User Privacy Preservation on Mobile Devices: Investigating the Role of Contextual Integrity

by

Ming Di Leom

MSc (Cyber Security and Forensic Computing)

Bachelor in Computing (Hons)

A thesis submitted for the degree of

Doctor of Philosophy

Computer and Information Science

School of Information Technology & Mathematical Sciences
Division of Information Technology, Engineering and the Environment

University of
South Australia

July 2020

Abstract

Privacy issues emerge when mobile devices can not only collect user information but also share it automatically in the background, opportunities for which were previously limited. The general approach of privacy preservation in mobile devices through permissions management alone is not optimal due to the gap between flexibility and usability. The framework of contextual integrity (CI) has been proposed to accommodate diversity in contexts and also users' privacy preferences. Accommodating the diversity in contexts and also users' privacy preferences is complicated by privacy paradox—a discrepancy between expressed concern and the actual behaviour. We examined how the framework can address privacy paradox and its implications on mobile devices in two user studies.

In the first study, we examined the prevalence of privacy paradox through the lens of the CI framework. The framework emphasises on the influence of contextual factors in our every day's mobile usage. We examined one such contextual factor is the recipients—user's attitude towards them. The results suggest trust having a significant influence on the user's disclosure behaviour, particularly on the relationship between privacy concern and self-disclosure. The mediation effect of trust in our results suggest its significant role in determining users' self-disclosure despite the existence of privacy concern. The findings offer a meaningful explanation behind privacy paradox; where a user is more likely to disclose to a trusted recipient, despite having privacy concern.

In the second study, we examined the impact of two contextual factors—recipient and information type—on the relationship between information relevance and self-disclosure. While there is evidence of a significant relationship between information relevance and disclosure, several discrepancies showed the relationship is not always clear-cut. The results highlight users' attitude on disclosure within the mobile ecosystem is often fraught with nuances and the use of generic information relevance in predicting the tendency to disclose may not be as effective as expected. Our results from the second study also cast doubt over the established effects of "sensitivity" and its usefulness in privacy enhancing technologies (PET). We observed inconsistent response in willingness to disclose a type of information across recipients. This further demonstrates that sensitivity can vary according to the intended recipient.

Overall, this thesis demonstrates the relevance of the CI framework in the mobile space and its potential to improve the current approach in PET, particularly the privacy recommendation system. The privacy recommendation system is a promising answer to the dilemma of having too little or too much privacy control. We believe by incorporating a crucial metric, "recipient", in addition to other contextual factors, the privacy recommendation system can advance its effectiveness. By taking into account of users' interactions with their recipients, the metric enables the ability to accommodate the ever-changing contexts and the diversity of users' privacy preferences.