DARK PATTERN TYPOLOGY: HOW DO SOCIAL NETWORKING SITES DETER DISABLING OF USER ACCOUNTS?

Dominique Kelly and Victoria L. Rubin

Faculty of Information & Media Studies, Western University

LITERATURE REVIEW: DEFINING DARK PATTERNS

- Dark patterns are user interface (UI) strategies deliberately designed to influence users to perform actions or make choices that benefit online service providers

- They typically exploit decision-making vulnerabilities like 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)

LITERATURE REVIEW: TYPES OF DARK PATTERNS

- **General contexts** (Brignull, n.d.; Gray et al., 2018)

- **Specific contexts**
  - **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)
  - **Online privacy choices** (Bösch et al., 2016; Commission Nationale de l'Informatique et des Libertés, 2019; Forbrukerrådet, 2018; Fritsch, 2017)

LITERATURE REVIEW: RESEARCH GAPS

- Studies have recognized that online service providers may deliberately frustrate users' attempts to disable their accounts (Bösch et al., 2016; Gray et al., 2018); however, there is a lack of research that examines the specific UI strategies employed for this purpose

- Little research has focused on identifying and describing dark patterns in social networking sites (SNSs)

STUDY OBJECTIVES

1. Identify dark patterns in the context of SNS users attempting to disable their accounts

2. Consolidate these tactics into a typology

3. Assess their prevalence in our sample

METHODS

- **Overview of methods**
  - We collected and content analyzed a dataset of recordings and associated email exchanges that captured our account disabling process for 26 sample SNSs

- **Sample selection**
  - The sample SNSs were those most highly ranked on Alexa's May 2020 Top Sites list that fit our inclusion criteria

METHODS

- **Data collection**
  - The first author conducted real-time recordings of her attempts to disable temporary accounts on 26 SNSs and screen-captured emails that were sent from sites after the user account had been disabled

- **Data analysis**
  - The first author manually coded the complete dataset for the presence of dark patterns

Proposed Dark Pattern Typology by Kelly and Rubin (2022), which combines, modifies, and extends earlier models by Brignull (n.d.), Conti and Sobiesk (2010), and Gray et al. (2018)
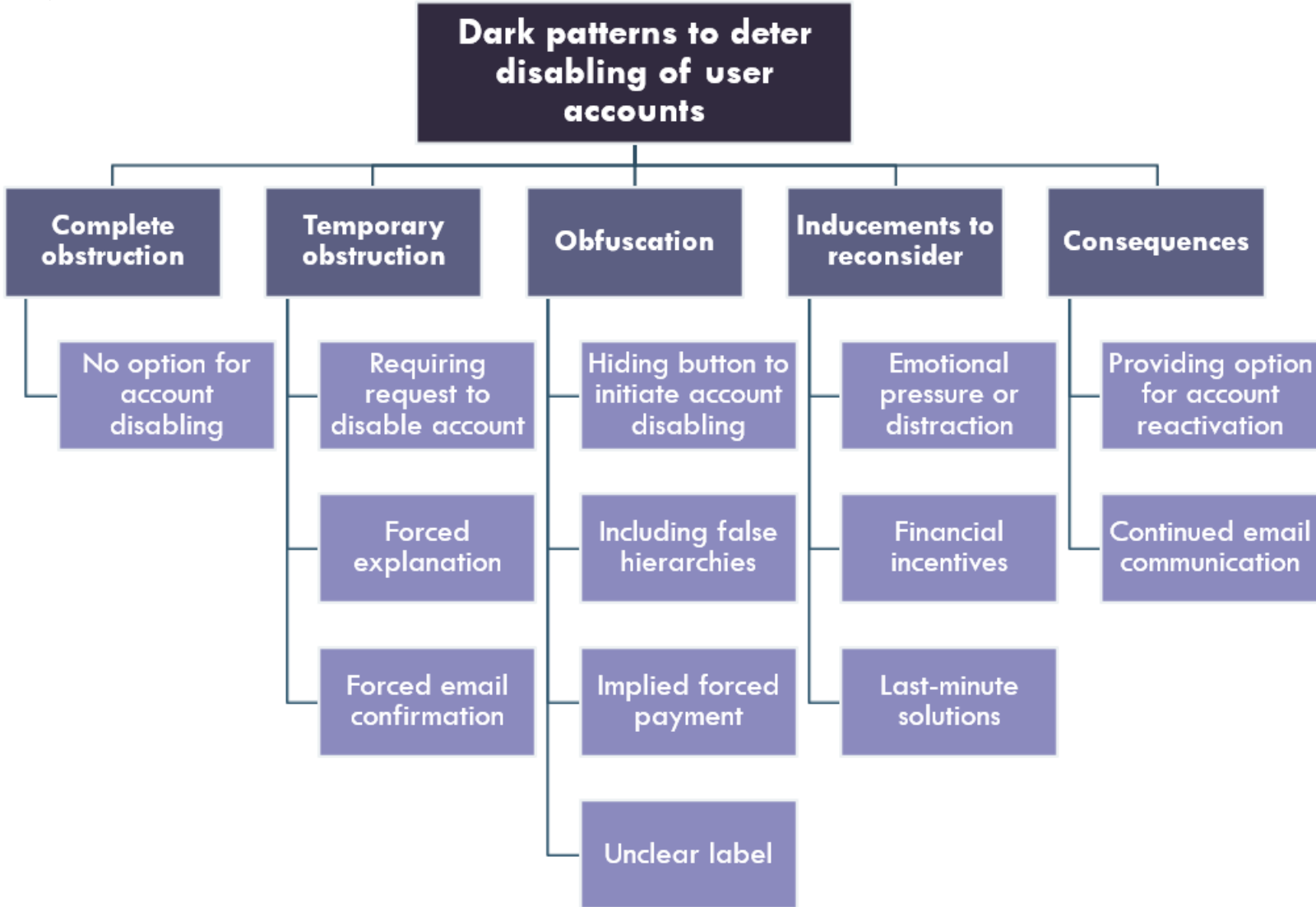
TYPE 1: COMPLETE OBSTRUCTION

