Indiana Law Journal

Volume 100 | Issue 4 Article 3

6-2025

Dark Patterns as Disloyal Design

Johanna Gunawan
Maastricht University, johanna.gunawan@maastrichtuniversity.nl

Woodrow Hartzog
Boston University School of Law, whartzog@bu.edu

Neil Richards
Washington University in St Louis, nrichards@wustl.edu

David Choffnes
Northeastern University, choffnes@ccs.neu.edu

Christo Wilson
Northeastern University, c.wilson@northeastern.edu

Dark Patterns as Disloyal Design

JOHANNA GUNAWAN,[*] WOODROW HARTZOG,[**] NEIL RICHARDS,[***]
DAVID CHOFFNES[****] & CHRISTO WILSON[*****]

Lawmakers have started to regulate "dark patterns," understood to be design practices meant to influence technology users' decisions through manipulative or deceptive means. Most agree that dark patterns are undesirable, but open questions remain as to which design choices should be subjected to scrutiny, much less the best way to regulate them.

In this Article, we propose adapting the concept of dark patterns to better fit legal frameworks. Critics allege that the legal conceptualizations of dark patterns are overbroad, impractical, and counterproductive. We argue that law and policy conceptualizations of dark patterns suffer from three deficiencies: First, dark patterns lack a clear value anchor for cases to build upon. Second, legal definitions of dark patterns overfocus on individuals and atomistic choices, ignoring de minimis aggregate harms and the societal implications of manipulation at scale. Finally, the law has struggled to articulate workable legal thresholds for wrongful dark patterns. To better regulate the designs called dark patterns, lawmakers need a better conceptual framing that bridges the gap between design theory and the law's need for clarity, flexibility, and compatibility with existing frameworks.

We argue that wrongful self-dealing is at the heart of what most consider to be "dark" about certain design patterns. Taking advantage of design affordances to the detriment of a vulnerable party is disloyal. To that end, we propose disloyal design as a regulatory framing for dark patterns. In drawing from established frameworks that prohibit wrongful self-dealing, we hope to provide more clarity and consistency for regulators, industry, and users. Disloyal design will fit better into legal frameworks and better rally public support for ensuring that the most popular tools in society are built to prioritize human values.

---

* Assistant Professor of Computer Science and Law, Faculty of Law, Maastricht University. We thank Kirsten Martin, Meg Leta-Jones, Ryan Calo, Scott Jordan, Sue Glueck, Alexis Shore, Sylvia Lu, Geffrey Gary, Mihir Kshirsagar, Katrina Geddes, Julie Cohen, Rohan Grover, Alissa Cooper, and the participants of the 2024 Privacy Law Scholars' Conference for their helpful comments and feedback on a prior version of this draft.

** Professor of Law, Boston University School of Law.

*** Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis.

**** Professor, Khoury College of Computer Sciences and Executive Director, Cybersecurity and Privacy Institute, Northeastern University.

***** Professor, Khoury College of Computer Sciences, Northeastern University.

INTRODUCTION

Lawmakers have started to regulate "dark patterns," understood to be design practices that influence technology users' decisions through manipulative or deceptive means.[1] The concept of calling some design features "dark patterns" has been helpful for people seeking to articulate, categorize, and understand why and how certain design choices in digital systems are problematic to the humans using digital technologies.

But the project of identifying and regulating dark patterns has had only mixed results. Most agree that dark patterns are undesirable, but there is less agreement about what constitutes a "dark pattern," why they are problematic, which design choices should be subject to scrutiny, and how they should be regulated. The concept of dark patterns has also proven to be of limited utility in legal or prescriptive contexts. Despite the rapid adoption of the dark patterns moniker and careful attempts at defining it, critics allege that the term as deployed in laws is overbroad,

1. The California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), define dark patterns as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation." CAL. CIV. CODE § 1798.140(l) (West 2022). Other explicit definitions are provided by the U.S. Federal Trade Commission in a staff report, as well as the E.U. Digital Services Act in Recital 67. FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 2 (2022); Commission Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 18.

impractical, and counterproductive. What some see as a harmful design, others see as "omnipresent" design practices inextricably woven into the fabric of the Internet. In the eyes of these critics, it is impossible to prohibit "dark patterns" without prohibiting the design of every user interface online. Courts unfamiliar with the term "dark patterns" have similarly struggled to ground their analysis of this new concept within established legal concepts. And despite great efforts, scholars studying dark patterns have also acknowledged the difficulty in assessing their harms.

In this Article, we propose adapting the concept of dark patterns to better fit our existing and well-established legal frameworks. We argue that making this shift is necessary because current legal conceptualizations of dark patterns suffer from three deficiencies. First, the "dark patterns" concept lacks consensus or centralized articulation in the context of legal doctrine as to what makes them problematic.[2] Current definitions tend to bounce between trying to prevent harm and protect autonomy without a broader vision for human values, or "value anchor," reflected in design. Second, current legal definitions of dark patterns focus too much on individual consumers making individual choices, ignoring vast aggregations of harms that might individually be *de minimis*—as well as the societal implications of manipulation at scale. Third, the law has struggled to articulate practically useful legal thresholds for wrongful dark patterns. To better regulate the problematic designs called "dark patterns," lawmakers need a better conceptual framing that bridges the gap between design theory and the law's need for clarity, flexibility, and compatibility with existing frameworks.

To remedy these three problems, we argue that disloyal self-dealing is at the heart of what is considered to be "dark" about certain design choices. Put simply, it is disloyal when designers take advantage of the power design gives them to influence for their own benefit vulnerable parties to the detriment of those vulnerable parties. To that end, we propose *disloyal design* as a reframing of dark patterns that is more compatible with pluralistic, established, and effective regulatory tools. That is, we

---

2. There are a multitude of potential approaches, some of which are more legally operable than others, and some definitions better suited to certain legal mechanisms than others. For example, Jarovsky perceives dark patterns (at least within the data protection context) as necessitating both "manipulati[on] and malic[e]," while Leiser and Yang align dark patterns (within a commercial practices context) to concepts of information asymmetry and the suppression of free choice. Luiza Jarovsky, Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness 6 (2022) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=4048582 [https://perma.cc/9J8C-P2SX]; Mark Leiser & Wen-Ting Yang, *Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice Under the Unfair Commercial Practices Directive*, 34 LOY. CONSUMER L. REV. 484, 484 (2022). More recent legal literature by Santos, Morozovaite, and DeConca builds a harm taxonomy towards better understanding how harms are addressed within EU approaches, also noting the diversity in perspectives and prior taxonomies of harm. *See* Cristiana Santos, Viktorija Morozovaite & Silvia De Conca, *No Harm No Foul: How Harms Caused by Dark Patterns Are Conceptualised and Tackled Under EU Data Protection*, *Consumer and Competition Laws*, INFO. & COMMC'NS TECH. L.J. (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4877439 [https://perma.cc/45NM-8MZK]. This Article explores the multitude of conceptual approaches further in the text.

consider disloyal design (and conversely, design loyalty) to be a unifier for dark patterns concepts.

In drawing from established frameworks that prohibit wrongful self-dealing, we hope to provide more clarity and consistency for regulators, industry, and users. We do not present disloyal design as a conceptual replacement to dark patterns, but rather a complementary and centralizing approach for improving the legal field's responses to such designs. In short, the "darkness" of dark patterns comes from a company's disloyalty to vulnerable people by designing interfaces to their detriment. We present this work as a provocation for encouraging pluralistic, relational perspectives for design regulation.

Our argument proceeds in three parts. Part I sets the stage by offering a conceptual history of "dark patterns," motivating the search for an alternative name for such phenomena and exploring the various alternative framings for dark patterns. In Part II, this Article explains how existing regulatory approaches are insufficient for dark patterns, including (1) their lack of a clear normative commitment (which we call "an unclear value anchor"); (2) the limits of an atomistic focus on individual choice; and (3) the lack of any consensus on how to measure the existence or problematic nature of a "dark pattern."

Part III explains the advantages of framing dark patterns in terms of design disloyalty. We demonstrate how focusing on loyalty and trustworthiness unites the strengths of present dark patterns regulatory approaches and centralizes them. By embracing disloyal design as the legal conceptualization of dark patterns, lawmakers will be able to more effectively implement human values in regulatory frameworks to address not just privacy and autonomy questions, but broader questions involving cybersecurity, health, energy, and environmental concerns, as well as the impacts of emerging technologies on marginalized and vulnerable communities. Framing dark patterns as disloyal design thus fits better into existing legal frameworks and is more likely to rally public support for ensuring that the most popular tools in society are built to prioritize human values.

I. DARK PATTERNS AS CONCEPT

A. A Conceptual History of Dark Patterns

Dark patterns frequently overlap, but are not synonymous, with manipulative advertising practices. However, the growth of the attention economy, in which user engagement and data are the primary resources fought over by technology organizations, has created powerful incentives for these organizations to deploy dark pattern designs in everyday user interfaces.[3] In *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet,* Tim Hwang illustrates how the economic shift from traditional journalism profit models to a reliance on third-party advertising and sensationalism have subjected the modern netizen to experiences that desperately depend on monopolizing user attention to survive.[4]

---

3. *See, e.g.*, Neil Richards & Woodrow Hartzog, *Against Engagement*, 104 B.U. L. REV. 1151 (2024).

4. *See generally* TIM HWANG, SUBPRIME ATTENTION CRISIS: ADVERTISING AND THE TIME

This bodes poorly for the design of digital services, which have consistently been exposed for overcollection of behavioral data and shady engagement practices in recent years.[5] The nature of online experiences is fundamentally different from the historical patterns of media consumption and technological interaction that came before it.[6] These data-intensive online experiences provide the corporations that deliver them immense power over users' daily lives, wallets, and information.[7] Richards and Hartzog articulate this behavior as corporate data opportunism when applied to the privacy and data protections context.[8] Power has shifted from the individual user to middleman companies or to the very large online platforms (referred to as "VLOPs" in the European regulatory regime), simply by virtue of how much control the designing party has over the end product.[9] This has tradeoffs; we give up individual labor and control for scale and efficiency, but this also makes it incredibly easy to deploy and distribute consumer-disadvantageous designs at scale.

Consider briefly the late 1990s and early aughts, in which the online experience was generally decentralized. Aesthetics were varied and, in many cases, dutifully (or perhaps haphazardly but affectionately) maintained by individuals and groups left to their own design devices.[10] It was a personal, independent choice to stuff a webpage full of MIDI file music-box tunes or glittery mouse icon animations. Or one could choose to publish long-form blog content to the barest of HTML pages: white background, default Times New Roman, and left-justified pages on pages of diary entries. This was the still-scaling design landscape for digital experiences, often driven by amateur technology enthusiasts—a stark contrast to the slick corporate Internet of the mid-2020s.

Today, anybody with a credit card and a few free hours can deploy websites and experiences with corporate-level polish. Vendors like SquareSpace and Wix eliminate the need for ordinary technology users to surmount a steep learning curve

---

BOMB AT THE HEART OF THE INTERNET (2020).

5. Richards & Hartzog, *supra* note 3.

6. Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 996 (2022) (describing the key traits of modern information relationships as (1) ongoing, (2) high frequency, (3) occurring within an interactive environment, (4) operating within an environment completely constructed for the individual, and (5) operating within an environment that is responsive to the individual by the dominant party).

7. *See generally* JULIE E. COHEN, BETWEEN TRUTH AND POWER (2019); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

8. Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law,* 99 WASH. U. L. REV. 961, 969 (2021).

9. The E.U. Digital Service Act defines VLOPs as "online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to paragraph 4 [of the DSA]." Regulation 2022/2065, *supra* note 1, at 63 (Article 33).

10. *See, e.g.*, *Web Design in the 90s*, WEB DESIGN MUSEUM, https://www.webdesignmuseum.org/exhibitions/web-design-in-the-90s [https://perma.cc/D3C3-EUBP]; Nadya Primak, *Why I Miss the Early Internet*, MEDIUM (June 11, 2019), https://code.likeagirl.io/why-i-miss-the-nineties-internet-part-1-multimedia-minds-eb60beebde84 [https://perma.cc/K5B2-JKGD].

for technical skills, while enterprise and business-to-business firms help each other deploy limitless configurations of content, buttons, and layouts at incredible scale.[11] Design power has shifted as a result, and in some ways, it has done so in both directions. Design software companies empower regular users by making the process of constructing an online experience incredibly simple and efficient, but despite vast libraries of templates and themes or powerful customization engines, this empowerment simultaneously centralizes control over resultant designs at the hands of the design company.

This power shift plays out beyond "traditional" web interfaces, with new stakeholders involved in the control of designs across the digital space. Mobile apps are an increasing necessity given the ubiquity of smartphones. Though many mobile phone vendors exist, the vast majority of users download their apps from Apple's "App Store" or the "Google Play" platform. These centralized application stores enforce requirements that constrain app design.[12]

Independent app developers and user experience (UX) professionals are of course still invited to flex their artistry and talent, but there are often rules to follow no matter if one designs their own app or works for a software company deploying a platform.[13] Dark patterns are a design vehicle for exercising such power, generally thought of in terms of getting a person to adjust their behavior towards decisions and outcomes that are beneficial to the dark pattern deployer.[14]

Before Harry Brignull coined the term, dark patterns and the phenomena underlying their designs were discussed under related terms, particularly "nudges," "influence," and "persuasion" as more positive concepts of directing user behavior and "manipulation" and "coercion" for those less desirable.[15] Under the centralized

---

11. *See* Swati Bucha, *Squarespace Versus Wix: Which Website Builder is Better for Small Businesses?*, NEO (Sept. 24, 2024), https://www.neo.space/blog/wix-versus-squarespace [https://perma.cc/RL9Y-B84F].

12. Android and Apple's developers' platforms provide detailed mobile development guidance for engineers wishing to deploy a mobile app through the Google Play Store or Apple App Store respectively. *See, e.g.*, *Developers*, ANDROID, developer.android.com [https://perma.cc/K5FX-2LNE]; *Developer*, APPLE, developer.apple.com [https://perma.cc/UG3M-VAWV].

13. *See Developers*, *supra* note 12; *Developer*, *supra* note 12. In the case of Google and Apple, both manufacturers commonly build their own developer tools to distribute to those seeking to publish apps on their platforms. These tools can directly constrain the resultant mobile app design both in the front-end and back-end.

14. Definitions of dark patterns from scholarship and enforcement agencies or regulators tend to centralize around outcomes that are against users' intentions. Gray et. al., in particular, consider when "user value is supplanted in favor of shareholder value." Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, *in* CHI '18: PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1, 1 (2018), https://doi.org/10.1145/3173574.3174108 [https://perma.cc/T8UM-5TUC]; *see* Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/ [https://perma.cc/UF6M-L4WC]; *Deceptive Patterns*, DECEPTIVE DESIGN, https://www.deceptive.design/ [https://perma.cc/3MWG-D7RT].

