TREO
Technology, Research, Education, Opinion

Modes of privacy settings and user privacy choices: An experimental study

Malgorzata Kolotylo-Kulkarni, Ph.D., Drake University, malgorzata.kolotylo-kulkarni@drake.edu;
Gurpreet Dhillon, Ph.D., University of North Carolina at Greensboro, gdhillon@uncg.edu;
Weidong Xia, Ph.D., Florida International University, xiaw@fiu.edu

Problem Definition. Choosing privacy settings is arguably one of the most crucial steps in protecting one's privacy online. Privacy settings are often established as default options in initial system installations. These default options can differ in terms of their characteristics and presentation formats. For instance, they can be provided as lists, varying in number of options, pre-set in ways that are directed at either sharing or keeping information private. Choosing privacy options is particularly important for users of health apps, as those apps are often unregulated and not always HIPPA-compliant. Furthermore, sharing health and fitness information can pose substantial risks or unintended consequences such as revealing the user's patterns of behaviors or their locations (Spinks, 2017). It is thus crucial to investigate how, and with what outcomes, users choose privacy settings for sharing health-related information when faced with different modes of delivery of privacy options.

Recently, research has examined the role of different forms of information presentation on user's privacy decision-making: investigating the effect of default options on privacy choices (Craciun 2018) or looking at the influence of choice frames on users' disclosure settings (Adjerid et al 2019). However, little is known about the interaction between the user and privacy settings interfaces designed as lists of options either turned on or off by default, and the role that it plays in user's choices; and, further, whether it may differ across users. Drawing from option framing research, this study aims to provide insights on the effect of additive and subtractive modes of delivery of privacy options on user's decisions and on how these effects vary for users exhibiting different privacy concerns.

Proposed methodology. The proposed methodology constitutes a 2 (privacy settings mode: additive vs. subtractive) x 2 (privacy concern weak vs. strong) experimental design.

Expected contribution. This study is expected to contribute to the privacy research literature by examining the differential effects that modes of privacy settings can have on users' privacy decisions. From a practical standpoint, the study results can educate users about the possible impacts of different modes of privacy settings on their choices and can inform system designers about how interactions between privacy setting modes and privacy concerns influence user choices so that they can take them into consideration when designing privacy options.

References

▪ Craciun, G. (2018). Choice defaults and social consensus effects on online information sharing: The moderating role of regulatory focus. *Computers in Human Behavior*, *88*, 89-102.

▪ Adjerid, I., Acquisti, A., & Loewenstein, G. (2018). Choice architecture, framing, and cascaded privacy choices. *Management Science*, *65*(5), 2267-2290.

▪ Spinks. R. (08/01/2017). Using a fitness app taught me the scary truth about why privacy settings are a feminist issue. *Quartz*. Retrieved from: https://tinyurl.com/yd9mlb9a

Presentation at TREO Talks in conjunction with the Fortieth International Conference on Information Systems, Munich 2019
All TREO Talks are available at https://github.com/mschermann/treoaticis2019