- **Definition:** Making it impossible for the user to disable their account through the site's UI; excluding any option for account disabling

TYPE 1: COMPLETE OBSTRUCTION

Don't create threads announcing that you are leaving. Just leave.

Don't ask us to delete your account or posts. We won't. That would make it too easy for you to return as a different user.
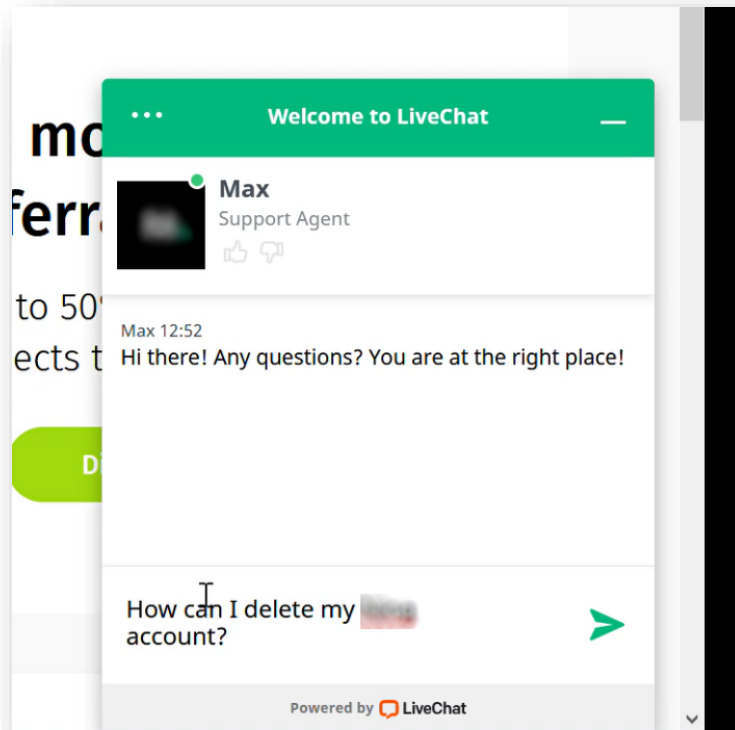
Don't create threads to discuss the banning of a particular member.

