Dominique Kelly
Western University, London, Ontario, Canada

Jacquelyn Burkell
Western University, London, Ontario, Canada

HOW DARK PATTERNS UNDERMINE USERS' SOCIAL PRIVACY ONLINE (Lightning Talk)

Abstract:

We performed a content analysis of the user interface (UI) designs for five social networking sites (SNSs) popular among teens. As a result of this analysis, we identified UI design tactics that undermine people's social privacy – or *privacy dark patterns* – and consolidated these tactics into a typology consisting of two main types (Obstruction and Obfuscation) and seven subtypes.

1. Background

Since 2010, research has documented the presence of manipulative user interface (UI) design tactics – or *dark patterns* (Brignull, 2010) – across various contexts, including shopping websites (Mathur et al., 2019), video games (Zagal et al., 2013), and online privacy notices (Nouwens et al., 2020). Some of these tactics, known as *privacy dark patterns*, nudge people to make choices or take actions that weaken their online privacy (Bösch et al., 2016; Fritsch, 2017). Privacy dark patterns often facilitate the corporate collection and use of users' personal data, thereby reducing their *institutional privacy* (Raynes-Goldie, 2010). Privacy dark patterns can also lead users to make decisions that increase other people's access to their personal data, ultimately reducing their *social privacy* (Raynes-Goldie, 2010). When social networking sites (SNSs) deploy dark patterns to encourage data sharing with other people, users are exposed to various privacy-related risks and harms, including identity theft, stalking, embarrassment, and blackmail (Gross & Acquisti, 2005).

Teens and young adults generally report greater concern for social privacy than institutional privacy (Adorjan & Ricciardelli, 2019; Raynes-Goldie, 2010), and research has uncovered a number of strategies that young people rely on to protect their social privacy online (Duffy & Chan, 2019; Hargittai & Marwick, 2016; Marwick & boyd, 2014; Raynes-Goldie, 2010). However, teens' attempts to preserve their social privacy could be undermined by the presence of dark patterns deliberately designed to increase other people's access to their personal data. Teens are avid users of the internet and social media, with platforms such as TikTok, Instagram, and Snapchat claiming high numbers of 13- to 17-year-old American users as of 2022 (Vogels et al., 2022). Moreover, dark patterns often exploit people's innate cognitive biases and heuristics (Lukoff et al., 2021; Mathur et al., 2019; Waldman, 2020), making them difficult to recognize and resist (Bongard-Blanchy et al., 2021; Di Geronimo et al., 2020).

2. Summary of Study

This talk will present the results of a study that documented privacy dark patterns designed to reduce users' social privacy on five SNSs popular among teens: Discord, Twitter, Instagram, TikTok, and Snapchat (Statista, 2021; Vogels et al., 2022). From March to May 2022, the first author screen-recorded her attempts to register an account, configure account settings, and log in and out of the account for each site, capturing a total of 185 minutes of user-SNS interactions. During each procedure, the first author aimed to make choices and take actions that protected the user's privacy as much as possible. We then content-analyzed the recordings for evidence of UI design strategies that could influence people to make choices that weaken their social privacy (i.e., choices that promote other people's access to their personal data, either by increasing the amount of data shared or expanding the size of the audience to whom that data is disclosed). In the coding process, we paid careful attention to visual and verbal UI design elements – such as buttons, text, pop-ups, pre-selected options, and images – as well as the size, colour, contrast, and placement of these UI elements. We focused on design strategies that operated by increasing the user's workload, misleading the user, or persuading the user through language and visuals (adapted from a model presented in prior work [Kelly & Rubin, 2022]).

We identified two main privacy dark pattern types (Obstruction and Obfuscation) and seven subtypes (Defaults, Confirmations, Interruptions, Missing Bulk Options, Attention Manipulation, False Private Account, and Concealed Settings) as a result of our content analysis of the recordings. Our findings indicate that sites employ a variety of strategies, often in combinations that complement and reinforce one another, to steer users to share a large amount of personal data with a wide audience. These strategies include hiding default settings that allow other site members to find users by their email address or phone number, prompting users to sync their contacts through pop-ups at login, and forcing users to confirm their choice when attempting to restrict the audience for their posts.

By influencing teens' online behaviour – sometimes in ways outside of their conscious awareness – privacy dark patterns hinder these young SNS users' attempts to protect their social privacy. There is a need for regulatory and educational initiatives to combat the proliferation of privacy dark patterns online and empower users to make conscious and informed choices about the disclosure of their personal data.

Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

References

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology/Revue Canadienne de Sociologie*, *56*(1), 8-29. https://doi.org/10.1111/cars.12227

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). "I am definitely manipulated, even when I am aware of it. It's ridiculous!" - Dark patterns from the end-user perspective. *DIS'21: Designing Interactive Systems Conference 2021*, 763-776. https://doi.org/10.1145/3461778.3462086

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. (2010). Dark patterns. https://www.darkpatterns.org/

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-14. https://dl.acm.org/doi/10.1145/3313831.3376600

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society, 21*(1), 119-138. https://doi.org/10.1177/1461444818791318

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

Gross, R., & Acquisti, A. (2005). Information relevation and privacy in online social networks. *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 71-80. https://doi.org/10.1145/1102199.1102214

Hargittai, E., & Marwick, A. E. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737-3757. https://doi.org/10.5167/UZH-148157

Kelly, D. & Rubin, V. L. (2022). Dark pattern typology: How do social networking sites deter disabling of user accounts? *12th International Conference on Social Media & Society*, July 18 -19, Toronto, Canada. https://easychair.org/publications/preprint/GD6S

Lukoff, K., Hiniker, A., Gray, C. M., Mathur, A., & Chivukula, S. S. (2021). What can CHI do about dark patterns? *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (*CHI EA '21*), 1-6. https://doi.org/10.1145/3411763.3441360

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051-1067. https://doi.org/10.1177/1461444814543995

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*(CSCW), 1-32. https://doi.org/10.1145/3359183

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (*CHI '20*), 1-13. https://doi.org/10.1145/3313831.3376321

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). https://doi.org/10.5210/fm.v15i1.2775

Statista. (2021). Most popular social networks of teenagers in the United States from fall 2012 to fall 2020. https://www.statista.com/statistics/250172/social-network-usage-of-us-teens-and-young-adults/

Vogels, E. A., Gelles-Watnick, R., Massarat, N. (2022). Teens, social media and technology 2022. *Pew Research Center*. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

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