Re-designing Permission Requirements to Encourage BYOD Policy Adherence

Lotus Lee(✉) and Jeremiah D. Still(✉)

San José State University, San Jose, CA, USA
{lotus.lee,jeremiah.still}@sjsu.edu

Abstract. Many corporations and organizations support a Bring Your Own Device (BYOD) policy, which allows employees to use their personal smartphones for work-related purposes. Access to proprietary company data and information from an employee's smartphone raises serious privacy and security concerns. Companies are vulnerable to data breaches if employees are unable to discern which applications are safe to install. Situating privacy requirements ought to encourage safer application install decisions and decrease risker ones. This study examines the use of context-relevant warning messages, which alert employees to be cautious when the company's BYOD policy may be violated. We also explore the impact of presenting permission requirements before and after making the install decision. We provide evidence that the presence of warnings, despite the timing of when they were presented, facilitated a lower number of risky installations. In situations when it was safe to install an application, warning messages presented before the install decision drastically encouraged installations compared to when there were no warnings. Interestingly, the opposite pattern was found when warning messages were presented after the decision. Overall, better privacy and security decisions will be made if permission requirements are displayed with relevant warning messages. In addition, safe installations will be encouraged through the placement of these meaningful warnings on the description page of a mobile application before a user has decided to install it.

Keywords: Decision-making · Interface design · Mobile security · Privacy · Trust · User experience

1 Introduction

Smartphones allow users to easily access and share valuable and sensitive data digitally (e.g., banking, intellectual property). This access is supported by a plethora of mobile applications (app) available for download from several official app stores (e.g., Apple's App Store, Android's Google Play). Apps are popular because they are perceived as useful (Mylonas et al. 2013). Unfortunately, approximately one-third of Android apps are over privileged (Felt, Chin, Hanna, Song and Wagner, 2011). In some cases over privileged apps threaten the security of sensitive data. When making a selection, users rely on information that is readily available on the description page of the mobile app. Ratings, reviews, cost, and number of downloads become some of the main criteria

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 369–378, 2015.
DOI: 10.1007/978-3-319-20376-8_33

used to make an install decision (Felt et al. 2012; Kelley et al. 2012; Kelley et al. 2013). Rarely do users consider company and personal privacy violations when installing an app. Mylonas et al. (2013) found that privacy was ranked near the bottom of the app decision criteria. Most smartphone users are unaware of the severity of the risks associated with an app installation because they rely on an external entity for protection (i.e., the app store) (Mylonas et al. 2013). Part of the reason is because the majority of smartphone users are not security experts (Mylonas et al. 2013). Users are not equipped with the right mental models to understand how their actions impact their privacy. Privacy self-management is also not considered to be their primary task (Pfleeger and Caputo, 2012). However, an important part of the app store experience requires users to consent to a certain level of data access that may involve detrimental consequences like identity theft. Several studies have demonstrated that there are inherent vulnerabilities with consent-based permission systems unbeknownst to smartphone users (Balebako et al. 2014; Barrera et al. 2010; Felt et al. 2011). Attempts to incorporate warning messages have failed as users will act on privacy related information even if they do not fully comprehend its meaning (Felt et al. 2012).

A growing concern in the field of mobile security within the enterprise space is that the majority of smartphone users do not exhibit the ability to maintain their privacy to avoid increased risk for themselves or associated organizations (Solove, 2013). There are several factors that come into play when examining the behaviors that dictate a smartphone user's absence of privacy self-management. Users will dismiss or overlook privacy related information due to technical jargon or becoming habituated to their prevalence (Felt et al. 2012). Over time, smartphone users have been trained to ignore privacy policies, warning messages, consent dialogs, and permission request screens (Bohme and Kopsell, 2010; Chia et al. 2012; Kelley et al. 2012). Although risk communication could help facilitate a heightened awareness of the potential dangers associated with installing mobile apps, the consent-based permission systems ought to be improved in a way that naturally encourages users to make informed decisions through more direct communication. Altering risky user behavior can be accomplished by communicating how the harm can personally relate back to users and their associated organizations' Bring Your Own Device (BYOD) policies (Pfleeger and Caputo, 2012).

Users are simply not provided with the proper information needed to flag privacy concerns. The task of maintaining awareness of personal and professional risk on a smartphone is becoming increasingly difficult. Therefore, the use of contextual warning messages may help to convey relevant privacy and security information that transparently and effectively connect risk with permission requirements. As a caveat, attention and comprehension to privacy information on a smartphone is significantly different than when using a desktop computer. 50 % of users take no more than 8 s to read consent dialogs on websites (Bohme, 2010). Therefore, the mobility and form factor of a smartphone requires immediate recognition of privacy relevant information that will prompt users at the appropriate time when making a decision to install an app. They cannot be overloaded with too much information that distracts them from moving forward or it will be ignored. Several studies have experimented with the timing and presentation of privacy information to motivate securer behavior and prevent risk in other contexts (Akhawe and Felt, 2013; Egelman et al. 2009; Kelley et al. 2013). In this study, we seek to explore the impact