Example from dataset

TYPE 2: TEMPORARY OBSTRUCTION

- **Definition:** Increasing the user's workload; requiring the completion of actions that should not be inherently necessary to proceed in the task flow
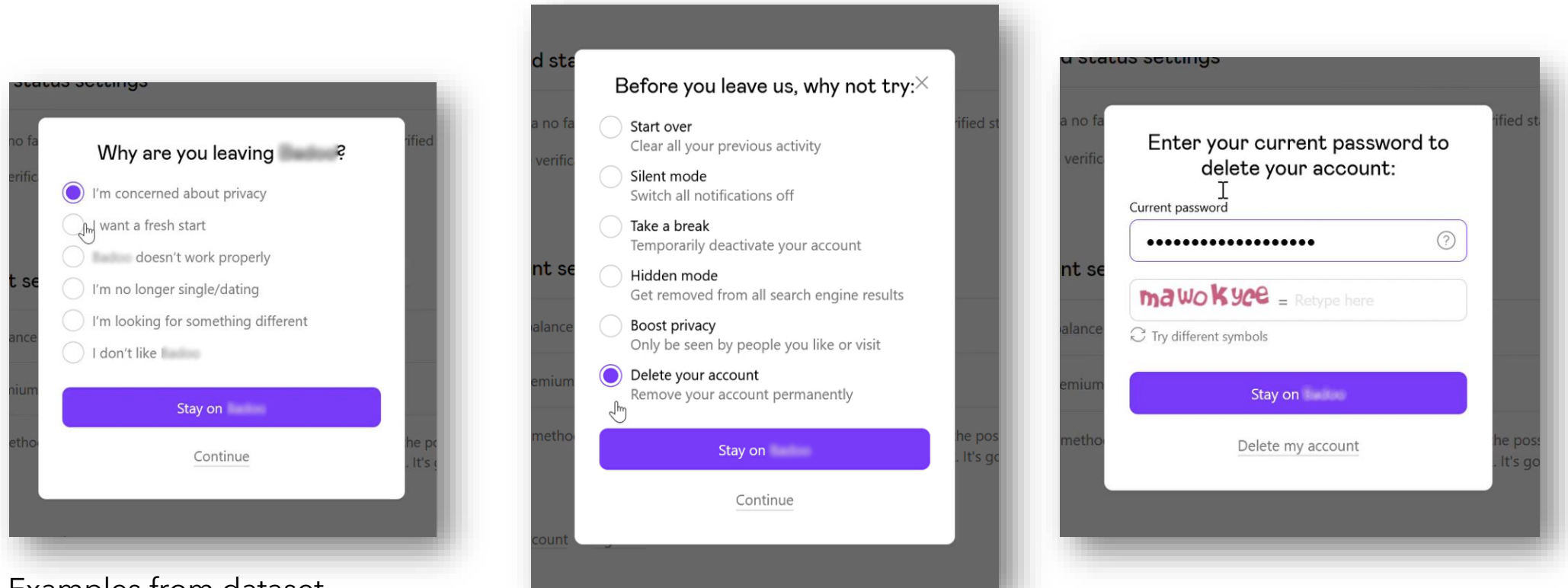
TYPE 2: TEMPORARY OBSTRUCTION

Example from dataset

TYPE 3: OBFUSCATION

- **Definition:** Confusing or misleading the user; obscuring information and/or options that would allow the user to initiate or advance in the task flow
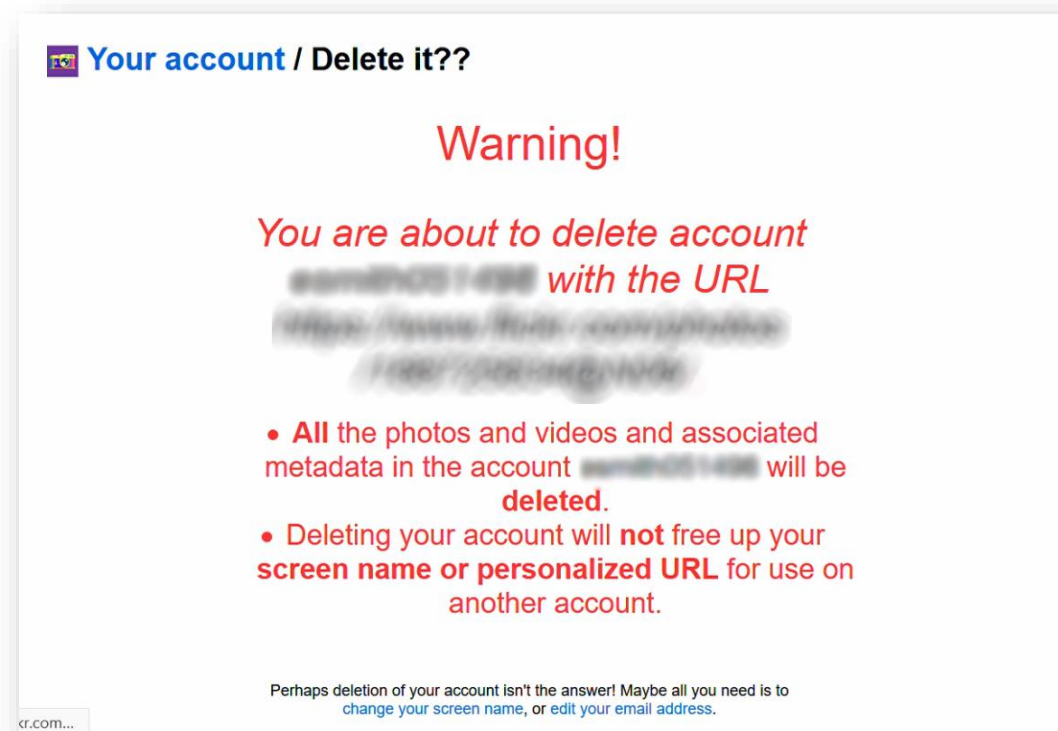
TYPE 3: OBFUSCATION

