Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 7-19-2017

Expecting the Unexpected in Security Violations in Mobile Apps

Yijing Li
University of New South Wales, yijing.li@unsw.edu.au

Ben C.F. Choi
Nanyang Business School, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798, Singapore and School of Information Systems, Technology and Management, UNSW Australia Business School Sydney, ben.cf.choi@gmail.com

Expecting the Unexpected in Security Violations in Mobile Apps

Research-in-Progress

Yijing Li
School of Information Systems and Technology Management, UNSW Australia Business School
Sydney, NSW 2052, Australia
yijing.li@unsw.edu.au

Ben C.F. Choi
Nanyang Business School, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798, Singapore
and
School of Information Systems, Technology and Management, UNSW Australia Business School
Sydney, NSW 2052, Australia
ben.cf.choi@gmail.com

Abstract

Mobile apps often require numerous access and control over smartphone functionalities and users' personal data. This increased access and control may raise users' perception of heightened privacy leakage and security issues. This is especially the case if users' awareness and expectations of this external access and control is not accurately recognized through proper security declarations. This proposal thus attempts to put forth an investigation on the effect of mobile users' privacy expectation disconfirmation on their continued usage intention of mobile apps sourced from app distribution stores. Drawing upon the APCO framework, security awareness literature and the expectation-disconfirmation perspective, two key types of security awareness information are identified; namely access annotation and modification annotation. It is noted that these types of information can be emphasized in app distribution stores to reduce subsequent privacy expectation disconfirmation. Hence, this study plans to examine the downstream effect of privacy expectation disconfirmation on users' continued usage intention. To operationalize this research, a laboratory experiment will be conducted.

Keywords*: Privacy Expectation, Security Awareness, Expectation Disconfirmation, Mobile Apps, Mobile App Distribution Platforms, Privacy Guidelines*

Introduction

The number and variety of smartphone apps has grown exponentially since the introduction of mobile app distribution markets. The two leading app distribution markets, Google Play (Android) and Apple App Store (iOS) respectively, offered more than 3.1 million apps with over 300 billion downloads and are expected to generate a revenue of more than 100 billion US dollars by 2020 (Statista 2015a; Statista 2015b; Woods). These mobile apps often require numerous access and control over smartphones, such as accessing users' current location, retrieving contact lists, and collecting other personal information - in exchange for more customized, relevant, and efficient services. This increased access and control may raise users' perception of heightened privacy leakage and security issues. This is especially the case if users' awareness and expectations of this external access and control is not sufficiently raised or managed through proper security declarations (e.g.,Gatto et al. 2015).

Indeed, the privacy measures and security measures taken by app distribution platforms to protect end-users has been noted as a key factor in motivating mobile app installations. In particular, past research has highlighted two key ways of conveying specific privacy and security requirement to end-users (Hoffman 2013). By forming pre-usage privacy expectations, users may hence be in a better position to confirm privacy expectations and increase the probability of their intention to continue their usage of the mobile app. Additionally, emerging research suggests that individuals' privacy dispositions are largely stable over time and can play a key role in shaping the effects of privacy expectations on behaviors.

The objective of this research proposal is to extend existing mobile privacy research by determining the extent of the role of privacy expectation disconfirmation in user's eventual continued or discontinued usage intention of mobile apps. Specifically, drawing on the Antecedents – Privacy Concerns – Outcomes (APCO) framework and the Expectation Disconfirmation Theory (EDT), this study sets to identify two key types of security-awareness annotation, namely access annotation and modification annotation, and explore the impact of annotations jointly on privacy expectation disconfirmation, which in turn influence continued usage intention. Furthermore, this study posits that the impact of annotation on privacy expectation is moderated by dispositional privacy concerns.

