Do Mobile App Providers Try Enough to Protect Users’ Privacy? – a Content Analysis of Mobile App Privacy Policies

Mehrdad Koohikamali
University of Redlands

Dan J. Kim
University of North Texas, Dan.Kim@unt.edu

Follow this and additional works at: http://aisel.aisnet.org/sigbd2016

Recommended Citation

http://aisel.aisnet.org/sigbd2016/1

This material is brought to you by the Special Interest Group on Big Data Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in International Conference Information Systems 2016 Special Interest Group on Big Data Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Do Mobile App Providers Try Enough to Protect Users’ Privacy? – a Content Analysis of Mobile App Privacy Policies

Mehrdad Koohikamali¹, Dan J. Kim ²
¹School of Business, University of Redlands, 1200 East Colton Ave P.O., 3080 Redlands, CA 92373, United States
²Information Technology & Decision Sciences, College of Business, University of North Texas, 1155 Union Circle, 305249 Denton, TX 76203, United States
Dan.Kim@unt.edu

Do Mobile App Providers Try Enough to Protect Users’ Privacy?

Privacy policies are widely used to draw clear image of risks to users’ personal information in different contexts such as mobile apps. Nonetheless, many believe privacy policies are ineffective tools to notify and aware users about possible risks to information privacy merely because most users have a very low tendency to go through privacy policies to read and comprehend them. Due to intimacy of mobile apps, much of personal information disclosed to them are at risk. Specially, when mobile app users share sensitive personal information to apps chance of privacy violation and consequent risks are higher. It is not only important to understand how mobile developers practically implement a contract to protect users’ privacy based on users’ preferences but also crucial to examine the role of sensitivity of information on developers’ emphasis on different aspects of privacy.

This research focuses on two aspects to understand the circumstance users experience when privacy policies are presented: efforts users have to make to read and understand privacy policies in terms of readability and length of statements, and developers’ emphasis on aspects of information privacy with respect to sensitivity of information. To elucidate easiness of reading privacy policy statements, readability and length are calculated. Through the lens of framing concept of prospect theory, this study investigates the information sensitivity level effect on developers’ emphasis on privacy dimensions. Three mobile app categories deal with different levels of sensitive data are health, navigation, and game apps. To differentiate between emphasis on different privacy dimensions when information sensitivity differs, a text mining method is developed in R to analyze the weights of four key privacy dimensions (collection, secondary use, improper access, and error).

We downloaded 90 unique mobile app privacy policies. Readability calculations reveal that users should have a minimum of 12 years of secondary education to easily understand privacy policies. The average length of privacy policies is at least 1900 words, which hinders a thorough reading. ANOVA results show a significant difference between secondary uses of information in app privacy policies dealing with higher sensitive data. In addition, the findings demonstrate collection is more emphasized in health than game app privacy policies but do not find any significant difference between improper access dimensions. This study has made two key contributions. First, by building upon the framing concept of prospect theory, this research provides an effective framework to understand the organizational perspective of privacy concerns. Second, the results demonstrate the information sensitivity level is important for measuring privacy concerns.
Do Mobile App Providers Try Enough to Protect Users’ Privacy?

References


Do Mobile App Providers Try Enough to Protect Users’ Privacy?


Do Mobile App Providers Try Enough to Protect Users’ Privacy?


Liu, Z., Shan, J., Bonazzi, R., and Pigneur, Y. Privacy as a tradeoff: Introducing the notion of privacy calculus for context-aware mobile applications. in System Sciences (HICSS), 2014 47th Hawaii International Conference on. 2014. IEEE.


Pavlou, P.A. State of the information privacy literature: where are we now and where should we go? MIS Quarterly. 35.4 (2011).


Do Mobile App Providers Try Enough to Protect Users’ Privacy?


Talib, S., Razak, A., Munirah, S., Olowolayemo, A., Salependi, M., Ahmad, N.F., Kunhamoo, S., and Bani, S.K. Perception analysis of social networks’ privacy policy: Instagram as a case study. in Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on. 2014. IEEE.


Weible, R.J., Privacy and data: an empirical study of the influence of types of data and situational context upon privacy perceptions, in Department of Business and Industry. 1993, Mississippi State University. p. 378.


Xue, M., Liu, Y., Ross, K.W., and Qian, H. I know where you are: thwarting privacy protection in location-based social discovery services. in Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on. 2015. IEEE.


Young, J.D. and Anton, A.I. A method for identifying software requirements based on policy commitments. in Requirements Engineering Conference (RE), 2010 18th IEEE International. 2010. IEEE.