Examples from dataset

TYPE 4: INDUCEMENTS TO RECONSIDER

- **Definition:** Persuading the user to reconsider their choice to disable their account; presenting the option to stay on the site favourably through language, visuals, or incentives
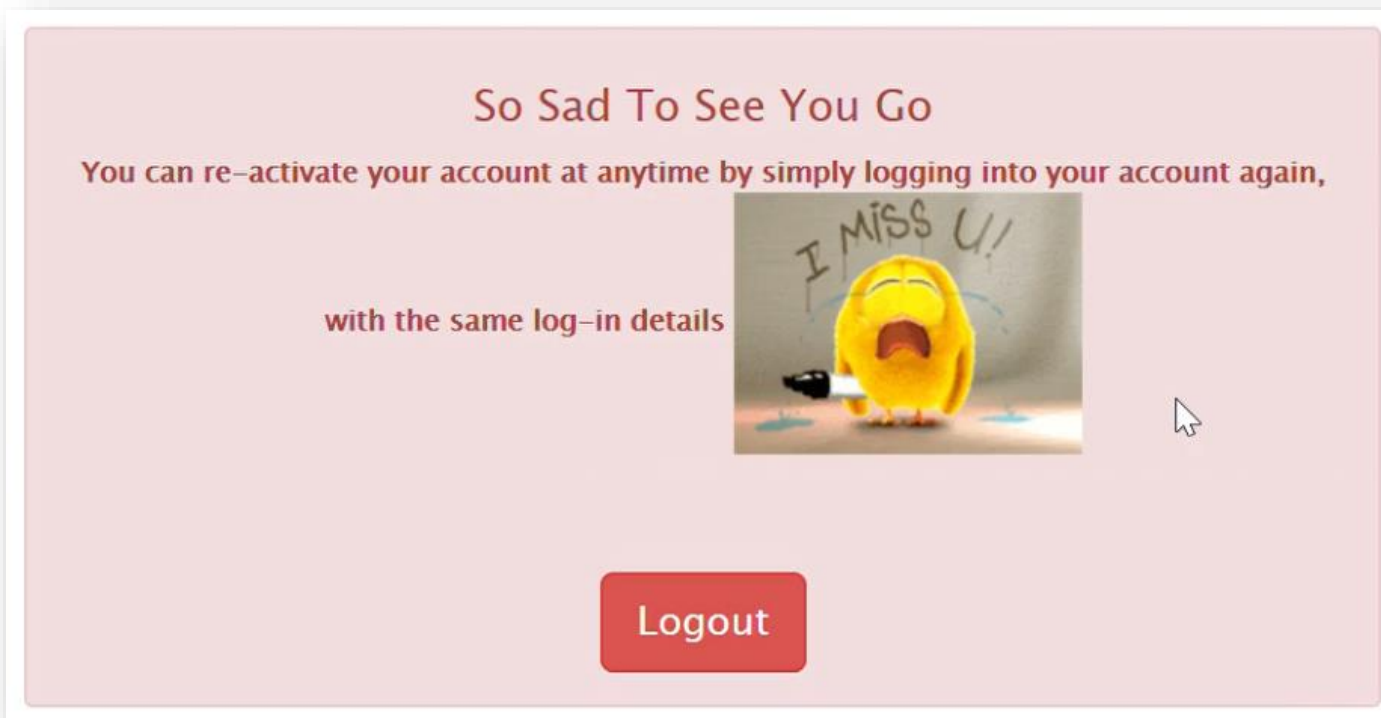
TYPE 4: INDUCEMENTS TO RECONSIDER

Example from dataset

TYPE 5: CONSEQUENCES

- **Definition:** Encouraging the user to return to the site after their account has been disabled; reducing the effort required to return or continuing to communicate with the user

TYPE 5: CONSEQUENCES

Example from dataset

QUANTITATIVE RESULTS

- All of the 26 sampled SNSs were identified using at least one type of dark pattern

- Five (5) out of 26 SNSs (19%) attempted to manipulate the user at least five or more times during their account disabling process

CONCLUSION

- In this study, we created an empirically verified typology of dark patterns in the context of online services using UIs to sabotage users' efforts to disable their accounts

- The Dark Pattern Typology contributes to future work that:
  - Documents the prevalence of dark patterns in SNSs
  - Identifies dark patterns in other online services
  - Investigates users' perceptions and experiences of dark patterns
  - Determines the effects of dark patterns on user behaviour

REFERENCES

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). http://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-63722

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

REFERENCES

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.

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., 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