Literature Review

The Antecedent Privacy Concern Outcomes (APCO) Framework

The conceptualization of privacy and examination of privacy-related behavioral outcomes have long been the focus of information privacy research (e.g.,Hong and Thong 2013; Malhotra et al. 2004), which has identified a myriad of determinants of privacy perceptions in both offline and online environments (e.g.,Awad and Krishnan 2006; Milberg et al. 2000; Wall et al. 2016). In an interdisciplinary review of privacy-related research, Smith et al. (2011) integrated the major privacy perspectives to propose an integrative privacy-specific framework, namely the Antecedents-Privacy Concerns-Outcomes (APCO) framework. Specifically, the framework posits that individuals' responses to external stimuli result in deliberate privacy tradeoff that leads to fully informed privacy-related behaviors. Overall, the APCO framework can be summarized into four key elements of privacy processing, namely privacy antecedents, privacy evaluation, privacy dispositions, and privacy-related behavior. In the following sections, the two key elements of the APCO framework are discussed.

Privacy Antecedents and Privacy Expectation Formation

According to the APCO framework, privacy evaluation is a central concept which subsumes individuals' initial privacy expectation formulation and subsequent confirmation, when they engage in actions that could potentially result in privacy invasive actions (Smith et al. 2011). Past research has mainly focused on examining the effects of expectation in guiding regulatory behaviors and sustained behaviors (Okazaki et al. 2009; Solove 2006). Ample IS research has examined the importance of expectation in inducing technology adoption and usage. In general, expectation is defined as an individual's belief that a given behavior will lead to the expected outcome. Accordingly, in this study, privacy expectation is defined as the extent to which a user believes that the app will have implemented mechanisms to safeguard their privacy.

Past work examining privacy expectation has focused on understanding individuals' mental models regarding security in using information technologies. For example, Camp (2009) found that educating users about the statistical and technical details of security risks were difficult, if not entirely unproductive. The author further revealed that mental models was useful mechanism to communicate

to end users about security risks. Collectively, past research largely agrees that mental models are important in helping individuals construct accurate expectations specific to privacy and security issues.

Security Awareness

The main thrust of privacy research has focused on understanding the importance of eliciting the awareness of individuals about security and privacy control (e.g.,Skinner 1996). Ample research suggests that awareness elicitation is a critical issue in information security. Hartono et al. (2014) conducted an extensive literature review on past information security research and identified two key aspects of security awareness, namely confidentiality awareness and integrity awareness. Confidentiality awareness is defined as the understanding of mechanisms that protect users' information against improper disclosures and leakages (Tsiakis and Sthephanides 2005). Past research has revealed robust evidence about the importance of confidentiality awareness on privacy expectation formulation. Accordingly, this research focuses on the awareness annotation, which refers to the availability of information with regards to privacy exposure in using mobile apps.

Integrity awareness is about understanding the availability of prevention against improper modifications to information (Tsiakis and Sthephanides 2005). Strong integrity is essential to preventing improper modification of information, such as faulty alternation, deletion, and addition. Although modification of information can be accidental and user-driven, such modification could be performed by malicious apps. Some of the common security measures to maintain integrity include anti-virus apps that prevent malevolent apps from destroying data. However, anti-virus apps for mobile phones are not very commonly used by smartphone owners, where approximately 40% of users have no antivirus software on their smartphones (Kaspersky 2012).

Accordingly, this research focuses on modification annotation, which refers to the availability of information with regards to the dedication of change permissions to mobile apps. Specifically, corresponding to the importance of confidentiality awareness, this study focuses on access annotation refers to the availability of information regarding the privacy exposure in using a mobile app. Likewise, reflecting the importance of integrity awareness, this study examines modification annotation, which refers to the availability of information regarding the dedication of change permission to a mobile app.

Expectation (Dis-)Confirmation and Privacy Evaluation

The expectation (dis-)confirmation literature has mainly focused on examining the effect of expectation in guiding regulatory behaviors and sustained behaviors (Okazaki et al. 2009; Solove 2006). For instance, expectation is known to be the key motivation in sustaining participations in physical fitness activities (Rejeski and Kenney 1988). Likewise, ample IS research has examined the importance of expectation in inducing technology adoption and usage. In general, expectation is defined as an individual's belief that a given behavior will lead to the expected outcome (Bandura 1977; Bandura 1994).

