

Design Loyalty Approaches for Dark Patterns

Johanna Gunawan*, David Choffnes*, Woodrow Hartzog†, Christo Wilson*

**Khoury College of Computer Sciences*

Northeastern University, Boston, Massachusetts

gunawan.jo@northeastern.edu, choffnes@ccs.neu.edu, cbw@ccs.neu.edu

† *School of Law*

Boston University, Boston, Massachusetts, USA

whartzog@bu.edu

Abstract—

Lawmakers worldwide [1]–[7] have taken notice of “dark patterns:” design practices that “[deceive, manipulate, or otherwise distort with technology users’ ability to make informed decisions].” [2] HCI scholarship has revealed dark patterns’ pervasiveness [8], [9] in ubiquitous [10]–[16] and emergent technologies [17], users’ opinions of dark patterns [10], [11], [18]–[20], and dark patterns in contexts like consent and privacy [19]–[27]. Critics, however, allege that the term (in law) is overbroad, impractical, and counterproductive insofar as it applies to normative, “omnipresent” design practices [28].

Established legal frameworks prohibit wrongful self-dealing in fields like finance (e.g., fiduciary duty) and medicine (e.g., “do no harm”). Scholars suggesting similar frameworks for privacy and technology like a “duty of loyalty for privacy law, [29]” in which platforms should act in the best privacy interests of end users. *In this research proposal we explore a loyalty framework for dark patterns and design from interdisciplinary CS and law perspectives.*

1. Motivation

Inter- and Cross-disciplinary Dark Patterns Scholarship. In both computer science and law disciplines, scholars discuss implications of their field’s findings for the other’s use [30], [31]. A growing body of collaborative scholarship across these disciplines explore dark patterns in accordance to extant regulations like the GDPR [22], as well as potential avenues for regulating dark patterns in practice [32], [33].

Asymptotes for Harms Approaches. Though prior taxonomies have robustly considered dark patterns harms [31] and design values [8], the question of how to best measure dark patterns harms remains unanswered. The law often requires proof and/or severity thresholds of harm in order to remedy issues, but dark patterns need not result in unavoidable or proven harms to be risky or problematic user designs. What should be done about disadvantageous designs, or designs that may cause harm in aggregate but individually present as harmless or *de minimus* (or otherwise below-threshold) harms? Harms

This research was supported in part by NSF grants (#1955227 and #CNS-1900879).

approaches to dark patterns may only go so far, so we then turn to consumer-protective theories that rely less heavily on them.

Borrowing from Privacy Studies (and Other Legal Subfields). Dark patterns scholarship has often focused on privacy [19]–[23], [26], and new global privacy regulations [3], [4], [34], [35] (which include guidelines for technology and data practices writ large) have rapidly emerged in the past decade. From this momentum, privacy provides an case study by which to expand consumer protections overall.

We focus on a duty of loyalty for privacy law [29] as initial motivation for this work. Duties of care and loyalty are essentially end-user protections, for specific subgroups of users. Thus we are interested in understanding why other subfields follow loyalty principles closely and why privacy or technology have yet to adopt them. Next, if loyalty minimizes harms and maximizes benefits, privacy offers other inspiration through data minimization. Prior work [13] suggests “design appropriateness” (inspired by data minimization, and meant to minimize “nagging” or redundant designs that may detract from UX quality) to reduce dark patterns in user interfaces.

2. Towards Design Loyalty and Appropriateness: Provocations

We intend to explore the operability of a duty of loyalty (and design appropriateness) for user experiences and thus dark patterns. Specifically, we ask the following questions:

- Is design loyalty potentially feasible as a consumer protection measure against dark patterns and related UX issues? Why or why not, and what evidence suggests feasibility or lack thereof?
- Are there unique traits in digital consumer protections or design (as compared to fields traditionally employing care and loyalty duties, like medicine and finance) that impact design loyalty implementations?
- If harm is centralizing factor for duties of care and loyalty in other disciplines, what makes harms approaches more difficult for digital experiences?

- To what extent does industry self-governed ethical or value-sensitive UX achieve the goals of design loyalty? What operational or technical mechanisms might a legal approach to design loyalty help mandate?
- Can designs be effectively “minimized” in a similar manner to data minimization? What consequences would such an approach lead to?

Answering such questions, we believe, requires stakeholders from both quantitative and qualitative CS scholarship, as well as from law and other disciplines. Thus we present the concept of design loyalty as a provocation to the ConPro’24 community in the hopes of fostering discussion and future work.