15. The following citation provides a handy acronym for remembering some of the various "persuasive design/technologies" terms. Parisa Eslambolchilar, Max Wilson, Ian

moniker, dark patterns scholarship has proliferated in the years following 2010, with particularly sharp increases in annual scientific publications in the latter half of the 2010s and onward.[16] As a field of study, dark patterns attract, involve, and implicate theory and scholarship from computer scientists (including privacy/security, human-computer interaction, and other subfields), behavioral psychology, sociology, media studies, law and policy, and of course business and marketing research.[17]

This explosion of scholarship spans many lines of inquiry, with more technical studies exploring how to quantify or measure dark pattern presence and impact (with varying success in automated methods), while user studies and experiments investigate how people feel about dark patterns writ large or in specific contexts.[18]

Oakley & Anind Dey, *PINC: Persuasion, Influence, Nudge & Coercion Through Mobile Devices*, *in* CHI '11 EXTENDED ABSTRACTS ON HUMAN FACTORS IN COMPUTING SYSTEMS 13, 14–15 (2011), https://dl.acm.org/doi/10.1145/1979742.1979586 [https://perma.cc/D8VB-U9K7]. For an influential exploration of "malicious interfaces," see Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, *in* WWW '10: PROCEEDINGS OF THE 19TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB, 271, 272–73 (2010), https://doi.org/10.1145/1772690.1772719 [https://perma.cc/GH4Y-ALK7].

16. *See* Colin M. Gray, Lorena Sánchez Chamorro, Ike Obi & Ja-Nae Duane, *Mapping the Landscape of Dark Patterns Scholarship: A Systematic Literature Review*, *in* DIS '23 COMPANION: COMPANION PUBLICATION OF THE 2023 ACM DESIGNING INTERACTIVE SYSTEMS CONFERENCE 188, 188 (2023), https://dl.acm.org/doi/10.1145/3563703.3596635 [https://perma.cc/8TMS-2DQ4].

17. Broadly speaking, much of the foundational human-computer interaction (HCI) work (particularly those building taxonomies or exploring concepts of manipulation and beyond) nod to the conceptual history of dark patterns from older concepts of manipulation, deception, and coercion—all of which implicate how the human mind operates. *See, e.g.*, Gray et al., *supra* note 14; Lorena Sánchez Chamorro, Carine Lallemand & Colin M. Gray, *"My Mother Told Me These Things Are Always Fake" - Understanding Teenagers' Experiences with Manipulative Designs*, *in* DIS '24: PROCEEDINGS OF THE 2024 ACM DESIGNING INTERACTIVE SYSTEMS CONFERENCE 1469 (2024) [hereinafter Chamorro et al., *"My Mother Told Me These Things Are Always Fake"*], https://dl.acm.org/doi/10.1145/3643834.3660704 [https://perma.cc/7BUD-C3US]. However, with dark patterns essentially constituting a critical perspective of the design of consumer technologies, the term is less commonly implicated in business. Reem Rafiq Al-Tabakhi, Mohammad Hamdi Al Khasawneh & Ala' Omar Dandis, *Investigating Dark Patterns on Social Media: Implications for User Engagement and Impulse Buying Behavior*, 23 J. INTERNET COM. 469 (2024); Kawon (Kathy) Kim, Woo Gon Kim & Minwoo Lee, *Impact of Dark Patterns on Consumers' Perceived Fairness and Attitude: Moderating Effects of Types of Dark Patterns, Social Proof, and Moral Identity*, 98 TOURISM MGMT. 1, 4 (2023); Woo Gon Kim et al., *Dark Patterns Used by Online Travel Agency Websites*, 88 ANNALS OF TOURISM RSCH. 1, 4 (2021).

18. Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021); Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig & Gabriele Lenzini, *"I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" - Dark Patterns from the End-User Perspective*, *in* DIS '21: PROCEEDINGS OF THE 2021 ACM DESIGNING INTERACTIVE SYSTEMS CONFERENCE 763 (2021), https://dl.acm.org/doi/10.1145/3461778.3462086 [https://perma.cc/8VB7-ARXC]; Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula & Liyang Qu, *End User Accounts of Dark Patterns as Felt Manipulation*, PROC. ACM ON HUM.-COMPUT. INTERACTION, Oct. 2021, at 372:1; Ida Borberg, René Hougaard, Willard Rafnsson & Oksana Kulyk, *"So I Sold My Soul":*

Taxonomies have both iterated upon the Brignull collection and been created anew to serve the conceptual needs of different fields, roughly including legal scholarship,[19] computer science scholarship,[20] and regulatory practice.[21]

As this scholarship has proliferated, so have descriptions of dark patterns across scholarship[22] and institutional guidance.[23] To avoid oversaturation and confusion among dark pattern names, types, and categories, Gray et al. settled extant taxonomies from both academia and regulatory guidance into a unified ontology with which to reason through the different structures of dark patterns.[24] The ontology

---

Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions, USABLE SEC. & PRIV. SYMP., Mar. 2022, at 1; Chamorro et al., *"My Mother Told Me These Things Are Always Fake"*, *supra* note 17; Lorena Sánchez Chamorro, Romain Toebosch & Carine Lallemand, *Manipulative Design and Older Adults: Co-Creating Magic Machines to Understand Experiences of Online Manipulation*, *in* DIS '21: PROCEEDINGS OF THE 2024 ACM DESIGNING INTERACTIVE SYSTEMS CONFERENCE 668 (2024) [hereinafter Chamorro et al., *Manipulative Design and Older Adults*], https://dl.acm.org/doi/10.1145/3643834.3661513 [https://perma.cc/54JU-QLF5]; Gray et al., *supra* note 16.

19. Luguri & Strahilevitz, *supra* note 18, at 102; Leiser & Yang, *supra* note 2, at 487.

20. Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova & Thomas Mildner, *An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building*, *in* CHI '24: PROCEEDINGS OF THE CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2024), https://dl.acm.org/doi/10.1145/3613904.3642436 [https://perma.cc/C5TP-USH9]; Colin M. Gray et al., *supra* note 14, at 3; Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 4 PROC. ON PRIV. ENHANCING TECHS. 237, 238–39 (2016). The taxonomies listed herein present only a short list following the Brignull taxonomy. The 2024 Gray ontology provides a robust mapping across multiple known taxonomies (including Conti and Sobiesk, Luguri and Strahilevitz, Brignull, and regulatory bodies). We list the two Gray taxonomies for brevity but do note that pre-Brignull taxonomies of deceptive practices are often incorporated into the literature.

21. FED. TRADE COMM'N, *supra* note 1; OECD, DARK COMMERCIAL PATTERNS (Oct. 2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf [https://perma.cc/FN59-U75T]; COMPETITION & MKTS. AUTH., ONLINE CHOICE ARCHITECTURE: HOW DIGITAL DESIGN CAN HARM COMPETITION AND CONSUMERS (2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf [https://perma.cc/99NJ-K2Z9].

22. Gray et al., *supra* note 20; Bösch et al., *supra* note 20; Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan R. Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, PROC. ACM ON HUM.-COMPUT. INTERACTION., Nov. 2019, at 1; Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba & Alberto Bacchelli, *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, *in* CHI '20: PROCEEDINGS OF THE 2020 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1 (2020).

23. FED. TRADE COMM'N, *supra* note 1; COMPETITION & MKTS. AUTH., EVIDENCE REVIEW OF ONLINE CHOICE ARCHITECTURE AND CONSUMER AND COMPETITION HARM (Apr. 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069423/OCA_Evidence_Review_Paper_14.4.22.pdf [https://perma.cc/W3YR-4T7J]; COMPETITION & MKTS. AUTH., *supra* note 21; OECD, *supra* note 21.

24. Gray et al., *supra* note 20.

centralizes dark patterns conceptual knowledge as of 2024, stratifying dark patterns into high, meso, and low levels that describe the underlying design strategies at varying levels of domain or context specificity, abstraction, and mechanism. According to the ontology, high-level patterns refer to general design strategies used across technological modalities and are context and domain agnostic; that is, whether a high-level pattern appears in a mobile app or Internet of Things devices doesn't change the pattern's definition. These patterns include "Obstruction," "Sneaking," "Interface Interference," "Forced Action," and "Social Engineering."[25] Meso-level patterns are still context-agnostic, but rather describe a specific angle of attack— that is, *how* the high-level strategy is executed. Meso-level patterns also describe how user expectations from a design are subverted. Finally, low-level patterns are those specifically situated in a given context or domain and articulate a specific "means of execution."[26]

The low- and meso-level patterns map to the high-level strategies. To illustrate, the high-level strategic dark pattern of Obstruction contains the meso-level "Roach Motel" dark pattern beneath it. Roach Motels in the Gray ontology are defined as patterns that "subvert[] the user's expectation that an action will be as easy to reverse as it is to make, instead creating a situation that is easy to get into, but difficult to get out of."[27] Two low-level patterns are mapped to the Roach Motel meso-level dark pattern: "Immortal Accounts" and "Dead Ends." Immortal Accounts are designs in which is impossible or considerably difficult to delete a created user account, while Dead Ends prevent information discovery by "ending" the path to information through dead links, redirects, or otherwise preventing the display or access of relevant information. The ontology then provides definitions for each low-level pattern that implicates the higher-level patterns related to it, thus an Immortal Account is described as "creating" a Roach Motel by "using" Obstruction: the low-level pattern operates in a meso-level manner corresponding to a high-level strategy.

This work provides ample opportunity for cross-disciplinary collaboration and evidence in support of rigorous dark patterns regulation, with many scholars co-authoring in interdisciplinary teams or across disciplinary publishing venues, or discussing implications for policymakers and the legal field in their publications.[28]

---

25. *Id.*; *see also* Colin M. Gray, Cristiana Santos, Nataliia Bielova & Thomas Mildner, *An Ontology of Dark Patterns*, DARK PATTERNS ONTOLOGY (2024), https://ontology.darkpatternsresearchandimpact.com/wp-content/uploads/2024/05/2024_Grayetal_CHI_OntologyReferenceSheet.pdf [https://perma.cc/8APN-DNNR] (providing a handy reference sheet of all pattern types at all levels).

26. Gray et al., *supra* note 25.

27. Gray et al., *supra* note 20, at 10.

28. Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox*,*'* 31 CURRENT OP. PSYCH. 105 (2020); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 156 (2018); Sorin Berbece, *'Let There Be Light!' Dark Patterns Under the Lens of the EU Legal Framework* (2019) (Master's thesis, KU Leuven), https://papers.ssrn.com/abstract=3472316 [https://perma.cc/S6DL-P4P8]; Inge Graef, *The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?*, *in* Ramsi A. Woodcock, TOWARD AN INFRAMARGINAL REVOLUTION: MARKETS AS WEALTH DISTRIBUTORS (2023); Alison Hung, Note, *Keeping Consumers in the Dark: Addressing "Nagging" Concerns and Injury*, 121 COLUM. L. REV.

B. Dark Patterns in Regulation

Dark patterns are currently governed by a smattering of different regulations, drawn from distinct yet overlapping areas of law and non-binding guidelines. For example, privacy and data protection regulations prohibit the use of dark patterns in consent or opt-in regimes.[29] Meanwhile, consumer protection agencies relate dark patterns to unlawful business practices subject to enforcement under their mandates. Few laws describe dark patterns by name, but many agencies make use of other mechanisms like informal investigations[30] or guideline creation[31] to assert which practices they would like to see from technology corporations.

2483 (2021); Monica Kowalczyk, Johanna T. Gunawan, David Choffnes, Daniel J. Dubois, Woodrow Hartzog & Christo Wilson, *Understanding Dark Patterns in Home IoT Devices*, *in* CHI '23: PROCEEDINGS OF THE 2023 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2023), https://doi.org/10.1145/3544548.3581432 [https://perma.cc/ENS8-H3BZ]; Johanna Gunawan, Cristiana Santos & Irene Kamara, *Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions*, *in* CSLAW '22: PROCEEDINGS OF THE 2022 SYMPOSIUM ON COMPUTER SCIENCE AND LAW 181 (2022), https://dl.acm.org/doi/10.1145/3511265.3550448 [https://perma.cc/98AV-CJ8N]; Gray et al., *supra* note 16; Cristiana Santos & Arianna Rossi, *The Emergence of Dark Patterns as a Legal Concept in Case Law*, INTERNET POL'Y REV. (July 31, 2023), https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept [https://perma.cc/4NQ4-TDZN]; Célestin Matte, Nataliia Bielova & Cristiana Santos, *Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*, 2020 IEEE SYMP. ON SEC. AND PRIV. 791; Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth & Damian Clifford, *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective*, *in* CHI '21: PROCEEDINGS OF THE 2021 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2021), https://dl.acm.org/doi/10.1145/3411764.3445779 [https://perma.cc/B989-MZMS]; Santos et al., *supra* note 2; Chamorro et al., *Manipulative Design and Older Adults*, *supra* note 18 (discussing room for countermeasures with policy implications); Brennan Schaffner, Neha A. Lingareddy & Marshini Chetty, *Understanding Account Deletion and Relevant Dark Patterns on Social Media*, *in* PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION 21–22 (2022), https://dl-acm-org.proxyiub.uits.iu.edu/doi/10.1145/3555142.

29. *See e.g.*, CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020, CAL. CIV. CODE §§ 1798.100–1798.199 (2020).

30. INT'L CONSUMER PROT. & ENF'T NETWORK, ICPEN DARK PATTERNS IN SUBSCRIPTION SERVICES SWEEP PUBLIC REPORT (2024), https://icpen.org/sites/default/files/2024-07/Public%20Report%20ICPEN%20Dark%20Patterns%20Sweep.pdf [https://perma.cc/WDB5-FJNE]; Julie Beaumont, *2024 GPEN Sweep on Deceptive Design Patterns*, GLOB. PRIV. ENF'T NETWORK (July 9, 2024, 3:00 AM), https://www.privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns [https://perma.cc/MLH5-E28F].