Privacy evaluation is a psychological process in which individuals evaluate their initial privacy expectation with actual experience. Past work examining privacy expectation has focused on understanding individuals' mental models regarding security in using information technologies. For example, Camp (2009) found that educating users about the statistical and technical details of security risks were difficult, if not entirely unproductive. The author further revealed that mental models was useful mechanism to communicate to end users about security risks. Accordingly, drawing on the expectation (dis-)confirmation literature and past research examining privacy evaluation, this study defines privacy expectation as the extent to which a user believes that the app will have implemented mechanisms to safeguard their privacy.

It is worthy to note that individuals' privacy expectation can be highly contextualized and hence a privacy expectation about a specific mobile app might not be entirely applicable to an individual's expectation over other apps. For instance, in evaluating the Amazon app, individuals would expect the app to collect their emails, residential addresses, and credit card information. However, when evaluating the Google Map app, individuals might expect their real-time location data to be collected but not their personal information. Nonetheless, through the perspective of privacy expectation, privacy violation can be elucidated as disconfirmation of privacy expectation that is formed specific to a context.

Research Model and Hypotheses Development

The proposed research model is presented in Figure 1.

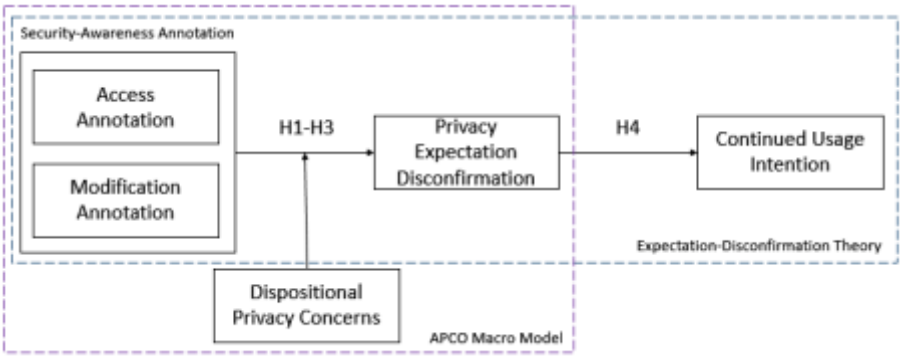

Figure 1. Research Model

Determinants of Privacy Expectation Disconfirmation

In evaluating mobile apps, users might be challenged with a huge collection of mobile apps. Consequently, it becomes highly challenging for users to clearly understand the access restrictiveness and modify restrictiveness in choosing an app. In such a case, annotated information provides users explicit indications of the extent of access restrictiveness and modify restrictiveness. Research suggests that users tend to rely on explicit information in making technology adoption decision in the online environment (e.g.,Li and Hitt 2008). In particular, annotated information provided by the app market is often considered fair evaluations, which are credible and trustworthiness. Therefore, when access restrictiveness and modify restrictiveness are annotated in the app market, users will be alerted about the potential privacy implication in installing the apps. Accordingly, users are less likely to over-estimate the extent of their privacy is protected and hence less likely to develop privacy expectation disconfirmation subsequently.

However, when the annotated information is not available, users are likely to develop privacy expectation based on general understanding and assumption. In particular, since the apps are offered in established app markets (e.g., Android and iOS), given the lack of specific security-related information, users might rely on convenient evaluation by extending their trust on the app market as a whole. Similarly, in evaluating mobile apps, in cases where annotated information is unavailable, users are likely to rely on their dispositional beliefs on the app markets. By relying on the general opinion on the app market, users are likely to develop inaccurate understanding of privacy protection mechanisms in apps. Therefore, when annotated information is unavailable, users might over-estimate their privacy expectation and hence are likely develop privacy expectation disconfirmation after usage. Hence,

H1a: Compared to the absence of access annotation, the presence of access annotation will lead to less privacy expectation disconfirmation.

