pertaining to 'disguised advertisement' questions the value of regulations launched by the Advertising Standards Council of India, which proposed a much clearer jurisprudence and specific purposes revolving around advertisements[76]. At the same time, the Guidelines also tried to regulate and restrict malware attacks by classifying 'rogue malware' as a dark pattern, however, since this mechanism is not common in business practices as a weapon used for deceptive selling, it could have been better regulated under the Information Technology

---

[69] Mark, *supra* note 49, at 25.
[70] Mark, *supra* note 49, at 25.
[71] The Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019), § 2 (1) (28).
[72] The Guidelines for Prevention and Regulation of Dark Patterns at 4, § 2 (e).
[73] INDIA CORPORATE LAW, https://corporate.cyrilamarchandblogs.com/2023/12/dark-pattern-guidelines-illuminating-or-illusory/ (last visited on Jan 28, 2024).
[74] The Guidelines for Prevention and Regulation of Dark Patterns at 4, § 3.
[75] The Guidelines for Prevention and Regulation of Dark Patterns at 4, Annexure 1.
[76] The Guidelines for Prevention and Regulation of Dark Patterns at 4, § 2 (28).

Act, 2000[77].

Owing to the burden and the difficulties faced by the Consumer Courts in India, The Consumer Protection Forum should dedicate a separate department to deal with consumer complaints around dark patterns. The most critical part is the fact that since dark patterns constitute a wide amount of deceptive selling through online intermediaries and platforms, it is important to ensure speedy trial and due justice, thereby creating the necessity to dedicate a separate sub-forum or a separate department to deal with consumer affairs and issues due to employment of dark pattern mechanisms. At the same time, the Forum should also focus on training lawyers and staff of the Consumer Fora to ensure expertise and knowledge to deal with cases pertaining to dark patterns. Viewing in light, to the ever-growing digital world, and the lack of accurate information and statistical data, it is also important that the Indian laws keep updated to fit the growing regulatory demands around technological advances and innovations. Therefore, a small department under the CCPA should be constituted to observe the evolution of dark patterns thereby also focussing on inference of the data points generated, hereby contributing to the amendment of the Indian Guidelines to deal with the complex issues with the advent of advanced technologies like Artificial Intelligence (AI), Non-Fungible Tokens (NFT) and Internet of Things (IOT) and their intersection with dark patterns. This department should then work closely with the appointed ombudsman, hereby launching schemes like the Ombudsman Scheme for Non - Banking Financial Companies 2018[78] and the Banking Ombudsman Scheme 2006.[79] Furthermore, the Consumer Forum should also launch awareness campaigns and initiatives like public consultation papers to ensure enough public participation, and to promote the reporting of frauds due to Dark Patterns.

CONCLUSION

Through the arguments above, thereby using judicial authorities and existing discourse, it can be inferred that regulation of dark patterns is critical for the protection of privacy and to ensure ethical consumer behaviour. India, as a jurisdiction should focus on globalisation through laws and statutes adept to the current technological advances and innovation, hereby taking inspirations for various jurisdictions, like Singapore and the European Union. It is critical to understand the importance of strong cybersecurity frameworks, and its intersection with regulatory requirements, to build a strong foundation striking a balance between the economic perspective around profits and utilitarianism and the moral perspective around ethics and justice.

---

[77] Information Technology Act, No. 21 of 2000, INDIA CODE (2000) § 66.
[78] Ombudsman Scheme for Non - Banking Financial Companies 2018.
[79] Banking Ombudsman Scheme 2006.

Therefore, it is important to navigate the way forward using the aforementioned suggestions, and initiating discussions with the Consumer Forum.