31. FRANCISCO LUPIÁÑEZ-VILLANUEVA ET AL., DIRECTORATE-GENERAL FOR JUST. & CONSUMERS, BEHAVIOURAL STUDY ON UNFAIR COMMERCIAL PRACTICES IN THE DIGITAL ENVIRONMENT: DARK PATTERNS AND MANIPULATIVE PERSONALISATION (2022), FED. TRADE COMM'N, *supra* note 1; Press Release, Ministry of Consumer Affs., Food & Public Distrib., Central Consumer Protection Authority Issues 'Guidelines for Prevention and Regulation of Dark Patterns, 2023' for Prevention and Regulation of Dark Patterns Listing 13 Specified Dark

Of the explicit mentions of dark patterns, Recital 67 of the European Union's Digital Service Act (DSA) provides a robust legal definition.[32] It describes dark patterns as:

> practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them.[33]

The DSA then prohibits "deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof."[34]

Recital 67 provides a detailed and explicit list of examples of prohibited behaviors, which map to the Brignull taxonomy's "nagging," "hard to cancel," "preselection," and "fake scarcity patterns,"[35] as well as Bösch et. al.'s "bad defaults."[36] How well the DSA combats dark patterns in practice remains to be seen (this Article was drafted within four months of the DSA going into effect), but the depth and detail of the DSA's definition and described prohibitions have great potential for widespread impact, at least for the examples provided.

Prior to the DSA, explicit dark patterns regulatory efforts were primarily seen within the California Consumer Privacy Act (CCPA), which prescribes required practices for equivalently presenting opt-in and opt-out designs through amendment to the CCPA that followed, called the California Privacy Rights Act (CPRA).[37] Other amendments through the CPRA further note that consent obtained through dark patterns is considered invalid.[38] The CPRA defines dark patterns as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."[39]

The Colorado Privacy Act (CPA) follows suit, taking the same definition as the CPRA, and additionally requiring that consent for the collection of sensitive data (including children's data) be free of dark patterns.[40]

Patterns (Dec. 8, 2023, 3:55 PM), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1983994 [https://perma.cc/BZ6G-26QC]; EUR. DATA. PROT. BD., GUIDELINES 03/2022 ON DECEPTIVE DESIGN PATTERNS IN SOCIAL MEDIA PLATFORM INTERFACES: HOW TO RECOGNISE AND AVOID THEM (2023), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en [https://perma.cc/834Q-L2U3].

32. Regulation 2022/2065, *supra* note 1.

33. *Id.*

34. *Id.*

35. *Types of Deceptive Patterns*, DECEPTIVE PATTERNS, www.deceptive.design/types [https://perma.cc/S6FB-MH8V].

36. Bösch et al., *supra* note 20, at 248.

37. *See generally* CAL. CIV. CODE § 1798.135(b)(2)(A)–(B) (West 2023).

38. *Id.* § 1798.140(h).

39. *Id.* § 1798.140(l).

40. COLO. REV. STAT. § 6-1-1301 (2024); *see also* COLO. CODE REGS. § 904-3 (2024),

In the United States, dark patterns cases[41] are largely handled by the Federal Trade Commission (FTC) under its authority to prohibit unfair or deceptive trade practices, or by state attorneys general using their analogous authority under state "unfair and deceptive acts and practices" (UDAP) statutes.[42] Most cases to date have been primarily framed as deception claims. Within such cases, the FTC's orders against offending companies may also implicate violations of other relevant regulations, like the Restore Online Shoppers' Confidence Act (ROSCA),[43] Gramm-Leach-Bliley

---

Rule 7.09 ("Consent obtained through Dark Patterns does not constitute valid Consent . . . ."): According to Rule 7.09, the following principles should be considered when designing a user interface or a choice architecture used to obtain Consent:

> 1. Consent choice options should be presented to Consumers in a symmetrical way that does not impose unequal weight or focus on one available choice over another such that a Consumer's ability to consent is impaired or subverted. . . .
> 2. Consent choice options should avoid the use of emotionally manipulative language or visuals to unfairly, fraudulently, or deceptively coerce or steer Consumer choice or Consent. . . .
> 3. A Consumer's silence or failure to take an affirmative action should not be interpreted as acceptance or Consent. . . .
> 4. Consent choice options should not be presented with a preselected or default option. . . .
> 5. A Consumer should be able to select either Consent choice option within a similar number of steps. A Consumer's ability to exercise a more privacy-protective option shall not be unduly longer, more difficult, or time-consuming than the path to exercise a less privacy-protective option. . . .
> 6. A Consumer's expected interaction with a website, application, or product should not be unnecessarily interrupted or intruded upon to request Consent. . . .
> 7. Consent choice options should not include misleading statements, omissions, affirmative misstatements, or intentionally confusing language to obtain Consent. . . .
> 8. The vulnerabilities or unique characteristics of the target audience of a product, service, or website should be considered when deciding how to present Consent choice options. . . .
> 9. User interface design and Consent choice architecture should operate in a substantially similar manner when accessed through digital accessibility tools.

COLO. CODE REGS. § 904-3 (2024).

41. A community-maintained repository of dark patterns cases, including pending cases and decided cases worldwide, contains a non-exhaustive list compiled by legal dark patterns scholars and other members of the research and advocacy community. *Legal Cases*, DECEPTIVE PATTERNS, www.deceptive.design/cases [https://perma.cc/8DZU-6DCS].

42. *See* 15 U.S.C. § 45; Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) (providing an overview of state UDAP laws in this context).

43. *See, e.g.*, Complaint at 1, Fed. Trade Comm'n v. Amazon.com, Inc., No. 2:23-cv-00932 (W.D. Wash. June 21, 2023); Complaint at 1, Fed. Trade Comm'n v. Age of Learning,

Act (GLBA),[44] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM),[45] and state consumer protections laws.[46] More recently, the FTC has begun to explicitly mention dark patterns in case documents. One example is *In re Epic Games, Inc.,* in which the final Complaint document notes that Epic "employ[ed] myriad design tricks known as 'dark patterns.'"[47] At the state level, Attorneys General are filing suit against companies (like the District of Columbia AG) or are otherwise warning their constituencies about dark patterns and related anti-consumer practices.[48]

Other laws in practice regulate dark patterns even though they do not explicitly mention the term or adjacent terms like "deceptive designs." For example, the Consumer Financial Protection Bureau (CFPB) dissuades many kinds of dark patterns in effect through its authority to regulate abusive acts or practices. An abusive act or practice is one that obscures important features of a product or service or takes an unreasonable advantage of people's gaps in understanding, unequal bargaining power, and reliance.[49]

Across the Atlantic, European Union member states can make use of the European Data Protection Board (EPDB) and European Commission mandates in data protections, privacy, and consumer protections to combat dark patterns. Newer or proposed regulations like the Digital Markets Act (DMA)[50] or Artificial Intelligence

---

Inc., No. 2:20-cv-7996 (C.D. Cal. Sept. 1, 2020).

44. *See, e.g.*, Complaint at 2, Fed. Trade Comm'n v. LendingClub Corp., No. 3:18-cv-02454 (N.D. Cal. Apr. 25, 2018).

45. *See, e.g.*, Complaint at 2, Fed. Trade Comm'n v. Effen Ads, LLC, No. 2:19-cv-00945 (C.D. Utah Nov. 26, 2019).

46. *See, e.g.*, Complaint at 2, Fed. Trade Comm'n v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017).

47. Final Complaint and Order, *In re* Epic Games, Inc., FTC Docket No. C-4790 (Mar. 13, 2023); *see also* Amended Complaint, FTC v. Amazon.com, Inc., No. 2:23-cv-00932 (W.D. Wash. Sept. 20, 2023).

48. Press Release, Att'y Gen. for the D.C., AG Racine Announces Google Must Pay $9.5 Million for Using "Dark Patterns" and Deceptive Location Tracking Practices hat Invade Users' Privacy (Dec. 30, 2022), https://oag.dc.gov/release/ag-racine-announces-google-must-pay-95-million [https://perma.cc/V8F8-D7NY]; *Attorney General Raoul Urges the Federal Trade Commission to Address Deceptive "Dark Patterns" in Digital Advertising*, ILL. ATT'Y GEN. (Aug. 3, 2022), https://illinoisattorneygeneral.gov/dA/dc23f1da69/202208-03%20URGES%20THE%20FEDERAL%20TRADE%20COMMISSION%20TO%20ADDRESS%20DECEPTIVE%20DARK%20PATTERNS%20IN%20DIGITAL%20ADVERTISING.pdf [https://perma.cc/Y39W-P39W].

49. 12 U.S.C. § 5531(d) (2012) (defining an abusive act or practice as one that "(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of-- (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer"); *see also Policy Statement on Abusive Acts or Practices*, CONSUMER FIN. PROT. BUREAU (Apr. 03, 2023) https://www.consumerfinance.gov/compliance/supervisory-guidance/policy-statement-on-abusiveness/#footnote-source-13 [https://perma.cc/MGF8-CUSX].

50. Council Regulation (EU) 2022/1925 of the European Parliament and of the Council

Act (AI Act)[51] involve prohibitions of dark pattern behavior. Some countries pursue dark patterns more aggressively than others; the French Data Protection Authority (CNIL), for example, frequently targets dark patterns in both its formal enforcement and other investigatory mechanisms (e.g., sweeps).[52] The Italian Data Protection Authority (Garante)[53] conducted an EU first with an enforcement decision explicitly relating dark patterns to General Data Protection Regulation (GDPR) infringements.[54]

Beyond formal regulation, however, a battery of guidelines, white papers, and reports provide some guidance for the industry to follow as dark patterns enforcement evolves (authoring institutions include consumer councils,[55] competition and markets agencies,[56] and industry or trade organizations).[57] Though nonbinding, such reports offer local guidance specific to the citizens of a given state or companies who wish to conduct business in-state, and do not universally protect consumers on the globalized web. These reports often follow internal investigations that produce additional categories of dark patterns that can be used to identify and label undesirable designs.[58]

C. A Semantic Reckoning for Dark Patterns

Separate from concerns over patchwork dark patterns enforcement, within the research community there exists increasing discomfort with the "dark patterns"

---

of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1; *see also EU: Commission Publishes Final proposals for Digital Services Act and Digital Markets Act for Regulating Digital Platforms*, DATAGUIDANCE, (Dec. 15, 2020), https://www.dataguidance.com/news/eu-commission-publishes-final-proposals-digital [https://perma.cc/KBB6-LYC6].

51. *EU AI Act: First Regulation on Artificial Intelligence*, EUROPEAN PARLIAMENT, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence [https://perma.cc/T3N8-T8WP] (last updated Feb. 19, 2025).

52. *Sweeps*, EUROPEAN COMM'N, https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en [https://perma.cc/FBG2-PNUG].

53. Santos & Rossi, *supra* note 28.

54. *Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. - 23 febbraio 2023 [9870014]* [Prescriptive and Sanctioning Provision Against Ediscom S.p.A. - 23 February 2023 [9870014]], GARANTE PER LA PROTEZIONE DEI DATI PERSONALI [Guarantor for the Protection of Personal Data] (Feb. 23, 2023), https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9870014 [https://perma.cc/W466-JKLX].

55. NORWEGIAN CONSUMER COUNCIL, DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY (2018).

56. COMPETITION & MKTS. AUTH., *supra* note 21.

57. OECD, *supra* note 21.

58. OECD, *supra* note 21; COMPETITION & MKTS. AUTH., *supra* note 23.

moniker itself.[59] This motivates, from a normative standpoint, the need for a new name or framing.

Across technology disciplines, there exists a growing movement to equalize practitioner terminology. Such efforts often question the necessity, accuracy, and relevance of certain technical vocabulary. For example, the use of "master/slave" to describe architectural hierarchies and relationships between machines has been put out of vogue and given alternative options like "parent/child," "writer/reader," "leader/follower," or "active/standby" to more equitably label parties.[60] Similarly, cybersecurity professionals are urged to refrain from using "blacklists" to describe lists of adversarial IP addresses or parties that users should block access to architectures from (with the counter-term for approved items called "whitelists"), with "deny lists" (as in, "allow/deny") or "blocklists" as suggested options.[61]

One of the primary criticisms is over the "dark" modifier's potential for negative and racially problematic connotations.[62] "Darkness" captures the opacity or *hidden* nature of dark patterns' true design intentions, and in a similar manner the term "black box" has been retained in technology circles to describe opaque business practices, particularly for algorithmic decision-making or artificial intelligence mechanisms. However, "black box" as a descriptor is potentially neutral; not all non-transparent technology company practices are necessarily harmful and in some ways a manner of protecting intellectual property. Dark patterns, on the other hand, may benefit from a shift to alternative modifiers that offer greater diversity, inclusivity, and equity in an industry that is in many ways still dominated by Western, white male professionals. Even Harry Brignull, thought to be the originator of the 'dark patterns' moniker in 2010, responded to the community's increasing discomfort and updated the prior darkpatterns.org website URL and title to deceptive.design instead (which is current as of the submission of this Article in 2025).

Though the imagery of something hidden in the dark helps conceptualize the subversive nature of dark patterns, "dark" is additionally a vague term with many potential interpretations. Beyond the capacity for problematic connotations, "dark patterns" runs the risk of becoming overused—a risk that Angel and Calo warn

---

59. Much of this commentary comes from the UX community in passionate blog posts. *See, e.g.*, Amy Hupe, *Why It's Time to Update our Language About Bad Design Patterns*, AMY HUPE (July 1, 2022), https://amyhupe.co.uk/articles/changing-our-language-on-bad-patterns/ [https://perma.cc/9GZJ-3TAQ]; Todd Libby, *Enough with "Dark Patterns" Already!*, TODD LIBBY (Jan 1, 2023), https://toddl.dev/posts/enough-with-dark-patterns-already/ [https://perma.cc/3Z5U-C33C]. King and Stephan refer to concerns over the potentially racialized connotation of "dark" to describe negative traits in dark patterns. Jennifer King & Adriana Stephan, *Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from the California Privacy Rights Act*, 5 GEO L. TECH. REV. 250, 253 n.3 (2021). Other dark patterns scholars have also addressed this concern. *See, e.g.*, Caroline Sinders, *What's in a Name? Unpacking Dark Patterns Versus Deceptive Design*, MEDIUM (June 17, 2022), https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns-versus-deceptive-design-e96068627ec4 [https://perma.cc/V4JL-UYGB].

60. Elizabeth Landau, *Tech Confronts Its Use of the Labels 'Master' and 'Slave*,*'* WIRED (July 6, 2020, 7:00 AM), https://www.wired.com/story/tech-confronts-use-labels-master-slave/ [https://perma.cc/H7EG-E48F].

61. *Id.*

62. *See supra* note 58.

against for "privacy," lest the concept of privacy be "diffuse[ed] into a meaningless catch-all."[63] Then, for the law, "darkness" has minimal benefit as a descriptor as opposed to terms that have distinct legal meanings (e.g., "unfairness," "deception," lack of "care," and "trustworthiness").