H1b: Compared to the absence of modification annotation, the presence of modification annotation will lead to less privacy expectation disconfirmation.

In cases where modification annotation is absent, the mobile app does not inform the user of what changes it can make to users' phones and their personal data. Similarly, in cases where access annotation is absent, the mobile app does not inform the user of what it can collect from their phone and personal data. Subsequently, in the absence of modification annotation, the effect of access annotation is pronounced. This is because the absence of access annotation will give the user no information to form their privacy expectations around, other than their existent beliefs and attitudes towards the mobile app. This is most likely very inaccurate as they have not used the app before. Further, the presence of access annotation will enable users to form basic privacy expectations based on what personal data the app can view, albeit inaccurate due to insufficient information about how the mobile app will change personal data on the phone. The inaccuracy of this privacy expectation hence cause privacy expectation to be disconfirmed.

In the presence of modification annotation, the effect of access annotation on privacy expectation disconfirmation is expected to be even more so amplified. This is because when modification annotation is available, individuals are likely to be more concerned with the privacy implications it

can have on their personal data since the mobile app can now change their personal data as opposed to just collecting or viewing it. Hence, it is more likely that users will scrutinize the security annotation, and thus form more accurate privacy expectations, hence reducing the potential of privacy expectation disconfirmation.

H2: The effect of access annotation on privacy expectation disconfirmation is stronger in the presence of modification annotation condition than in the absence of modification annotation condition.

When individuals have low dispositional privacy concerns, they generally coarsely trust external parties to safeguard their personal data, and hence become highly insensitive towards security policies and privacy statements. As a result, when dispositional privacy concern is low, individuals are expected to largely ignore security-awareness annotation, and hence likely to form elevated initial privacy expectation. Given the unrealistic initial privacy assessment, it is likely that their expectation will be violation, and hence leading to privacy expectation disconfirmation.

In contrast, individuals with high dispositional privacy concerns are typical ultra-sensitive towards protecting their personal information in online transactions. Consequently, in evaluating privacy expectation, they are likely to pay special attention to the available security-awareness annotation. As individuals are highly prudent in scrutinizing security annotation information, they are likely to form more realistic privacy expectation, which is less likely to be violated subsequently. In sum, we posit

H3: Compared to low dispositional privacy concerns, high dispositional privacy concerns will strengthen the positive moderation influence of modification annotation on the impact of access annotation on privacy expectation disconfirmation.

When the intensity of privacy expectation disconfirmation increases, users' psychological discomfort is likely to become stronger because inconsistency among her beliefs, attitudes, or actions increases. Thus, it is expected that more privacy expectation disconfirmation (i.e. less confirmation) will reduce intention to continue using mobile applications. Therefore,

H4: Privacy expectation disconfirmation will reduce continued usage intention.

Research methodology

Data Collection

To operationalize the research model, we plan to conduct a 2x2 full factorial design experiment. Subjects will be asked to imagine they need to "update a mobile application that they often use". Before the experiment, a workshop on mobile app security and privacy will be conducted. In the workshop, subjects will be briefed on the types as well as extent of information collection and threats to personal privacy in using mobile apps. Additionally, subjects will be ask to complete a short survey that measures their dispositional privacy concerns. They will then be asked to indicate a mobile app that they currently used on their smartphone for contextual understanding. Upon indicating the app, they will be presented with a hypothetical "app update" scenario where they will be asked to imagine that the app they named beforehand required an update which had some new privacy and security setting access. The security awareness information provided will be constructed based on the actual privacy policies and security statement provided by the respective app developers. Subjects will be asked to imagine that this scenario is real. Upon completing the evaluation, they will be instructed to begin answering a questionnaire, which measures their pre-usage privacy expectation. A second scenario will then be shown that the mobile app has potentially become privacy invasive due to the actual permission requirement discovered on usage. Upon evaluating this scenario, the participants will be asked to complete their responses the questionnaire, to measure their post-usage privacy expectation and continued usage intention. Upon completing the questionnaire, subjects will be debriefed and thanked.

