Dark Pattern Typology: How Do Social Networking Sites Deter Disabling of User Accounts?

Dominique Kelly and Victoria L. Rubin

June 21, 2022

Dark Pattern Typology: How Do Social Networking Sites Deter Disabling of User Accounts?

Dominique Kelly and **Victoria L. Rubin**
Western University, London, Ontario, Canada
dkelly48@uwo.ca, vrubin@uwo.ca

Background

Dark patterns are user interface (UI) strategies deliberately designed to influence users to perform actions or make choices that benefit online service providers. Often, dark patterns operate by exploiting users' decision-making vulnerabilities such as cognitive biases (Bösch et al., 2016; Mathur et al., 2019; Waldman, 2020). Users may be encouraged to purchase unneeded goods or disclose their personal information (Luguri & Strahilevitz, 2021; Narayanan et al., 2020).

Scholarly interest in dark patterns has grown rapidly in recent years. Building on seminal work completed by user experience (UX) practitioner Harry Brignull, Gray et al. (2018) presented five general categories of manipulative UI design: Nagging, Obstruction, Sneaking, Interface Interference, and Forced Action. Researchers have also identified dark patterns that arise in specific contexts such as video games (Lewis, 2014; Zagal et al., 2013), shopping websites (Mathur et al., 2019), proxemic interactions (Greenberg et al., 2014), home robots (Lacey & Caudwell, 2019), and online privacy choices (Bösch et al., 2016; Commission Nationale de l'Informatique et des Libertés, 2019; Forbrukerrådet, 2018; Fritsch, 2017).

Studies have recognized that online service providers may deliberately frustrate users' attempts to withdraw from their services by, for example, deterring the user from disabling their account (Bösch et al., 2016; Gray et al., 2018). However, there is a lack of research that examines the specific UI strategies employed by online service providers to deter disabling of user accounts. Furthermore, little research has focused on identifying and describing dark patterns in social networking sites (SNSs). In the context of SNSs, potential motivations to withdraw from a service include privacy and security concerns, addiction, and the perception that one's time could be invested in more value-adding or productive activities (Baumer et al., 2013; Grandhi et al., 2019).

Objectives

We identify dark patterns in the context of SNS users attempting to disable their accounts (i.e., delete or deactivate the service), consolidate these tactics into a typology, and assess their prevalence in our sample. We use our findings to propose recommendations for the design of user-friendly account disabling UIs that aid – rather than undermine – the user in their effort to withdraw from social media.

Method

For the above objectives, we systematically collected and content analyzed a dataset of recordings and associated email exchanges that captured our account disabling processes for 26 sample SNSs, most highly ranked on Alexa's May 2020 Top Sites list and fitting our inclusion criteria. We considered *account disabling* to refer to any option that allowed the user to withdraw from the service; this encompasses permanent deletion as well as temporary deactivation of the user account. The *account disabling process* refers to the total steps that must be completed by the user to disable their account.

The first author conducted real-time recordings of her attempts to disable her temporary accounts on 26 SNSs. The recordings show the user's website login, navigation, and selection of the options deemed appropriate for the user's intent to discontinue subscribing to the service offered by each SNS. The recordings are uninterrupted and allow time for the user to make choices among available options (e.g., tabs, check boxes or radio buttons) and read various pop-up screens, notifications, or other legal terms presented to the user by the UI design. The first author also monitored her associated email account and screen-captured emails that were sent from sites after the user account had been disabled.

Manual coding of the recordings and emails was performed following basic steps in Klaus Krippendorff's (1980, 2004) Content Analysis methodology. The complete dataset was reviewed and coded (by the first author) for the presence of dark patterns during the user-SNS interaction. A timestamp and a dark pattern type and a subtype were recorded for each instance of the dark pattern, following our Dark Pattern Classification coding scheme.

The second author served as a secondary coder who reviewed seven (7) sites randomly selected out of 26 SNSs (27%). This verification step was intended to confirm the presence of the dark patterns and assess the intercoder consistency. Using the same Dark Pattern Classification coding scheme and agreed-upon codebook outlining the definitions and procedures, the second author identified and classified each instance.

Results

As a result of the systematic Content Analysis, we uncovered five major types of dark patterns (Complete Obstruction, Temporary Obstruction, Obfuscation, Inducements to Reconsider, and Consequences) and 13 subtypes. To develop the Dark Pattern Typology, we combined, modified, and extended the dark pattern models from earlier works by Brignull (n.d.), Conti and Sobiesk (2010), and Gray et al. (2018). The major types of dark patterns are described below.

Complete Obstruction refers to making it impossible for the user to disable their account through the site's UI by excluding any option for account disabling.

Temporary Obstruction describes strategies that increase the user's workload during the account disabling process. This is accomplished by requiring the user to complete actions that should not be inherently necessary in order to proceed in the task flow. For example, the user could be forced to submit a request for account disabling, either by filling out an online form or by communicating with a company representative in real time.