In the wake of this semantic reckoning, viable alternatives are needed. Common substitutes like "deceptive design patterns" or "manipulative design patterns" are easy to interpret and fairly recognizable, but do not fully encompass the range of potential designs under one umbrella the way that "dark patterns" currently does. Some dark patterns may be fairly transparent or obvious, especially so if encountered by an informed, aware user—but awareness of a dark pattern does not negate the risk of negative or unwanted outcomes. "Deception" helps directly relate designs against Section 5 of the FTC Act on *deceptive trade practices*, but "deceptive designs" then excludes unfair but non-deceptive designs that still cause harm or operate against end users.[64] Antonym-based options like "bright" or "fair" patterns describe good behavior (in the way that "loyal design" would be opposite of "disloyal design"). These could be viable, positively-framed alternatives, but suffer from the same conceptual vagueness as the word "dark"—the true meaning of the analogy is wide open for interpretation.

In the search for a better term of phrase, we are left to consider what is desirable for digital designs. Some inspiration may come from enumerating the human values we seek (value-sensitive design),[65] or generally prescribing a need for ethical design. Conceptually, a new term (particularly for the legal field) should have the *breadth* that "dark patterns" currently seems to span, while perhaps tightening the *operational* concepts behind the phrase. Note that all of the following are desirable traits for consumer-facing digital designs. The following subsections illustrate the multitude of values implicated in dark patterns or deceptive designs, demonstrating the difficulty in articulating a centralized concept of dark patterns.

1. Designing for "Brightness" or "Lightness"

"Bright" patterns[66] provide the same breadth as "dark" patterns do, while evoking the same imagery of hidden ("dark"/"in-the-dark") versus illuminated ("bright")

---

63. María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507, 541 (2024).

64. *See* 15 U.S.C. § 45(a). "Unfair and deceptive designs" could be useful, but in the effort of centrally articulating what it is about dark patterns needs to be minimized, it is important to remember that the FTC has treated unfairness and deception as distinct concepts. *See* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785 (2015).

65. Batya Friedman, *Value-Sensitive Design*, 3 INTERACTIONS, Nov.-Dec. 1996, at 17; BATYA FRIEDMAN & DAVID G. HENDRY, VALUE SENSITIVE DESIGN: SHAPING TECHNOLOGY WITH MORAL IMAGINATION (2019).

66. Paul Graßl, Hannah Schraffenberger, Ferderik Zuiderveen Borgesius & Moniek Bujizen, *Dark and Bright Patterns in Cookie Consent Requests*, 3 J. DIGITAL SOC. RSCH. 1, 1 (2021); Hauke Sandhaus, *Bright Patterns*, BRIGHT PATTERNS, https://brightpatterns.org/ [https://perma.cc/Z27E-HP66]; Hauke Sandhaus, Promoting Bright Patterns 1 (Apr. 3, 2023)

design. To the legal field, however, the concepts or intention behind a "brightness" moniker are perhaps less useful and not grounded in extant legal definitions in the manner that transparency or fairness are (at least in various legal subfields). "Lightness" similarly evokes illuminative imagery, but carries similar risk for the racial connotations that are currently known to plague dark patterns. Such terms' strength lies in their evocative power, relative catchiness, and direct relation to "dark" patterns—this benefit should not be understated, even if both terms are not as immediately operable within the legal field as some of the following concepts.

2. Designing for Fairness

"Fair" patterns provide a similarly broad-yet-illustrative term as do "dark" patterns. However, "fairness" is laden with several other meanings depending on the area of technology or law one looks at; in machine learning and algorithmic auditing,[67] fairness aims to correct bias and discrimination, whereas in competition fairness ensures equal opportunity.[68] Even after selecting a definition of fairness, the question of "fairness to whom" remains. Efforts to reduce dark patterns thus far have focused on fairness between platforms or services and end users, but other definitions of fairness such as those in competition law or machine learning seek fairness across multiple groups, thus "leveling the playing field," reducing bias, or equally distributing resources. Thus, the parties involve relationships between multiple platforms or groups of users, rather than exclusively the relationship between a platform and an individual user.

With regards to fair competition (and fair market dynamics between platforms), Gregory Day and Abbey Stemler argue that digital manipulation and dark patterns should be considered as anti-competitive.[69] This departs from a traditional antitrust perspective of influencing a consumer as a form of competitive behavior. In particular, Day and Stemler discuss the difference between persuasion (considered as pro-competitive influence over a consumer) and coercion (considered as anti-competitive).[70] Day and Stemler orient this issue along a need for decisional privacy and freedom from interference with consumers' rational thought, relating as well to the autonomy and choice perspectives common in dark patterns scholarship.[71]

Setting aside field-specific definitions of fairness and focusing on consumer protections or commercial practices exclusively, both the European Union and the

---

(unpublished manuscript) (on file with arXiv), https://arxiv.org/abs/2304.01157 [https://perma.cc/XFM7-ATZP].

67. Simon Caton & Christian Haas, *Fairness in Machine Learning: A Survey*, 56 ACM COMPUT. SURV. 1 (2024); Luca Oneto & Silvia Chiappa, *Fairness in Machine Learning*, *in* RECENT TRENDS IN LEARNING FROM DATA: TUTORIALS FROM THE INNS BIG DATA AND DEEP LEARNING CONFERENCE (INNSBDDL2019) 155 (Luca Oneto et al. eds., 2020); ALEXANDRA CHOULDECHOVA & AARON ROTH, THE FRONTIERS OF FAIRNESS IN MACHINE LEARNING (2018).

68. This, of course, is a non-exhaustive enumeration of fairness concepts in different tech/law subdisciplines.

69. Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?*, 72 ALA. L. REV. 1 (2020).

70. *Id.* at 27–34.

71. *Id.* at 29.

United States commonly rely on unfairness tests[72] to determine violations. However, such tests commonly require thresholds to be met and place a burden of proof for articulating resultant harms or risk of harm. This may present too high a standard by which to regulate *de minimis* issues arising from dark patterns, particularly when examining dark patterns at an individual scale. Scholars have identified a need for alleviating such burdens of proof,[73] in the hopes that future uses of enforcers' fairness mechanisms might be more effectively applied.

Mark Leiser and Wen-Ting Yang orient known dark patterns into their law-oriented taxonomy, which sorts certain patterns into two mechanisms of manipulation—information asymmetry and the repression of free choice—then apply this taxonomy to the provisions of the EU Unfair Commercial Practices Directive (UCPD).[74] The UCPD's scope pertains to unfair practices impacting the "economic behavior" of consumers,[75] thus protecting against transgressions such as those plaguing freemium or free-to-play models. As such, even as consumer fairness perspectives might present some of the strongest defenses against dark pattern behavior, there still exist jurisdictional limits depending on where this fairness is sought.[76] While fairness as a concept holds great promise for mitigating vulnerabilities in design, lawmakers would need to refine the concept a bit more, even in the E.U. where the concept is deployed more centrally in information rules.[77]

---

72. Marie Jull Sørensen, *The Unfairness Test: From Sleeping Beauty to Little Mermaid*, 32 EUR. REV. PRIV. L. 387 (2024); J. Howard Beales III, Director, Bureau of Consumer Protection, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003), https://www.ftc.gov/news-events/news/speeches/ftcs-use-unfairness-authority-its-rise-fall-resurrection [https://perma.cc/H37P-E362].

73. Hans-W. Micklitz, Natali Helberger, Betül Kas, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax & Michael Veale, *Towards Digital Fairness*, 13 J. EUROPEAN CONSUMER MKT. L. 24, 29 (2024), https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\EuCML\EuCML2024004.pdf [https://perma.cc/K37H-RZ2M]; Gunawan et al., *supra* note 28, at 186–87.

74. Leiser & Yang, *supra* note 2, at 509–10.

75. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), 2005 O.J. (L 149) 22, at 6 (art. 5(2–3)).

76. That is, the UCPD scope of unfairness, which includes misleading or aggressive behavior beneath it, still primarily pertains to commercial scope with material harms implications. *See id.* at 7 (art 5(4)). Jurisdictional limits are necessary and good—the UCPD should not be regulating outside of consumers' economic behaviors—but while such limitations are useful for operationalizing the law they are less useful for selecting a unifying and sufficiently broad term of art.

77. *See* Gianclaudio Malgieri, *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation*, *in* FAT* '20: PROCEEDINGS OF THE 2020 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 154 (2020) (noting that fairness within the GDPR has been interpreted as "loyalty" in some European countries).

3. Designing for Autonomy and Choice

Autonomy and choice framings of dark patterns, of which the EU DSA definition is one of, take an individualistic approach to dark patterns. Comparatively popular, these approaches rally against (intentional) manipulation[78] or otherwise undue influence over the user (and subsequently their decisions or actions within a digital service).[79]

While autonomy and choice are necessary to concepts of dark patterns, particularly insofar as they describe the manner in which cognitive biases are exploited to direct user behavior, we consider them necessary but not sufficient for a pluralistic perspective of dark patterns. In some ways, this is due to variance in users' decision-making abilities or particular vulnerabilities (e.g., a user with attention deficit disorders is potentially more likely to be susceptible to attention-grabbing dark patterns like nags, whereas a user with a gambling addiction may be particularly susceptible to gamification or achievement-related dark patterns). Similarly, children and elderly adults are users all the same, but have different

---

78. In particular, we refer to manipulation's definition within psychology, which is "behavior designed to exploit, control, or otherwise influence others to one's advantage" as per the American Psychological Association. *APA Dictionary of Psychology: Manipulation*, AM. PSYCH. ASS'N, https://dictionary.apa.org/manipulation [https://perma.cc/A6HQ-5C87] (last updated Apr. 19, 2018).

79. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1040 (2014); Michael Sobolev, *Online Choice Architecture: The Good, the Bad, and the Complicated*, COMPETITION POL'Y INT'L (Oct. 31, 2022), https://www.pymnts.com/cpi_posts/online-choice-architecture-the-good-the-bad-and-the-complicated/ [https://perma.cc/PXV3-U6PA]; Jan Trzaskowski, *Persuasion, Manipulation, Choice Architecture and 'Dark Patterns'*, *in* RESEARCH HANDBOOK ON EU INTERNET LAW 22–23 (2d ed. 2023), https://papers.ssrn.com/abstract=4491820 [https://perma.cc/CC65-GVWP]; Eric Tjong Tjin Tai, Contract Law and Persuasive Design: Dark Patterns, AI and the Concept of Free Choice 11 (Feb. 1, 2023) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=4537170 [https://perma.cc/V4K9-LYN5]; Rossana Ducato & Enguerrand Marique, Come to the Dark Side: We Have Patterns. Choice Architecture and Design for (Un)Informed Consent, (July 1, 2018) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=3365952 [https://perma.cc/5Z4K-RR6Q]; Michael Evans, Lianne Kerlin, Joanne Parkes & Todd Burlington, *"I Want to Be Independent. I Want to Make Informed Choices.": An Exploratory Interview Study of the Effects of Personalisation of Digital Media Services on the Fulfilment of Human Values*, *in* IMX '22: PROCEEDINGS OF THE 2022 ACM INTERNATIONAL CONFERENCE ON INTERACTIVE MEDIA EXPERIENCES 325, 328 (2022), https://dl.acm.org/doi/10.1145/3505284.3532977 [https://perma.cc/HP6W-65RP]; Kirsten Martin, *Manipulation, Privacy, and Choice*, 23 N.C. J.L. & TECH. 452 (2022); Evan Selinger & Kyle Whyte, *Is There a Right Way to Nudge? The Practice and Ethics of Choice Architecture*, 5 SOCIO. COMPASS 923, 925 (2011); Stuart Mills, Deceptive Choice Architecture and Behavioural Audits 6 (Oct. 2023) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=4575923 [https://perma.cc/BLB6-KMGK]; Matte et al., *supra* note 28, at 13; Gray et al., *supra* note 28; Gunawan et al., *supra* note 28, at 183; Mario Martini & Christian Drews, Making Choice Meaningful – Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy La*w* 24 (Oct. 25, 2022) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=4257979 [https://perma.cc/5UYL-UH5V].

approaches to technology use, different needs, and unique vulnerabilities.[80] This sentiment is shared by a growing body of literature within the digital vulnerabilities space, as well as in dark patterns' technical scholarship: Researchers are increasingly studying dark patterns in specific user contexts such as these.[81]

4. Designing for Transparency

Hidden information and related dark patterns articulate design problems by obscuring, hiding, missing, or otherwise not disclosing relevant information to consumers at critical moments.[82] Transparency is the inverse, instead toting the need for clear, conspicuous provision of information as well as its availability.[83]

Luiza Jarovsky argues for Transparency-by-Design (TbD) in the effort against privacy-related dark patterns[84] which takes a GDPR-oriented framing to consider how non-transparency leads to increased unfairness. Though Jarovsky's scope is privacy-focused, a TbD perspective for other common dark patterns contexts like e-commerce still holds—an informed consumer is in theory more capable of making better decisions for themselves.

The problem with transparency is that it is limited in the context of daily usability. Transparency is certainly desired and necessary for provisioning consumers with relevant information, but consumers themselves may prioritize other values in a given UX decision, like efficiency, affordability, or simplicity. Efforts like "disclosure-by-design"[85] offer a partial solution, especially when considering the

---

80. The Federal Trade Commission, for example, distinguishes unique privacy concerns for children, and notes that older adults are often more susceptible to online fraud. These are only a few examples of areas where children or older adults are at risk; marketing, advertising, or behaviorally influencing designs like dark patterns may exploit children's still-developing neurology or older adults' digital unfamiliarity. *See* FED. TRADE COMM'N, *Children's Privacy*, https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy [https://perma.cc/AD5U-TEJ7]; Bridget Small, *Fighting Fraud Against Older Adults*, FED. TRADE COMM'N (Oct. 18, 2023), https://consumer.ftc.gov/consumer-alerts/2023/10/fighting-fraud-against-older-adults [https://perma.cc/884B-ZXZF].

81. Chamorro et al., *"My Mother Told Me These Things Are Always Fake"*, *supra* note 17; Chamorro et al., *Manipulative Design and Older Adults*, *supra* note 18.

82. Gray et al., *supra* note 14.

83. Considerable literature in privacy or technology ethics, spanning both computer science and legal scholarship, discuss transparency at length. For black-box algorithms and sophisticated systems, for example, the Association for Computing Machinery Fairness, Accountability, and Transparency Conference (FAccT) solicits and aggregates research that often spans policy or regulatory implications.

84. Luiza Jarovsky, Transparency by Design: Reducing Informational Vulnerabilities Through UX Design (2022) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=4119284 [https://perma.cc/2XGB-3SKU]; Jarovsky, *supra* note 2, at 5.