Expected Contributions

This study will extend the APCO framework to the mobile app distribution market context by identifying the key APCO components (antecedents, privacy beliefs/ attitudes, outcomes) specific to distribution markets. Additionally, many studies in IS research have focused on technology adoption. However, few prior studies have elucidated the way to help users develop accurate initial expectations in evaluating technologies, even though initial expectation has been recognized as one of the key success factors in technology adoption. To develop rich insights into privacy issues associated with

mobile app usage, this study will draw on the expectation-disconfirmation theory to formally conceptualize and empirically validate the centrality of privacy expectation disconfirmation in driving continued app usage through its research models.

References

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS quarterly*), pp. 13-28.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological review* (84:2), p. 191.

Bandura, A. 1994. "Self-Efficacy. Wiley Online Library,").

Camp, L. J. 2009. "Mental Models of Privacy and Security," *IEEE Technology and society magazine* (28:3).

Gatto, J. G., Meyer, C. D., Broeker, E. S., and Pierce, A. L. 2015. "Ftc Issues New Guidance for Mobile App Developers That Collect Location Data."

Hartono, E., Holsapple, C. W., Kim, K.-Y., Na, K.-S., and Simpson, J. T. 2014. "Measuring Perceived Security in B2c Electronic Commerce Website Usage: A Respecification and Validation," *Decision Support Systems* (62), pp. 11-21.

Hoffman, C. 2013. "Ios Has App Permissions, Too: And They're Arguably Better Than Android's."

Hong, W., and Thong, J. Y. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.

Kaspersky. 2012. "Number of the Week: 40% of Modern Smartphones Owners Do Not Use Antivirus Software." Retrieved 11/10/2016, from http://www.kaspersky.com/about/news/press/2012/number-of-the-week-40-percent-of-modern-smartphones-owners-do-not-use-antivirus-software

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., and Wetherall, D. 2012. "A Conundrum of Permissions: Installing Applications on an Android Smartphone," *International Conference on Financial Cryptography and Data Security*: Springer, pp. 68-79.

Li, X., and Hitt, L. M. 2008. "Self-Selection and Information Role of Online Product Reviews," *Information Systems Research* (19:4), pp. 456-474.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information systems research* (15:4), pp. 336-355.

Milberg, S. J., Smith, H. J., and Burke, S. J. 2000. "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), p. 35.

Okazaki, S., Li, H., and Hirose, M. 2009. "Consumer Privacy Concerns and Preference for Degree of Regulatory Control," *Journal of Advertising* (38:4), pp. 63-77.

Rajivan, P., and Camp, J. 2016. "Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices," *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*: USENIX Association.

Rejeski, W. J., and Kenney, E. A. 1988. *Fitness Motivation: Preventing Participant Dropout*. Human Kinetics.

Skinner, E. A. 1996. "A Guide to Constructs of Control," *Journal of personality and social psychology* (71:3), p. 549.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS quarterly* (35:4), pp. 989-1016.

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania law review*), pp. 477-564.

Statista. 2015a. "Number of Apps Available in Leading App Stores as of July 2015." from http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Statista. 2015b. "Number of Downloads from the Apple App Store." from http://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/

Tsiakis, T., and Sthephanides, G. 2005. "The Concept of Security and Trust in Electronic Payments," *Computers & Security* (24:1), pp. 10-15.

Wall, J. D., Lowry, P. B., and Barlow, J. B. 2016. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association for Information Systems* (17:1).

Woods, B. "Google Play Had Twice as Many App Downloads as Apple's App Store in 2015." from http://thenextweb.com/apps/2016/01/20/google-play-had-twice-as-many-app-downloads-as-apples-app-store-in-2015/