Obfuscation refers to strategies that confuse or mislead the user prior to or during the account disabling process. This is achieved by obscuring information and/or options that would allow the user to initiate or advance in the task flow. The service provider might make buttons that allow the user to keep their account active visually salient, while hiding buttons that allow the user to proceed toward account disabling.

Inducements to Reconsider are strategies that attempt to persuade the user to reconsider their decision to disable their account during the account disabling process. This is accomplished by using language, visuals, or incentives to present the option to stay on the site favourably. Typically, the service provider highlights benefits that the user will accrue if they keep their account active or emphasizes costs that the user will suffer if they disable their account. For example, the option to disable the account could be worded in such a way that it evokes guilt, fear, or doubt in the user.

Consequences are strategies that encourage the user to return to the site after their account has been disabled. Dark patterns of this type operate in two ways: by making it easy for the user to reverse their decision to disable their account, or by sending unsolicited messages to the user that promote activity on the site and/or attempt to persuade them to return. As an example, the user might retain the ability to reactivate their account through login indefinitely.

All of the 26 sampled SNSs were identified using at least one type of dark pattern. Most SNS UIs attempted to manipulate the user once or twice, for example, by providing an option for account reactivation, by emotional pressure/distraction, or by hiding the button to initiate account disabling. Five (5) out of 26 SNSs (19%) attempted to manipulate the user at least five or more times during their account disabling process.

Future Work

In this study, we confirmed the presence of dark patterns in the context of SNS users attempting to disable their accounts. The Dark Pattern Typology contributes to future work in: a) documenting the prevalence of dark patterns in SNSs; b) identifying dark patterns in the user account disabling process for a range of other online services; c) investigating users' perceptions and experiences of dark patterns; and, d) determining the effects of dark patterns on user behaviour. Further research could connect the dark patterns in our typology to the cognitive biases they exploit and the design attributes they exhibit, as exemplified by Mathur et al.'s (2019) study of shopping websites.

References

Baumer, E. P. S., Adams, P., Khovanskaya, V. D., Liao, T. C., Smith, M. E., Sosik, V. S., & Williams, K. (2013). Limiting, leaving, and (re)lapsing: An exploration of Facebook non-use practices and experiences. *CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3257-3266. https://doi.org/10.1145/2470654.2466446

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies, 2016*(4), 237-254. http://dx.doi.org/10.1515/popets-2016-0038

Brignull, H. (n.d.). Dark patterns. https://www.darkpatterns.org/

Commission Nationale de l'Informatique et des Libertés. (2019). *Shaping choices in the digital world.* https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

Conti, G., & Sobiesk, E. (2010). Malicious interface design: Exploiting the user. *WWW'10: Proceedings of the 19th international conference on World wide web*, 271-280. https://doi.org/10.1145/1772690.1772719

Forbrukerrådet. (2018). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Fritsch, L. (2017). Privacy dark patterns in identity management. In L. Fritsch, H. Roßnagel, & D. Hühnlein (Eds.), *Open Identity Summit 2017: Proceedings* (pp. 93-104). Gesellschaft für Informatik.

Grandhi, S. A., Plotnick, L., & Hiltz, S. R. (2019). Do I stay or do I go? Motivations and decision making in social media non-use and reversion. *Proceedings of the ACM on Human-Computer Interaction, 3*, 1-27. https://doi.org/10.1145/3361116

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-14. https://doi.org/10.1145/3173574.3174108

Greenberg, S., Boring, S., Vermeulen, J., & Dostal, J. (2014). Dark patterns in proxemic interactions: A critical perspective. *DIS '14: Proceedings of the 2014 Conference on Designing Interactive Systems*, 523-532. http://dx.doi.org/10.1145/2598510.2598541

Krippendorff, K. (1980). Validity in content analysis. In E. Mochmann (Ed.), *Computerstrategien Für Die Kommunikationsanalyse* (pp. 69-112). Campus.

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology* (2nd ed.). Sage Publications, Inc.

Lacey, C., & Caudwell, C. (2019). Cuteness as a 'dark pattern' in home robots. *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI*), 374-381. https://doi.org/10.1109/HRI.2019.8673274

Lewis, C. (2014). *Irresistible apps: Motivational design patterns for apps, games, and web-based communities*. Apress.

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis, 13*(1), 43-109. https://doi.org/10.1093/jla/laaa006

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM Human-Computer Interaction*, *3*, 1-32. https://doi.org/10.1145/3359183

Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: Past, present, and future. *Communications of the ACM, 63*(9), 42-47. https://doi.org/10.1145/3397884

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox.' *Current Opinion in Psychology, 31*, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

Zagal, J. P., Björk, S., & Lewis, C. (2013). Dark patterns in the design of games. *Proceedings of the 18th International Conference on the Foundations of Digital Games (FDG 2013),* 39-46. http://www.fdg2013.org/program/papers/paper06_zagal_etal.pdf