85. Chris Norval, Jennifer Cobbe, Kristin Cornelius & Jatinder Singh, *Disclosure by Design: Designing Information Disclosures to Support Meaningful Transparency and Accountability*, *in* FAccT '22: PROCEEDINGS OF THE 2022 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 679 (2022), https://dl.acm.org/doi/10.1145/3531146.3533133 [https://perma.cc/3D4Z-BFGB].

potential for information overload or users becoming so inured to overcommunication that they begin to ignore it.[86]

Relatedly, trustworthiness, or trustworthy patterns, perhaps provide the closest definition of what might be a desirable antithesis to dark patterns. Trust implicates a degree of transparency without the tensions between lengthy (but transparent) disclosures and efficient usability for a digital service. Conceptually, however, trust (while necessary for the smooth operation of daily modern life) is described by Richards and Hartzog as nearly impossible without loyalty—rather, they describe loyalty as the mechanism by which trust is meaningfully enabled.[87]

II. THE LIMITATIONS OF REGULATING "DARK PATTERNS"

Despite a rapidly growing body of rules, rights, and scholarship, dark patterns regulatory approaches contain weaknesses that industry proponents tend to rely on in critiques. Objections from industry and interested parties like the Disruptive Competition Project, for example, claim that:

> [C]ontrary to what the FTC seems to believe, these design practices are not harmful to consumers. Consumers are in fact aware of many of these choices by businesses, and they are beneficiaries of the choices, not victims. The American consumer is an informed and educated consumer that understands how online retail works and how these business practices function.[88]

Such criticism exploits what we consider to be three main pathologies plaguing dark patterns regulation: first, that this still-developing body of regulatory approaches lacks a clear value anchor; second, that many of the leading approaches are overly focused on discrete and atomized choices instead of the big picture and effects at scale; and finally, that measurement-reliant approaches use prohibitively restrictive criteria that make it difficult to judge something as fluid and subjective as design.

Legal scholars make several contributions towards solving the dark patterns problem, some of which already influenced regulations now in effect. Jennifer King and Adriana Stephan, for example, discuss the operationalization of dark patterns regulation with the CCPA as a case study, with Jennifer King acting as one of the

---

86. In fact, the blindness that occurs from habit can sometimes facilitate the effectiveness of dark patterns. Take, for example, consent banners in mobile interfaces that put one option frequently on the right side (where the majority of right-handed users might tap by default) as opposed to a less common space on the screen. If not paying close attention to every notice, the cognitive bias of inattentive blindness may be exploited if the notice options are suddenly switched with little other indication.

87. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 436 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*].

88. Daniel Luque, *Examining the FTC's Hostility to Common Design Practices*, DISRUPTIVE COMPETITION PROJECT (Dec. 20, 2023), https://project-disco.org/competition/examining-the-ftcs-hostility-to-common-design-practices/ [https://perma.cc/UQY6-N8HS].

consultants for the dark patterns provision present within the California regulation.[89] This body of literature unsurprisingly spans a wealth of perspectives, from consumer law to competition, privacy regulations, and beyond.

A. Unclear Value Anchor

Within dark patterns legal scholarship, a multitude of potential approaches (similar to privacy legal scholarship) further reveals variety in what values are prioritized first or in lieu of others. Autonomy, fairness, equity, accessibility, and transparency are but a few of these desired traits for digital designs. But even the definition of each of these terms (and what should be prioritized within each value) is also up for ample debate.

What counts as fairness? What do we mean by autonomy? Do we prefer to align it more with agency or choice? Designs that promote one value may result in negative or undesirable effects that undermine other values. For example, providing users with highly granular choices and detailed disclosures may make design more transparent, but does little to solve decision fatigue. Instead, such design choices actually increase cognitive labor for an end user. On the other hand, failing to provide appropriate disclosures and options can disproportionately sway design outcomes towards the design deployer. These tensions present an unclear value anchor for the reduction of dark patterns in digital interfaces. We have a long wish list of values, and no current standard by which to effectively manage them.

Autonomy and choice arguments are particularly popular in anti-dark patterns regulation and scholarship.[90] This popularity raises questions of which direction to improve online choice architecture (OCA); should more choices be provided (increasing autonomy and thus countering dark patterns like *bad defaults*), or should less choices be available (assuming, of course, that the underlying default settings are 'good' or in users' benefit)? "*Bright patterns*"[91] combat the undesirable nature of dark patterns with counterexamples but may risk potential paternalism through a loss of autonomy—as such, many approaches still tout the necessity of free choice.[92]

---

89. King & Stephan, *supra* note 59, at 250.

90. Leiser & Yang, *supra* note 2; Sobolev, *supra* note 79; Matte et al., *supra* note 28; COMPETITION AND MKTS. AUTH., *supra* note 23; Ducato & Marique, *supra* note 79; Martin, *supra* note 79; Selinger & Whyte, *supra* note 79; Kathleen D. Vohs, Roy F. Baumeister, Brandon J Schmeichel, Jean M. Twenge, Noelle M. Nelson & Dianne M. Tice, *Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative*, 94 J. PERSONALITY & SOC. PSYCH. 883 (2008); Andrea Kiesel, Annika Wagener, Wilfried Kunde, Joachim Hoffmann, Andreas J. Fallgatter & Christian Stöcker, *Unconscious Manipulation of Free Choice in Humans*, 15 CONSCIOUSNESS & COGNITION 397 (2006); *IP Report: Shaping Choices in the Digital World*, LABORATOIRE D'INNOVATION NUMÉRIQUE DE LA CNIL (Apr. 16, 2020), https://linc.cnil.fr/ip-report-shaping-choices-digital-world [https://perma.cc/3SWT-VHQZ].

91. Graßl et al., *supra* note 66; *see also* Sandhaus, *supra* note 66 (providing a resource of bright pattern examples by scholar Hauke Sandhaus).

92. Leiser & Yang, *supra* note 2.

It is yet unclear, however, if the availability of more choices is always better.[93] What happens if greater autonomy is not what the user wants? More toggles, choices, and control may sound better than the status quo of comparatively limited choice, but what if consumers want the number of options in an interface to remain the same from a design standpoint and instead want choice offerings to be better, fairer, or more loyal instead? And yet, approaches that reduce decision-making labor and friction (by making better privacy default settings, for example, without the provision of additional toggles) fails to improve user control and could veer into paternalism and interfere with a consumer's other desires. Users are known to have some positive feelings toward personalized advertising or recommendations[94] (which a privacy-forward design might turn off by default, or not provide at all) insofar as it provides utility or customer service.

Similarly, "fair patterns" may be desirable, but "fairness" takes many definitions at the intersection of technology and law and additionally raises the question of "fairness to/for *whom*." Fairness perspectives may also be more reliant on threshold or balancing scale tests (e.g., determining what is fair between two parties or across multiple groups), and—depending on the selected definition of fairness—may be more oriented towards equality rather than equity, which may be desirable to prevent harms to especially vulnerable groups.

Improving privacy also has its quirks. The concept of nudging *for* privacy is an area of extensive exploration in both the legal and computer science fields.[95] In the

---

93. *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); Jordan Francis, Woodrow Hartzog & Neil Richards, *Privacy's Autonomy Thicket, Untangling Choice, Consent, and Control*, 1 GEO. WASH. J.L. & TECH. (forthcoming 2025); Daniel J. Solove and Woodrow Hartzog, *Kafka in the Age of Ai and the Futility of Privacy As Control*, 104 B.U. L. Rev. 1021 (2024).

94. Evans et al., *supra* note 79; Katie O'Donnell & Henriette Cramer, *People's Perceptions of Personalized Ads*, *in* WWW '15 COMPANION: PROCEEDINGS OF THE 24TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 1293 (2015), https://dl.acm.org/doi/10.1145/2740908.2742003 [https://perma.cc/7KAA-VQMH]; Leslie K. John, Tami Kim & Kate Barasz, *Ads That Don't Overstep*, HARV. BUS. REV., Jan.-Feb. 2018, at 62.

95. Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget & N. Sadeh, *A Field Trial of Privacy Nudges for Facebook*, *in* CHI '14: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 2367 (2014), http://dl.acm.org/citation.cfm?doid=2556288.2557413 [https://perma.cc/W8RJ-DKCY]; Yang Wang, Pedro Giovanni Leon, Xiaoxuan Chen, Saranga Komanduri, Gregory Norcie, Kevin Scott, Alessandro Acquisti, Lorrie Faith Cranor & Norman Sadeh, *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307 (2013); Yang Wang, Pedro Giovanni, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti & Lorrie Faith Cranor, *Privacy Nudges for Social Media: An Exploratory Facebook Study*, *in* PROCEEDINGS OF THE 22ND INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 763 (2013); Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE SEC. & PRIV. 82 (2009); Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50 ACM COMPUTING SURVS. 1 (2017); Selinger & Whyte, *supra* note 79; Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito & Koji Yatani, *Exploring Nudge Designs to Help Adolescent SNS Users Avoid Privacy and Safety Threats*, *in* CHI '20: PROCEEDINGS OF THE 2020 CHI CONFERENCE ON HUMAN

privacy field, nudges are a viable tool to promote transparency and prod users in more privacy-protective directions. Considering the recent history of dark patterns regulation and enforcement being frequently handled by data protection regulations like the GDPR and CCPA, this raises questions of whether prioritizing certain values like privacy results in interfaces which consumers might consider as 'dark patterns' that interfere with their ability to most efficiently use a digital service.

Brenncke focuses on autonomy, critiquing extant regulations for the lack of a centralized and powerful autonomy model.[96] He highlights the regulation of dark patterns as "normatively challenging," because determining what nudging is legitimate and what nudging is not remains a legal gray zone.[97] While the autonomy model proposed by Brenncke is valuable and desirable, autonomy offers a limited and comparatively less flexible solution compared to loyalty. Loyalty, we argue, is better suited to navigating that gray area.

B. Atomistic Approaches, Especially for Choice

A focus on discrete, atomistic choices and individual harms, particularly when taken to a highly granular level (e.g., the harm arising from a single dark pattern) has

---

FACTORS IN COMPUTING SYSTEMS 1 (2020), http://doi.org/10.1145/3313831.3376666 [https://perma.cc/PX9E-95ZF]; Bo Zhang & Heng Xu, *Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes*, *in* CSCW '16: PROCEEDINGS OF THE 19TH ACM CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING 1676 (2016), http://doi.org/10.1145/2818048.2820073 [https://perma.cc/8K2F-79F6]; Logan Warberg, Alessandro Acquisti & Douglas Sicker, *Can Privacy Nudges Be Tailored to Individuals' Decision Making and Personality Traits?*, *in* WPES '19: PROCEEDINGS OF THE 18TH ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 175 (2019), http://doi.org/10.1145/3338498.3358656 [https://perma.cc/8ACD-YYCB]; Yifat Nahmias, Oren Perez, Yotam Shlomo & Uri Stemmer, *Privacy Preserving Social Norm Nudges*, 26 MICH. TECH. L. REV. 43 (2019); Sven Bock & Nurul Momen, *Nudging the User with Privacy Indicator: A Study on the App Selection Behavior of the User*, *in* NORDICHI '20: PROCEEDINGS OF THE 11TH NORDIC CONFERENCE ON HUMAN-COMPUTER INTERACTION: SHAPING EXPERIENCES, SHAPING SOCIETY 1 (2020), http://doi.org/10.1145/3419249.3420111 [https://perma.cc/T3HW-28UD]; Hazim Almuhimedi, Florian Schaub, N. Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor & Yuvraj Agarwal, *Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging*, *in* CHI '15: PROCEEDINGS OF THE 33RD ANNUAL ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 787 (2015), http://doi.org/10.1145/2702123.2702210 [https://perma.cc/FVU5-Z67S]; Torben Jan Barev & Andreas Janson, *Towards an Integrative Understanding of Privacy Nudging – Systematic Review and Research Agenda*, *in* PROCEEDINGS OF THE 18TH ANNUAL PRE-ICIS WORKSHOP ON HCI RESEARCH IN MIS 1 (2019), https://www.alexandria.unisg.ch/258828/ [https://perma.cc/VR6M-239Q]; Brett M. Frischmann, Nudging Humans (Aug. 1, 2019) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=3440791 [https://perma.cc/KS87-Y3H7].

96. M. Brenncke, *A Theory of Exploitation for Consumer Law: Online Choice Architectures, Dark Patterns, and Autonomy Violations*, 47 J. CONSUMER POL'Y 127 (2024); Martin Brenncke, *Regulating Dark Patterns*, 14 NOTRE DAME J. INT'L & COMPAR. L. 39 (2024) [hereinafter Brenncke, *Regulating Dark Patterns*].

97. Brenncke, *Regulating Dark Patterns*, *supra* note 96.

several failings. Current approaches are over-reliant on such atomistic perspectives. This subjects current enforcement or regulation to industry criticism[98] while also making individual court claims potentially quite difficult if consumers seek redress.

Recently developed rules and guidance tend towards consent-based or options-based applications, like the dark patterns provisions for the CCPA through the CPRA and the definition provided by the DSA.[99] In doing so, the DSA's definition potentially necessitates a concept of what qualifies as reasonable control, which is difficult to standardize. Overreliance on autonomy additionally presumes that users are fully autonomous; this neglects situations or populations in which people may exercise less autonomy in a given decision interaction. For example, membership in a vulnerable population (children, the elderly, or the cognitively impaired)[100] or imbalanced, inherent power dynamics (employees using corporate software, gig workers, etc.) may preemptively enter users into a state where the immediate decision in question under dark patterns regulation is already problematic.

---

98. Luque, *supra* note 88.

99. Conversely, older enforcement actions more commonly refer to dark patterns in case-adjacent documentation in the absence of explicit provisions to refer to. *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service (Nov. 3, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service [https://perma.cc/MDX9-L6HQ]; *Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc.*, FED. TRADE. COMM'N (Sept. 2, 2020), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-rohit-chopra-regarding-dark-patterns-matter-age-learning-inc [https://perma.cc/V33Y-A3MB]. As such, relevant case documents often do not include the term "dark patterns" in case facts. However, in the wake of the DSA and CPRA definitions, as well as the FTC's "Bringing Dark Patterns to Light" workshop staff report, we expect to see more explicit references in enforcement to dark patterns. More recent cases, e.g. *In re Epic Games, Inc.,* and *FTC v. Amazon.com, Inc.*, have already begun to directly cite dark patterns in case texts. *See* Final Complaint and Order, *In re* Epic Games, Inc., FTC Docket No. C-4790 (Mar. 13, 2023); Amended Complaint, FTC v. Amazon.com, Inc., No. 2:23-cv-00932 (W.D. Wash. Sept. 20, 2023).