References

- [1] K. F. T. Commission, *Guidelines on online dark pattern self-regulation*, 2023. [Online]. Available: https://www.ftc.go.kr/www/selectReportUserView.do?key=10%5C&rpptype=1%5C&report%5C_data%5C_no=10140.
- [2] R. of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act), *Com(2020) 825 final*, 2022.
- [3] *California consumer privacy act of 2018 (ccpa)*, 2018. [Online]. Available: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.%5C&part=4.%5C&lawCode=CIV%5C&title=1.81.5.
- [4] *California privacy rights act of 2020 (cpra)*, 2020.
- [5] OECD, “Dark commercial patterns,” Tech. Rep., Oct. 2022. DOI: 10.1787/44f5e846-en. [Online]. Available: <https://www.oecd-ilibrary.org/content/paper/44f5e846-en>.
- [6] “Bringing dark patterns to light staff report,” Federal Trade Commission, Tech. Rep., Sep. 2022. [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%5C%20Dark%5C%20Patterns%5C%20Report%5C%209.14.2022%5C%20-%5C%20FINAL.pdf.
- [7] “Evidence review of online choice architecture and consumer and competition harm,” en, Tech. Rep., 2022, Accessed: 2022-4-13. [Online]. Available: <https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm>.
- [8] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, “The Dark (Patterns) Side of UX Design,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’18, Montreal QC, Canada: dl.acm.org, 2018, 534:1–534:14, ISBN: 9781450356206. DOI: 10.1145/3173574.3174108. [Online]. Available: <http://doi.acm.org/10.1145/3173574.3174108>.
- [9] C. M. Gray, C. Santos, and N. Bielova, “Towards a preliminary ontology of dark patterns knowledge,” in *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA ’23)*, 2023. DOI: 10.1145/3544549.3585676. [Online]. Available: <http://dx.doi.org/10.1145/3544549.3585676>.
- [10] J. Luguri and L. J. Strahilevitz, “Shining a light on dark patterns,” en, *Journal of Legal Analysis*, vol. 13, no. 1, pp. 43–109, Mar. 2021, ISSN: 2161-7201, 1946-5319. DOI: 10.1093/jla/laaa006. [Online]. Available: <https://academic.oup.com/jla/article/13/1/43/6180579>.
- [11] T. Mildner and G.-L. Savino, “Ethical user interfaces: Exploring the effects of dark patterns on facebook,” in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA ’21, Yokohama, Japan: Association for Computing Machinery, May 2021, pp. 1–7, ISBN: 9781450380959. DOI: 10.1145/3411763.3451659. [Online]. Available: <https://doi.org/10.1145/3411763.3451659>.
- [12] A. Mathur, G. Acar, M. J. Friedman, et al., “Dark patterns at scale: Findings from a crawl of 11K shopping websites,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, Article No. 81, Nov. 2019. DOI: 10.1145/3359183. [Online]. Available: <http://dl.acm.org/citation.cfm?doid=3371885.3359183>.
- [13] M. Kowalczyk, J. T. Gunawan, D. Choffnes, D. J. Dubois, W. Hartzog, and C. Wilson, “Understanding dark patterns in home IoT devices,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’23, Hamburg, Germany: Association for Computing Machinery, Apr. 2023, pp. 1–27, ISBN: 9781450394215. DOI: 10.1145/3544548.3581432. [Online]. Available: <https://doi.org/10.1145/3544548.3581432>.
- [14] L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, and A. Bacchelli, “UI dark patterns and where to find them: A study on mobile applications and user perception,” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’20, Honolulu, HI, USA: Association for Computing Machinery, Apr. 2020, pp. 1–14, ISBN: 9781450367080. DOI: 10.1145/3313831.3376600. [Online]. Available: <https://doi.org/10.1145/3313831.3376600>.
- [15] S. Hidaka, S. Kobuki, M. Watanabe, and K. Seaborn, “Linguistic dead-ends and alphabet soup: Finding dark patterns in japanese apps,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’23, New York, NY, USA: Association for Computing Machinery, 2023, ISBN: 9781450394215. DOI: 10.1145/3544548.3580942. [Online]. Available: <https://doi.org/10.1145/3544548.3580942>.