100. Chamorro et al., *supra* note 17; Chamorro et al., *Manipulative Design and Older Adults*, *supra* note 18; Arianna Rossi, Rachele Carli, Marietjie W. Botes, Angelica Fernandez, Anastasia Sergeeva, & Lorena Sánchez Chamorro, *Who Is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability*, 55 COMPUT. L. & SEC. REV., Nov. 2024, at 1, https://www.sciencedirect.com/science/article/pii/S0267364924000979 [https://perma.cc/C9EN-FA9X]; Kalya Win Aung, Ewan Soubutts & Aneesha Singh, *"What a Stupid Way to Do Business": Towards an Understanding of Older Adults' Perceptions of Deceptive Patterns and Ways to Develop Resistance*, 8 CHI PLAY 1 (2024); René Schäfer, Sarah Sahabi, Annabell Brocker & Jan Borchers, *Growing Up With Dark Patterns: How Children Perceive Malicious User Interface Designs*, *in* NORDICHI '24 PROCEEDINGS OF THE 13TH NORDIC CONFERENCE ON HUMAN-COMPUTER INTERACTION 1 (2024), https://dl.acm.org/doi/10.1145/3679318.3685358 [https://perma.cc/945N-52ZF].

C. Unresolved Measurement Methods

By design, many parts of the law rely on measurements in some form to determine whether evidentiary thresholds or other minimum bars are met.[101] Some legal subfields do so quite rigorously and effectively, like finance and medicine—fields with a remarkable affinity for granular risk assessments and detailed auditing procedures for protecting material goods.[102] Privacy, however, as intrinsically related to and intertwined with cybersecurity, has proven more difficult for ironing out regulatory thresholds and handling non-material harms.[103] Some scholars have suggested moving towards measurement-based approaches like impact assessments.[104] With some of the more established dark patterns remedies or prohibitions outlined in privacy and data protection laws like the GDPR and CCPA, lawmakers might be more attracted to more measurement-based thresholds. Learning from privacy law's struggles in measurement thresholds can better guide lawmakers in crafting rules for digital spaces and their design.

Like privacy, dark patterns regulation suffers from less-defined concepts of harm than older legal fields. Warren and Brandeis' first right to privacy takes a property-based (thus, material) stance that increasingly feels ill-suited to tackle the distributed, in-the-cloud expanse of the modern digital experience. To close the gaps that Warren and Brandeis could not have foreseen in their more-analog days, scholars like Citron and Solove articulate a new taxonomy of privacy harms that includes those less traditionally measured.[105] Specifically, Citron and Solove note that:

> The requirement of harm has significantly impeded the enforcement of privacy law. In most tort and contract cases, plaintiffs must establish that they have suffered harm. Even when legislation does not require it, courts have taken it upon themselves to add a harm element. Harm is also a requirement to establish standing in federal court. In *Spokeo, Inc. v. Robins* and *TransUnion LLC v. Ramirez,* the Supreme Court ruled that

---

101. *See, e.g.*, *Environmental Assessment Tools and Templates*, FEMA, https://www.fema.gov/emergency-managers/practitioners/environmental-historic/assessments [https://perma.cc/J33C-CQ2S] (last updated May 10, 2023).

102. For example, this includes approving the development of pharmaceutical drugs for consumer use. Russell Katz, *FDA: Evidentiary Standards for Drug Development and Approval*, 1 NEURORX 307 (2004). Various securities laws and rules, for example, or the Federal Deposit Insurance Corporation (FDIC) rules for banking and insurance. Or more simply, consider tax law and how evasion is evaluated. *See* Somchai Richupan, *Measuring Tax Evasion: An Introduction to Measurement Techniques*, 21 FIN. & DEV. 38 (1984).

103. *See, e.g.*, DANIEL J. SOLOVE AND WOODROW HARTZOG, BREACHED! WHY DATA SECURITY FAILS AND HOW TO IMPROVE IT 131–57 (2022).

104. *See, e.g.*, A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713 (2015); Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J.L. & TECH. 117 (2021).

105. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022).

> courts can override congressional judgment about cognizable harm and dismiss privacy claims.[106]

Following on the heels of years of ever-changing privacy regulation, digital service and experience laws have the unique opportunity of rectifying the wrongs that plagued (and continue to challenge) privacy law. How the DSA, DMA, and similar regulations will determine noncompliance in practice remains to be seen, but without greater flexibility regarding measurement methods, these laws risk the same toothlessness that many privacy laws or existing agency mandates are accused of having.

One of the primary challenges stymying scholars and governments alike in the battle against dark patterns is the measurement of harm.[107] While a single dark pattern design may result in extreme material harms to an individual encountering it, it is often acknowledged that the vast majority of dark patterns likely constitute *de minimis* harms when observed in isolation.[108] Take, for example, robust scholarship on dark patterns in consent regimes. One cookie consent banner dark pattern might not immediately result in a user's distinct perception of being harmed. But what of a user's experience in sum, across any length of an online interaction session?[109] A person may visit dozens of websites in quick succession, all while logged into a personal account in-browser or on-phone; if they are presented with deceptive or obfuscating cookie consent banners on each of these sites and the most efficient option on each is to accept all tracking, then the overall outcome of a few minutes of

---

106. *Id.* at 793.

107. *See, e.g.*, Justin Hurwitz, *Designing a Pattern, Darkly*, 22 N.C. J.L. & TECH. 57 (2020); Kyle Langvardt, *Regulating Habit-Forming Technology*, 88 FORDHAM L. REV. 129 (2019); Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021); Fabiana Di Porto & Alexander Egberts, *The Collective Welfare Dimension of Dark Patterns Regulation*, 29 EUROPEAN L.J. 114 (2024); Santos et al., *supra* note 2.

108. Arunesh Mathur, Mihir Kshirsagar & Jonathan Mayer, *What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods*, *in* CHI '21: PROCEEDINGS OF THE 2021 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1 (2021), https://doi.org/10.1145/3411764.3445610 [https://perma.cc/9679-SD5P]; Santos et al., *supra* note 2; Cristiana Santos & Arianna Rossi, *The Emergence of Dark Patterns as a Legal Concept in Case Law*, INTERNET POL'Y REV. (July 31, 2023), https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept [https://perma.cc/QC6F-Z8ML]; Cristiana Santos, Nataliia Bielova, Sanju Ahuja, Christine Utz, Colin Gray & Gilles Mertens, Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA? (July 24, 2024) (unpublished manuscript) (on file with SSRN), https://www.ssrn.com/abstract=4899559 [https://perma.cc/DY98-FWCB]; Johanna Gunawan, Cristiana Santos & Irene Kamara, *Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions*, *in* CSLAW '22: PROCEEDINGS OF THE 2022 SYMPOSIUM ON COMPUTER SCIENCE AND LAW 181 (2022), https://dl.acm.org/doi/10.1145/3511265.3550448 [https://perma.cc/PSL5-JSV7].

109. Gray et al., *supra* note 20. The authors find and discover a temporal component to how users perceive manipulation in digital technologies.

online interaction may be enough to expose their profile to hundreds, if not thousands, of third parties.[110]

III. DESIGNING FOR LOYALTY

In this Part, we outline the components of a design loyalty concept for the law, which looks to a designer's goals, how the risks and burdens resulting from a design are distributed, and the relative distribution of the benefits of a design. A design is disloyal when the risks and benefits disproportionately advantage a platform at the expense of a trusting party.

Richards and Hartzog build out a robust theory of loyalty for data relationships towards protecting and preserving user privacy.[111] The scholars have argued:

> [D]uty of loyalty framed in terms of the best interests of digital consumers is coherent and desirable and should become a basic element of U.S. data privacy law. Such a duty of loyalty would compel loyal acts and also constrain conflicted, self-dealing behavior by companies. It would shift the default legal presumptions surrounding a number of common design and data processing practices. It would also act as an interpretive guide for government actors and data collectors to resolve ambiguities inherent in other privacy rules. A duty of loyalty, in effect, would enliven almost the entire patchwork of U.S. data privacy laws. And it would do it in a way that is consistent with U.S. free expression goals and other civil liberties.[112]

The duty of loyalty proposed by Richards and Hartzog is *a response to the risk of opportunism* rampant in people's relationships with organizations that are largely mediated through technology. They wrote: "[T]he failures of American privacy law have enabled corporate opportunism and manipulation of consumers using human information."[113]

This has been a particular problem in the context of "personalized" technologies that promise to know us so that they can better satisfy our needs and wants. Insufficiently constrained by the law, companies can deploy a potent cocktail of techniques derived from cognitive and behavioral science to "nudge" or otherwise influence the choices we make.[114] But these highly capitalized tech companies have

---

110. Matte et al., *supra* note 28; Gray et al., *supra* note 28.

111. Richards & Hartzog, *supra* note 8; *see generally* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 87, at 457; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1198 (2017); Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579, 582 (2017); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection*?, 6 EUR. DATA PROT. L. REV. 492 (2020) [hereinafter Richards & Hartzog, *Relational Turn*]; Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022); Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022).

112. Richards & Hartzog, *supra* note 8, at 966–67.

113. *Id.* at 967.

114. *Dark Patterns - When a Nudge Becomes a Shove*, CDS (April 2023), https://blog.cds.co.uk/dark-patterns-when-a-nudge-becomes-a-shove [https://perma.cc/S9LP-

not acted like the benevolent "choice architects" some had hoped they might become. Technologies—and choice architecture—advertised as serving consumers have instead become weaponized, serving commodified consumers up to the companies and their commercial and political advertiser clients.[115]

We return to the debate on updating the "dark" patterns term. Alternatives like "deceptive" or "manipulative" certainly describe some kinds of dark pattern designs, as do "sludges,"[116] but no single term pulls as much weight as has been prescribed to "dark patterns" by stakeholders across disciplines and research areas. Even the DSA's lengthy and articulate definition of dark patterns, complete with explicit

---

ZZ9G]; Stuart Mills, *Nudge/Sludge Symmetry: On the Relationship Between Nudge and Sludge and the Resulting Ontological, Normative and Transparency Implications*, BEHAVIOURAL PUB. POL'Y 1 (2020); Şebnem Özdemir, *Digital Nudges and Dark Patterns: The Angels and the Archfiends of Digital Communication*, 35 DIGIT. SCHOLARSHIP IN THE HUMANS. 417 (2020); Jeni Paay & Yvonne Rogers, *The Dark Side of Interaction Design: Nudges, Dark Patterns and Digital Addiction: Panel Presented at OZCHI 2019*, *in* OzCHI '19: PROCEEDINGS OF THE 31ST AUSTRALIAN CONFERENCE ON HUMAN-COMPUTER-INTERACTION 2 (2020), https://doi.org/10.1145/3369457.3369547 [https://perma.cc/A7LD-KZJT]; Francis Joseph Costello, Jinho Yun & Kun Chang Lee, *Digital Dark Nudge: An Exploration of When Digital Nudges Unethically Depart*, *in* PROCEEDINGS OF THE 55TH HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES 4348 (2022), http://hdl.handle.net/10125/79868 [https://perma.cc/C9V3-SG4X]; Shruthi Sai Chivukula, Jason Brier & Colin M. Gray, *Dark Intentions or Persuasion? UX Designers' Activation of Stakeholder and User Values*, *in* DIS '18 COMPANION: PROCEEDINGS OF THE 2018 ACM CONFERENCE COMPANION PUBLICATION ON DESIGNING INTERACTIVE SYSTEMS 87 (2018), http://doi.org/10.1145/3197391.3205417 [https://perma.cc/U8Q6-JAXV]; Eslambolchilar et al., *supra* note 15; Shruthi Sai Chivukula, Chris Watkins, Lucca McKay & Colin M. Gray, *"Nothing Comes Before Profit": Asshole Design in the Wild*, *in* CHI EA '19: EXTENDED ABSTRACTS OF THE 2019 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1 (2019), https://doi.org/10.1145/3290607.3312863 [https://perma.cc/8B44-V572]; Colin M. Gray, Shruthi Sai Chivukula & Ahreum Lee, *What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit*, *in* DIS '20: PROCEEDINGS OF THE 2020 ACM DESIGNING INTERACTIVE SYSTEMS CONFERENCE 61 (2020), https://dl.acm.org/doi/10.1145/3357236.3395486 [https://perma.cc/LP5U-WPES].

115. Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U.L. REV. 961, 967 (2021).

116. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008); Olivia Goldhill, *Politicians Love Nudge Theory. But Beware Its Doppelgänger "Sludge,"* QUARTZ (July 31, 2019), https://qz.com/1679102/sludge-takes-nudge-theory-to-new-manipulative-levels/ [https://perma.cc/9XC9-ZEJ2]; Mills, *supra* note 114; Özdemir, *supra* note 114; Richard H. Thaler, *Nudge, Not Sludge*, 361 SCI. MAG. 431 (2018) https://science.sciencemag.org/content/361/6401/431 [https://perma.cc/Q83J-K6ZD]; Mark Petticrew, Nason Maani, Luisa Pettigrew, Harry Rutter & May Ci Van Schalkwyk, *Dark Nudges and Sludge in Big Alcohol: Behavioral Economics, Cognitive Biases, and Alcohol Industry Corporate Social Responsibility*, 98 THE MILBANK Q. 1290 (2020); Crawford Hollingworth & Liz Barker, *Sludge Detectives: The "BE Police" Take On Hotel Booking Sites*, BEHAVIORAL SCIENTIST (Oct. 9, 2018), https://behavioralscientist.org/sludge-detectives-the-be-police-take-on-hotel-booking-sites/ [https://perma.cc/38MD-ZZ4D].

examples of what VLOPs should *not* do, fails to encompass the full potential described by extant scholarly taxonomies.

It makes sense for regulators to seize upon notions of deception and harm to regulate adversarial design choices. The problem is that concepts of "harm" and "deception," by themselves, are underinclusive. A better approach would be to focus on the root pathology of dark patterns—abuse of the power to leverage design for self-dealing—as well as design negligence and failures to prevent outsized benefit for platforms.

Loyalty articulates the inherent vulnerability in relationships (articulated in socio-digital contexts by DiPaola and Calo).[117] If data relationships are design relationships, then data protection is less sensitive to the other relationships beyond it—privacy rules that we presently have often ignore or minimize the importance, impact, or variability in those relationships. Relationships are directly implicated in design loyalty, borrowing again from relational approaches to privacy and data protections.[118]

Relational approaches to tech regulation require a *perception of trust* beyond the trust one might place in the stability of building construction. Instead, trust in relationships carry temporal components (that is, relationships are ongoing rather than instantiated and static). The information era complicates the inherently social dynamic of trust, even as this trust is what cybersecurity expert Bruce Schneier argues is necessary for a thriving digital society.[119]

Richards and Hartzog discuss trust in-depth, noting that loyalty builds trust "in ways that existing models of privacy protection fail to achieve;"[120] thus their framework presents an alternative to prior approaches that should improve upon the rest. This proposed design loyalty approach is inherently closely tied to Richards and Hartzog insofar as it builds directly upon their argument, but with design loyalty the focus shifts from building trust through loyal design practices across a tech organization's overall practices to building trust where a user will actually pass judgment: through the interface directly. As such, design loyalty does not replace privacy loyalty but rather argues that the expansion from privacy and data concerns toward holistic digital experience issues improve consumer experiences of both. It reflects extant trends in technology regulations—specifically, the EU DSA and DMA demonstrate a recognized need for tech regulations at the service or platform level, beyond privacy and data protections afforded by the GDPR.

However, the DSA primarily focuses on the heavy hitters in the digital services industry: VLOPs to intermediaries. This does not account for the potential impact of various first-party users on each other within design spaces. The DSA also only covers EU citizens (though we may optimistically see potential impact on global interfaces), and dark pattern behaviors or user interface rules only feature minimally in the greater expanse of the full regulation. It does not fully address the challenges

---

117. Daniella DiPaola & Ryan Calo, Socio-Digital Vulnerability (Jan. 7, 2024) (unpublished manuscript) (on file with SSRN), https://papers.ssrn.com/abstract=4686874 [https://perma.cc/6FMJ-MXED].

118. Richards & Hartzog, *A Relational Turn*, *supra* note 111.

119. BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012).

120. Richards & Hartzog, *supra* note 8, at 1020.

present in dark patterns regulation overall, but instead provides an encouragingly robust example to continue developing further. As such, in this Part we demonstrate how the design loyalty components overcome the weaknesses of present dark patterns regulatory approaches and other conceptual alternatives.

In the United States, a design loyalty framing may contribute to the issuance of additional rules under Section 18 of the FTC Act via the Magnuson Moss Warranty—Federal Trade Commission Improvement Act (Magnuson Moss Act),[121] as discussed by Lindsay Wilson regarding the future regulation of dark patterns.[122] An example of such rules includes the 2010 Restore Online Shoppers' Confidence Act (ROSCA)[123] to prevent against "negative option marketing," relating to dark patterns like "Hidden Information," "Bundling," "Sneaking," "Adding Steps/Creating Barriers," and otherwise "Roach Motels."[124] Though ROSCA pertains exclusively to disclosures regarding consumer options, the FTC has increasingly relied on ROSCA to regulate against dark patterns, as with their settlements with MoviePass and Vonage in 2021 and 2022, respectively.

In prioritizing direct, front-end interfaces, design loyalty provides more for a user's immediate perception and development of trust in a platform (whereas some aspects of privacy loyalty may be partially achieved through back-end fixes, leaving breaches of privacy loyalty more capable of going unnoticed by consumers). An otherwise "neutral" website is anti-user if the back end is highly privacy invasive behind the scenes. However, design loyalty requires that the front-end communicate trustworthiness first and foremost, as well as having underlying architectures deliver upon interface promises. This provides greater potential for trust (and subsequently, awareness of broken trust) to be established quickly, which empowers consumers by giving back some control over their experiences without necessitating more control through more toggles.

Naturally, a popular[125] critique would be "well, what if the consumer WANTS a given design because it is more efficient (or time-saving, or simply more beautiful)?" Design loyalty does not prohibit efficient, time-saving, or aesthetic designs that serve

---

121. *Magnuson Moss Warranty-Federal Trade Commission Improvements Act*, FED. TRADE COMM'N, https://www.ftc.gov/legal-library/browse/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act [https://perma.cc/TW9U-FBVZ].

122. Lindsay Wilson, Note, *Is There a Light at The End of the Dark-Pattern Tunnel?*, 91 GEO. WASH. L. REV. 1048 (2023).

123. "Restore Online Shoppers' Confidence Act" (ROSCA), 15 U.S.C. §§ 8401–8405.

124. Gray et al., *supra* note 20.

125. "Popular," because dark patterns scholars who actively advocate against their deployment often encounter such comments in personal and professional conversations. One need only skim *amici* from opposing sides of ongoing dark patterns litigation to see such criticism formally, and in real-time, or refer to opposing opinions such as those from industry organizations like Project DISCO, which try to frame dark patterns as normal, conventional design practice (*see* Luque, *supra* note 88). *See, e.g.*, [Proposed] Brief of Amicus Curiae Interactive Advertising Bureau in Support of Defendants' Motions to Dismiss, Fed. Trade Comm'n v. Amazon.com, Inc., No. 2:23-cv-00932 (W.D. Wash. Oct. 25, 2023), https://www.iab.com/wp-content/uploads/2023/10/IAB-Amicus-Brief-re-FTC-v.-Amazon-Dark-Patterns.pdf [https://perma.cc/455H-PLDT] ("What the FTC's Complaint describes as 'dark patterns' are merely a series of normal and lawful business practices cobbled together and grouped under ominous buzzwords.").

consumers' other interests, but rather requires that tech organizations reflect upon whether a design maximizes efficiency at a cost to other values important to loyalty. That is, in maximizing efficiency for all users on their platform, are they potentially harming vulnerable populations like children or the cognitively impaired? Did a company diligently ensure that their design maximizes efficiency in a manner that still minimizes the costs potentially incurred by users (either one user at more vulnerable points of time, or for vulnerable users en masse)? Rather than tyrannizing aesthetic innovation and creativity in the design industry, design loyalty allows for design freedom but does not allow it to run unbridled. Instead, it seeks to balance asymmetries and promote fairness; designs made to maximize one value like profit or efficiency should not improperly infringe upon others, like well-being and privacy. Design loyalty thus demands trustworthy front-end experiences and equivalent trustworthiness from the back-end architectures that support them.

Our argument raises the question of whether Richards and Hartzog's original duty of loyalty proposal for privacy law is already sufficient for addressing dark patterns. Their proposal already implicates nudges, for example, and a loyalty principle in data relationships should, in theory, cover and resolve dark patterns applied to and deployed in privacy contexts like data collection, processing, sharing, and more. However, dark patterns may be deployed anywhere, and end users' resources might be exploited. For example, their time might be vied for by addictive video games or their emotions preyed upon during purchase interactions in e-commerce. In *Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps*, Marijn Sax echoes a beyond-privacy sentiment by describing a "privacy reflex" in discussions of the consequences of digital technologies—quick recognition of technologies' privacy threats is well and good, but in many cases might be a secondary problem rather than the heart of the issues that plague relationships within digital society.[126]

When comparing loyalty or disloyalty as a term of art against the other framings described in Part II, we believe that the lexical utility of loyalty unites the alternate framings more cohesively. If transparency is a vehicle for improving trust, then loyalty is achieved through building trust. If fairness carries both one-to-one relational implications as well as implications across multiple societal subgroups, loyalty's conceptual flexibility does not come into conflict with subfield-specific definitions of fairness (for example, algorithmic, consumer, or market fairness). If brightness and darkness are best at providing imagery or describing moral values but less operational clarity, then loyalty's relational structure helps us find middle ground.

A. Anchoring Values in Relationships

A loyalty framing prevents ideological drift between the many, and often competitive, values implicated in the effort to minimize dark patterns. Its main tenets

126. MARIJN SAX, BETWEEN EMPOWERMENT AND MANIPULATION: THE ETHICS AND REGULATION OF FOR-PROFIT HEALTH APPS 8 (Bernt Hugenholtz ed., 2021), https://www.ivir.nl/publicaties/download/Sax_INFO_47-1.pdf [https://perma.cc/J9YX-M7MN].

are relational: prioritizing people over profit, encouraging trust, and instilling an anti-betrayal ethos. This provides a centralized concept with which to reason through "darkness," spanning the normative (as well as instrumental) perspectives first compiled by Mathur et. al. in their work articulating the harms identified in dark patterns literature.[127]

The alternate framings mentioned in Part II typically center dark patterns around a given value, like autonomy or transparency. By proposing loyalty as a framing for dark patterns, we do not suggest that the other implicated values are unnecessary or not desirable; rather, design loyalty brings together prior suggestions into a more centralized lens.

1. Vulnerability and Power in Context

Context is imperative to understanding a given user's particular vulnerabilities or the relational power imbalances they are uniquely subject to.[128] Recent concepts of digital vulnerability[129] highlight the relational nature of user experiences, considering consumers not only as market actors but as societal actors as well.[130] Across a broad expanse of users, however, individuals will have different sensitivities and thus vulnerabilities in a variety of contexts. Such contexts impact one's perception of a relationship's success, failure, or health. Privacy, with ample dark patterns scholarship especially within the consent space, is a comparatively well-studied dark patterns context. Commerce and games are also popular targets for dark patterns enforcement.

Emergent work and case law inspecting the games industry (particularly gambling-inspired mechanisms like loot boxes and "free to play" systems) highlight power disparities within the developer-player relationship well. These cases demonstrate the need for an anti-betrayal ethos in the design of technologies, not only in the underlying business practices beneath glossy interfaces but in the user interface elements that deliver the final experience to users. In the United States and European Union, regulators have recently pursued enforcement actions against distributor Epic Games for anti-consumer mechanics in their wildly popular game *Fortnite*.[131] The Federal Trade Commission addressed the inconspicuous nature of

---

127. Mathur et al., *supra* note 108.

128. Michelle Liu, *Digital Vulnerability: Rethinking Power Imbalances in the Digital Age*, 32 EUR. REV. PRIV. L. 827 (2024), https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\ERPL\ERPL2024043.pdf [https://perma.cc/8PWD-NHQ7].

129. DiPaola & Calo, *supra* note 117.

130. Natali Helberger, Marijn Sax, Joanna Strycharz & Hans-Wolfgang Micklitz, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, 45 J. CONSUMER POL'Y 175 (2022).

131. Stipulated Order For Permanent Injunction and Civil Penalty Judgment, United States of America v. Epic Games, Inc., No. 5:22-CV-00518 (E.D.N.C. Feb. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1923203epicgamesfedctorder.pdf [https://perma.cc/E4H5-CVKB] [hereinafter Stipulated Order, Epic Games, Inc.]; Lesley Fair, *$245 Million FTC Settlement Alleges Fortnite Owner Epic Games Used Digital Dark Patterns to Charge Players for Unwanted In-Game Purchases*, FED. TRADE COMM'N (Dec. 19, 2022)

certain in-game purchase disclosures, juxtaposed against consumers' material, financial losses as a result of Epic's UX decisions. Parents' complaints were featured heavily in discussing the exploitation of minors' decision-making in-game.[132] The Dutch Authority for Consumers and Markets similarly pursued Epic Games for the use of false countdown timers within Fortnite's in-game item shop.[133] Such actions partially rectify the wrongs delivered via dark patterns, with resultant designs eliminating some aspects of item timers, reducing tiering indicators, and accurately disclosing when time-limited items will disappear.[134]

Other digital service subfields, however, are increasingly under scrutiny for the manners in which their developers interfere with user experiences. Mobile health (mHealth) is one such field, with scholars concerned over technology companies' merging of health *and* commercial content into mHealth apps.[135] The nature of some subfields, such as physical or mental health, comparatively "raise the stakes" for how loyalty should be delivered given the inherent vulnerabilities—or potential for vulnerability—in these contexts.[136]

2. Layered Relationships and Secondary Responsibility

The complex nature of digital relationships makes the title of "user" a moving target; this is of particular concern to a loyalty approach as it raises questions about to *whom* loyalty should be given to. Richards and Hartzog tackle this but do so largely within the scope of conflicting loyalties between the end user of a platform and its shareholders. Citing Lina Khan and David Posen's concerns, Richards and Hartzog ultimately assert that "trusting, vulnerable people should take primacy over shareholders," a statement which still holds true with design.[137] But as demonstrated earlier in this Article, intermediary design firms that contribute to the at-scale

---

https://www.ftc.gov/business-guidance/blog/2022/12/245-million-ftc-settlement-alleges-fortnite-owner-epic-games-used-digital-dark-patterns-charge [https://perma.cc/4R94-TPNE].

132. Stipulated Order, Epic Games, Inc., *supra* note 131.

133. Saskia Bierling, *ACM Imposes Fine on Epic for Unfair Commercial Practices Aimed at Children in Fortnite Game*, AUTH. FOR CONSUMERS & MKTS. (May 14, 2024), https://www.acm.nl/en/publications/acm-imposes-fine-epic-unfair-commercial-practices-aimed-children-fortnite-game [https://perma.cc/D9MP-47QX].

134. We note, however, that while the Dutch ACM later examined Epic Games' compliance to the decision and stipulated order, Epic Games' own statement notes that these consumer-forward changes apply *only* to their Dutch population of gamers. This, we find, suggests minimal compliance and is not demonstrative of a true design loyalty perspective, which would, in theory, result in the universal (global) implementation of dark patterns removal after any single-state or single-region case. This highlights the patchwork nature of technology enforcement.

135. Marijn Sax, Natali Helberger & Nadine Bol, *Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices*, 41 J. CONSUMER POL'Y 103 (2018).

136. In this regard, and given dark patterns' recent close history with privacy scholarship, design loyalty approaches call for an expansion of rules like HIPAA (which famously does not cover many direct-to-consumer health or well-being technologies if they do not fall under "covered entities").

137. Richards & Hartzog, *supra* note 8, at 1015.

proliferation of dark patterns must also consider trusting, vulnerable people (second-party users of theirs) as taking at least equivalent importance as the first-party users that may subscribe to their service (e.g., the craftspeople from our prior example).

In some ways, this is basic economics. A craftsperson selling wares with Shopify will make no online sales if there is no market of consumers to demand that craftsperson's supply. Thus, loyal design vendors should empower and enable their first-party users to act loyally towards their own customers in turn. The tech landscape, particularly that for design, implicates not only the creatives but the architects and technologists who build underlying structures upon which digital aesthetics lie. This involves vendors at many layers, with the "user" being one of several vastly different stakeholders at a given stage. Take, for example, an independent craftsperson looking to sell products online; if woodworking is their craft, it's likely that web or mobile design is not their particular forté, thus it would be in their best interests to turn to vendors like Squarespace, Shopify, or Wix to build a digital shopfront. Through such software, the craftsperson may configure any combination of designs for their own "users:" the customers who visit their website and make purchases via digital medium. While this craftsperson shares some responsibility for selling their wares fairly and transparently, a duty of loyalty may put the onus on the scaled stakeholder (thus, the software as a service (SaaS) vendor) to best provide options to their selling-users such that these users can act accordingly.

Design loyalty not only mandates companies to refrain from deploying dark patterns but additionally holds design firms and SaaS vendors accountable, implicating their role in the spread of dark patterns and related designs. A loyalty approach to design additionally supports extant industry efforts to minimize the deployment of dark patterns, like value-sensitive design or otherwise ethical design techniques and frameworks.[138]

B. Pluralistic Approaches and N-Dimensionality

If atomistic approaches make for rules that technology companies find easy to dodge, then design loyalty (through loyalty approaches generally) may help mitigate against technical, but otherwise barely effective, compliance. As a categorically broad concept that still retains usable scope, loyalty considers the expanse of potential wrongdoing rather than requiring finer-grained subsets of harms. Mark Leiser explicitly argues for regulatory pluralism against dark patterns within the

138. Evan Caragay, Jonathan Zong, Katherine Xiong & Daniel Jackson, *Beyond Dark Patterns: A Concept-Based Framework for Ethical Software Design*, *in* CHI '24: PROCEEDINGS OF THE 2024 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING INTERACTION (2024), https://doi.org/10.1145/3613904.3642781 [https://perma.cc/RZ78-RFZ4].