- [16] A. Chaudhary, J. Saroha, K. Monteiro, A. G. Forbes, and A. Parnami, ““are you still watching?”: Exploring unintended user behaviors and dark patterns on video streaming platforms,” in *Designing Interactive Systems Conference*, ser. DIS ’22, Virtual Event, Australia: Association for Computing Machinery, Jun. 2022, pp. 776–791, ISBN: 9781450393584. DOI: 10.1145/3532106.3533562. [Online]. Available: <https://doi.org/10.1145/3532106.3533562>.
- [17] K. Owens, J. Gunawan, D. Choffnes, P. Emami-Naeini, T. Kohno, and F. Roesner, “Exploring deceptive design patterns in voice interfaces,” in *Proceedings of the 2022 European Symposium on Usable Security*, ser. EuroUSEC ’22, New York, NY, USA: Association for Computing Machinery, 2022, pp. 64–78, ISBN: 9781450397001. DOI: 10.1145/3549015.3554213. [Online]. Available: <https://doi.org/10.1145/3549015.3554213>.
- [18] K. Bongard-Blanchy, A. Rossi, S. Rivas, S. Doublet, V. Koenig, and G. Lenzini, ““i am definitely manipulated, even when I am aware of it. it’s ridiculous!” - dark patterns from the End-User perspective,” in *Designing Interactive Systems Conference 2021*, ser. DIS ’21, vol. 1, Virtual Event, USA: Association for Computing Machinery, Jun. 2021, pp. 763–776, ISBN: 9781450384766. DOI: 10.1145/3461778.3462086. [Online]. Available: <https://doi.org/10.1145/3461778.3462086>.
- [19] I. Borberg, R. Hougaard, W. Rafnsson, and O. Kulyk, ““so I sold my soul”: Effects of dark patterns in cookie notices on End-User behavior and perceptions,” in *Usable Security and Privacy (USEC) Symposium 2022*, 2022. DOI: 10.14722/usec.2022.23026. [Online]. Available: <http://dx.doi.org/10.14722/usec.2022.23026>.
- [20] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, “Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence,” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’20, Honolulu, HI, USA: Association for Computing Machinery, Apr. 2020, pp. 1–13, ISBN: 9781450367080. DOI: 10.1145/3313831.3376321. [Online]. Available: <https://doi.org/10.1145/3313831.3376321>.
- [21] B. Schaffner, N. A. Lingareddy, and M. Chetty, “Understanding account deletion and relevant dark patterns on social media,” *Proc. ACM Hum.-Comput. Interact.*, vol. 6, no. CSCW2, Nov. 2022. DOI: 10.1145/3555142. [Online]. Available: <https://doi.org/10.1145/3555142>.
- [22] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, “Dark patterns and the legal requirements of consent banners: An interaction criticism perspective,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI’21, ACM Press, May 2021. DOI: 10.1145/3411764.3445779.
- [23] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfatthicher, “Tales from the dark side: Privacy dark strategies and privacy dark patterns,” *Proc. of PETS*, vol. 2016, no. 4, pp. 237–254, 2016. [Online]. Available: <https://content.sciendo.com/view/journals/popets/2016/4/article-p237.xml>.
- [24] D. Machuletz and R. Böhme, “Multiple purposes, multiple problems: A user study of consent dialogs after GDPR,” in *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 481–498, 2020. DOI: 10.2478/popets-2020-0037. [Online]. Available: <https://content.sciendo.com/view/journals/popets/2020/2/article-p481.xml>.
- [25] C. Bermejo Fernandez, D. Chatzopoulos, D. Papadopoulos, and P. Hui, “This website uses nudging: Mturk workers’ behaviour on cookie consent notices,” *Proc. ACM Hum.-Comput. Interact.*, vol. 5, no. CSCW2, Oct. 2021. DOI: 10.1145/3476087. [Online]. Available: <https://doi.org/10.1145/3476087>.
- [26] H. Habib, M. Li, E. Young, and L. Cranor, ““okay, whatever”: An evaluation of cookie consent interfaces,” in *CHI Conference on Human Factors in Computing Systems*, ser. CHI ’22, New Orleans, LA, USA: Association for Computing Machinery, Apr. 2022, pp. 1–27, ISBN: 9781450391573. DOI: 10.1145/3491102.3501985. [Online]. Available: <https://doi.org/10.1145/3491102.3501985>.
- [27] C. Santos, C. M. Gray, and N. Bielova, *Usable and accessible GDPR consent: Is it possible?* Privacy Law Scholars Conference (PLSC), Boston, MA, Jun. 2022.
- [28] D. Luque, *Examining the ftc’s hostility to common design practices*, 2023. [Online]. Available: <https://www.project-disco.org/competition/examining-the-ftcs-hostility-to-common-design-practices/>.
- [29] “A duty of loyalty for privacy law,” *Washington University Law Review*, vol. 99, 961 2021. [Online]. Available: <https://ssrn.com/abstract=3642217>.
- [30] A. Hung, “Addressing “nagging” concerns and injury,” *Columbia law review*, vol. 121, no. 8, pp. 2483–2520, 2021, ISSN: 0010-1958, 1945-2268. [Online]. Available: <https://www.jstor.org/stable/27093855>.
- [31] A. Mathur, M. Kshirsagar, and J. Mayer, “What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, May 2021, pp. 1–18, ISBN: 9781450380966. DOI: 10.1145/3411764.3445610. [Online]. Available: <https://doi.org/10.1145/3411764.3445610>.
- [32] J. King and A. Stephan, “Regulating privacy dark patterns in practice—drawing inspiration from california privacy rights act,” *Georgetown Law Technology Review*, vol. 5, 250.
- [33] J. Gunawan, C. Santos, and I. Kamara, “Redress for dark patterns privacy harms? a case study on consent interactions,” in *Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW ’22)*, 2022.

DOI: 10.1145/3511265.3550448. [Online]. Available:
<http://dx.doi.org/10.1145/3511265.3550448>.

- [34] *Colorado privacy act*, Jul. 2021. [Online]. Available:
https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.
- [35] E. Parliament and C. of European Union, *Eu general data protection regulation (gdpr)*, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>, Apr. 2016.