European perspective,[139] and in a similar fashion, Lindsay Wilson articulates a pluralistic strengthening of consumer protection rulemaking in the United States.[140]

Privacy implicates many fields and disciplines, from the legal field for traditions in property torts, to computer science for architectural and security-oriented technologies, to sociology and political science for questions of state surveillance and its effects on citizens, and many more. Dark patterns as a design concept necessitates similar dimensionality, if not implicating additional fields like cognitive and behavioral sciences, psychology, art, front-end development, and multiple subfields in business. Privacy implicates design methods (as in the aptly-named Privacy-by-Design), but does not necessarily involve a user's first-hand, direct interaction with a digital service. UX design, however, does explicitly; the human element is an immediately necessary component for improving upon bad design in a way that is not as integral for privacy.

Intersecting human behavior at individual and group levels as well as technology systems and design writ large, dark patterns also conceptually necessitate multi-disciplinary approaches—"n-dimensional[ity]"—for dark patterns phenomena, urging for "holistic analysis" from a multitude of perspectives including psychology, law, design, and more.[141] As a result, design loyalty by nature must include and account for lessons and perspectives from non-STEM disciplines, especially if it is to be convincing to courts and lawmakers as a viable alternative to traditional material thresholds. Human-centered expertise from social science and humanities disciplines should feature heavily in the development of design loyalty rules, particularly to ensure that measurement methods are not built exclusively upon other fields that are a poor fit for non-material or secondary harms. Further, design loyalty requires the inclusion of practice-based (designer or otherwise) perspectives to ensure that scholarship's operational or feasibility blind spots are accounted for.[142]

1. The Scale Problem

Consider a company's incentives within the broader digital market; if disloyalty is not only the norm but the only way to survive, then it is in the best interest of a

---

139. M. R. Leiser, *Dark Patterns: The Case for Regulatory Pluralism Between the European Unions Consumer and Data Protection Regimes*, *in* RESEARCH HANDBOOK ON EU DATA PROTECTION LAW 240 (2022), https://www.elgaronline.com/edcollchap/edcoll/9781800371675/9781800371675.00019.xml [https://perma.cc/9NAZ-SCWT].

140. Wilson, *supra* note 122.

141. Gray et al., *supra* note 28, at 13.

142. Potel-Saville Marie & Fabien Lechevalier, *Comment les dark patterns manipulent nos usages mobiles? Proposition de régulation pour un digital durable et centré sur l'humain.* (*How Do Dark Patterns Manipulate Our Mobile Uses? Regulation Proposal for Sustainable and Human-Centered Digital.)*, *in* NOUVEAUX ENJEUX LIÉS AUX USAGES DES APPLICATIONS ET DES SERVICES MOBILES: QUELLES OPPORTUNITÉS ET QUELS RISQUES? [NEW CHALLENGES RELATED TO THE USE OF MOBILE APPLICATIONS: WHAT OPPORTUNITIES AND WHAT RISKS?], AFCAS SYMPOSIUM (2023) (Fr.). Some consulting firms or related agencies have actively sought to bridge the gap between critical scholarship, regulators, and technology companies (practice) to call for sustainable regulation and designs that take human-behavior limitations into account.

given technology corporation to act as disloyally, if not more, than its competitors if it wants a piece of the market's pie. To some extent, this is the digital landscape we presently operate in; corporations are beholden to stakeholders who may see user data as a product to be mined and leveraged towards future purchases from those very same users. To satisfy their stakeholders, technology corporations must secure their share of the "eyeballs" and design accordingly—they vie for continued engagement, never-ending subscriptions, and ever-increasing amounts of trackable data. This results in a digital experience where a single cookie banner dark pattern is easy for a user to manage, but a minutes-long browsing session scales the impact of anti-consumer designs with the number of apps or websites visited (and secondarily further scales up the third parties a user might be exposed to if selecting the option preferred by a dark pattern design).

If one single instance of a dark pattern constitutes negligible and *de minimis* harm, then a loyalty framing for the design of digital technologies accounts for harm at-scale—whether that scale is per-session, no matter how short, or across a person's entire digital life. Design loyalty discourages a race to the bottom of netizens' data pockets, and instead encourages practices that reduce the scaling effect on resultant harm.

2. Individual Harms and Beyond: Collective Welfare

One motivation for the flexibility afforded by design loyalty involves the subjective nature of design, aesthetics, and individual perceptions of a central interface. When presented with a dark pattern design, it is highly possible that a given individual may not recognize a harm, or may prefer a dark pattern design despite their own interests, or may dismiss a grievance based on size. How a person may feel about a design is influenced by their cultural background, societal norms, personal preference, and myriad other aspects of regular human living. An individual may be more irritated by the same dark pattern one minute than the next. Participant studies showing that users often dislike dark patterns also reveal that many are unaware of them—or conversely, that users still perceive manipulation even if they have awareness.[143] Similarly, what a "reasonable person" may find acceptable in one context may be less acceptable in another, whether or not the context is digital or offline.

This returns the field of dark patterns to the question of "[w]hat [m]akes a [d]ark [p]attern . . . [d]ark?," which Mathur et al. tackle in a taxonomy considerate of the various potential harms dark patterns can cause.[144] As loyalty is less concerned by which specific types of harms are possible rather than the avoidance of harm overall, design loyalty does not require granular measurements to satisfy severity thresholds—making for a more flexible approach than the requirements in present unfairness tests, for example.

---

143. Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig & Gabriele Lenzini, *"I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" - Dark Patterns from the End-User Perspective*, *in* DIS '21: PROCEEDINGS OF THE 2021 ACM DESIGNING INTERACTIVE SYSTEMS CONFERENCE 763 (2021), https://dl.acm.org/doi/10.1145/3461778.3462086 [https://perma.cc/B48X-E22J].

144. Mathur et al., *supra* note 108.

Design loyalty helps reduce harms exacerbated by scale at an individual but temporal level; it similarly facilitates improvements to collective welfare across groups of users. This accounts for harms that cannot be felt individually but have outsized impact societally, like surveillant or over-collective designs that induce chilling effects, or anti-competitive designs that force users to incur opportunity and switching costs in a market that should be more fair to them. Such aggregate harms are considered in Mathur et al.'s dark patterns harm taxonomy.[145] In particular, loyalty bridges subfield-specific definitions of fairness under one umbrella, allowing for designs that prevent imbalances across a user population.

Fabiana Di Porto and Alexander Egberts[146] write about the skew towards individual welfare approaches in extant dark patterns regulation and highlight efforts to address collective welfare harms like the American Innovation and Choice Online Act (AICO),[147] the aforementioned DETOUR Act, the DMA, and the DSA. Di Porto and Egberts describe these efforts (which vary in the extent to which they achieve collective welfare goals) as supportive of risk-based approaches for dark patterns enforcement as well as guidance for selecting which contexts or scopes should be tackled first.[148]

3. "Digital" Beyond Data and Privacy

Richards and Hartzog[149] present a thorough argument for duties of loyalty with regard to privacy and data protections, particularly in the effort to combat increasingly surveillant technologies and overcollection of consumer data. In many ways, their thesis encompasses much of what design loyalty is intended to. However, we have demonstrated that privacy mechanisms only go so far in the regulation of dark patterns. And while dark patterns certainly implicate people's privacy, the risks of manipulative and deceptive designs touch other areas involving commerce, employment, our social lives, our mental wellbeing, democratic institutions, and the health of the public sphere.

Loyalty for privacy and data purposes may have front-end impact, but a design loyalty that demands more of the frontline experience for users works in the opposite direction: It lets front-end ethics and protections dictate back-end practices all the way to boardroom decisions instead of working from privacy architectures towards the resultant interfaces.

As such, design loyalty is a *complement* to a duty of loyalty in privacy contexts; if privacy is a "vertical" slice of the digital regulations space, then design is a "horizontal" slice that deals with the interfaces directly provided to end users to experience. Design loyalty also complements proposed regulation resulting from increasing concerns over artificial intelligence and large language models; in expanding regulatory concepts beyond specific designs in narrow contexts, design loyalty questions how digital experiences are built and how they are felt and utilized by netizens worldwide.

---

145. *Id.*
146. Di Porto & Egberts, *supra* note 107.
147. American Innovation and Choice Online Act, S. 2992, 117th Cong. (2022).
148. Di Porto & Egberts, *supra* note 107.
149. Richards & Hartzog, *supra* note 8.

4. Approaches Grounded in Design and Practice

If the law is concerned with determining reasonable expectations, then design practice offers a few tools that the law could directly borrow to determine when user expectations are subverted. In fact, the 2024 Gray et al. dark patterns ontology[150] frames "meso-level" dark patterns by the manners in which a design subverts user expectations. We turn to the vocabulary provided by the design and human-computer interaction fields. Design and human-computer interaction disciplines fundamentally understand and handle "affordances," described by usability engineer Donald Norman as:

> [T]he perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used. . . . Affordances provide strong clues to the operations of things. Plates are for pushing. Knobs are for turning. Slots are for inserting things into. Balls are for throwing or bouncing. When affordances are taken advantage of, the user knows what to do just by looking: no picture, label, or instruction is required.[151]

In short, affordances articulate what a design is intended to do and the extent to which a consumer or user understands how to use the design. Affordances are thus the design equivalent of a platform or service's representations to the user: representations from which a user derives their expectations of how to interact with an interface.

Design loyalty does not require that every single design be laden with transparent disclosures *accessible to the end user,* as users may have competing desires for a given design and may in fact prefer simplicity over full transparency in one situation and the opposite in another. Rather, loyalty requires that the platform or service carefully and thoughtfully consider their designs' affordances with (minimally) internal documentation to demonstrate a best effort at serving users' best interests for a given design within a given context. However, what those best interests are may differ from design to design or context to context. How, then, should a company's loyalty be determined?

Preemptive consideration of desired affordances and outcomes features commonly in design planning exercises, with tools like user stories, speculative enactments,[152] and more to help ensure that a design will be useful before it is built. What constitutes a "good" design depends on what the intended purpose is and how effectively a design achieves that purpose. Good design practices, however, can be used for ethical design or for profit-oriented design. Loyalty simply asks that relational ethics be explicitly accounted for during the design process.

In scholarship, computer scientists working on HCI, UX, and design topics often provide implications or suggestions for practitioners, with work increasingly focused on operationalizing ethical UX. Caragay et al. provide a conceptual framework that

---

150. Gray et al., *supra* note 20.

151. DONALD A. NORMAN, THE DESIGN OF EVERYDAY THINGS 9 (Doubleday 1990) (1988).

152. Lei Nelissen & Mathias Funk, *Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments*, 16 INT'L J. DESIGN 75 (2022).

may help implement design loyalty in practice: They present a method for determining what *to* do instead of what *not* to do with regard to dark patterns.[153] A concept of design loyalty empowers design teams who wish to incorporate more trust and loyalty into their practice. This is of special importance for frustrated practitioners who have raised objections to design decisions with upper management, only to have their suggestions brushed aside and ignored. Such behavior is not simply anecdotal; FTC dark pattern case documents reveal that practitioners do identify and document anti-consumer designs—and that other team members or higher-ups disregard practitioner concerns in favor of chasing other corporate incentives.[154] Participant studies affirm findings from enforcement cases, finding that practitioners "use existing laws and regulations as facts and evidence to push back against certain design requests and increase ethical awareness among stakeholders."[155]

Note also that loyalty is not a foreign concept to technology organizations, particularly with regard to their market perception. "Brand loyalty" is highly sought-after, with design and marketing thought leadership from industry outlining principles and best practices that (if followed) should raise a user's opinion of a company. Unlike loyalty for privacy or data protections, design loyalty more naturally ties into brand loyalty, insofar as the user experience and related designs communicate platforms' brand identities to the end user. By seeking brand loyalty, platforms engage with and understand the necessity of relationship building with their users, so the language of design loyalty may conceptually appeal to platforms' decision-makers. This could reduce opposing tensions in the field (like those between platforms vs. critics of dark patterns) and encourage cooperation (constructive critics helping platforms retain users rather than anger them).[156]

In a similar systemic vein, Mark Leiser and Cristiana Santos discuss not only front-end, interface designs but less-visible designs, for example, the design of the underlying systems beneath an interface.[157]

---

153. Caragay et al., *supra* note 138.

154. Complaint, Epic Games, Inc., F.T.C. 192-3203 (Dec. 19, 2022) (No. C-4790); Decision and Order, Epic Games, Inc., F.T.C. 192-3203 (Mar. 13, 2023) (No. C-4790).

155. Leah Zhang-Kennedy, Maxwell Keleher & Michaela Valiquette, *Navigating the Gray: Design Practitioners' Perceptions Toward the Implementation of Privacy Dark Patterns*, 8 PROC. ACM HUM.-COMP. INTERACTION 97:1, 97:17 (2024).

156. Groups like Amurabi frame the dark patterns problem in less accusatory manners to encourage platform compliance; as a "legal design agency," Amurabi's staff helps companies comply with ever-changing regulation—while explicitly mentioning the "fight against dark patterns" as part of their portfolio of offerings to potential clients. *Fight Against The Dark Patterns*, AMURABI, https://amurabi.eu/en/lutte-contre-les-dark-patterns/ [https://perma.cc/6SDD-GYLY]. This approach may appeal to platforms' desires to either do right by their users or at least be *seen* as doing so. Such organizations, which bridge legal practice and design practice, can help often siloed intraorganizational teams work more closely together toward the betterment of the resultant digital experience overall.

157. Mark Leiser & Cristiana Santos, *Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation Beneath the Interface*, 15 EUR. J.L. & TECH. 1 (2024).

CONCLUSION

Loyalty, in its effort to avoid wrongful self-dealing and the creation of power imbalances in platform-user relationships, provides a centralizing framing for dark patterns across extant and future regulation, diverse UX contexts, layers of design spanning front-end to systems, and of course the vast range of dark pattern types. We offer "disloyal patterns" as an alternative conceptual term for its moral and operational meanings while bridging legal and consumer or practitioner perspectives.

This Article presents the loyalty framing for dark patterns as a provocation for future lines of research as well as for clearer rules and more robust enforcement going forward. Specifically, loyalty grounds dark patterns and related design behaviors in relationships, then not only facilitates but encourages pluralistic approaches to combating dark patterns.