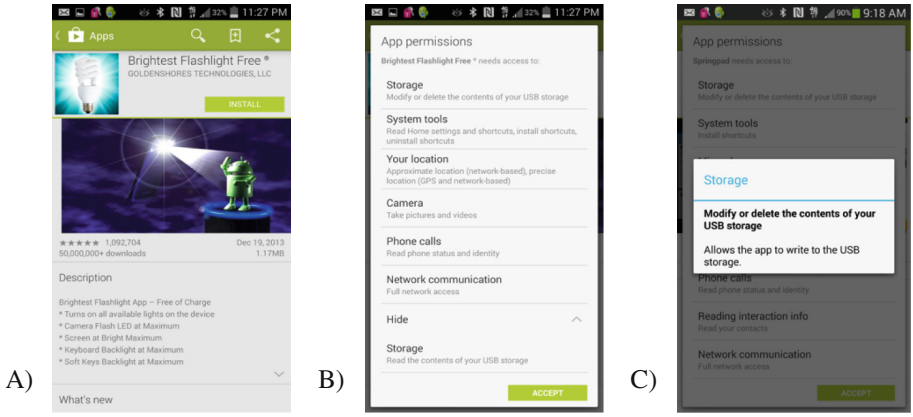

Fig. 1. Current Android mobile application screens

that warning messages and the temporal location of when permission requirements are presented have on the discernment of identifying risky and safe apps.

1.1 Relevant Warning Messages

Routinely experiencing the same standard warning messages may be misinterpreted overtime as trustworthy because of its sheer familiarity (Bohme and Kopsell, 2010). Similarly, default settings or Calls to Actions (CTAs) have an underlying influence on the user's privacy decisions without him being aware of it (Solove, 2013). Current defaults do not provide the appropriate framing necessary for users to proceed with caution. According to Jou, Shanteau and Harris (1996), "framing is a form of manipulating the salience or accessibility of different aspects of information" (p. 9). We propose that warning messages should be dynamic to the security needs of a particular context and be recognizable by the user. Figure 1 provides an example of an Android mobile app screen. As displayed in screen B, the interface provides a list of permission requirements without any visual indication to communicate risk or give warning that these items could potentially violate the user's privacy. Users are required to read through the information to interpret the risk and make their decisions accordingly without any visual support. Choe et al. (2013) found that the representation of privacy related information in a visual way could influence decision making, specifically with the use of color and symbols that resonate with common cultural experiences. Red has been used in privacy contexts to indicate conflicts between current settings and previous selections (Egelman et al. 2009). We explored the addition of warnings by highlighting risky permission requirements in red text, as well as placing a red stop sign to increase the likelihood that users will stop and attend to the permission requirements. We did not delineate the level or severity of risk per permission item. The level of risk has to be interpreted by the user. The warning message denotes permission requirements that are in violation of their BYOD policy or personal privacy.

1.2 Temporal Location of Permission Requirements

The timing of when privacy information is disclosed can nudge users towards installing a trustworthy or compromising app (Kelley et al. 2013). If users are presented with indicators of increased risk after a decision is made, they are more likely to disregard the new information (Egelman et al. 2009). According to Egelman et al. (2009), presenting privacy indicators on the search results page before a user makes a decision to proceed to a website optimized results in achieving higher levels of privacy in a shorter amount of time. Critically, once a user makes a decision, they are likely not to reverse it or spend extra time looking for alternatives (Akhawe and Felt, 2013). In other words, app stores are using a popular selling technique called low-balling to encourage the acceptance of uncomfortable risk. This persuasive method involves offering a great deal (e.g., a useful app) and asks for explicit agreement (e.g., to install) without presenting the unpleasant costs until later (c.f., Cialdini, Cacioppo, Bassett and Miller, 1978). The current Android app installation process, shown in Fig. 1, presents privacy requirements only after a user has made the decision to install the app (see screen B). Prior to the install decision, the user is given non-privacy related criteria (see screen A). Once the user has made the install decision by tapping on the Install button, screen B prompts them to "Accept" the required permissions. Please note, that screen C is hidden until the user taps on the individual permission items from screen B to get more details. The main CTAs on the first two screens (A and B) encourage users to install and then accept. There is no distinction on the user interface that explicitly distinguishes the binary choices to "Install" or "Not Install" on screen A, and "Accept" or "Not Accept" on screen B. Users are given permission requirements on screen B only after deciding to install the app on screen A. Kelley et al. (2013) found that users practically glossed over the permission requirements if presented after the install decision in the context of new apps. We propose to move the permission requirements from screen B to screen A to test which location facilitates safer choices and less risky behaviors.

1.3 Experiment Overview

Identifying malicious apps from safe ones is a difficult task, especially when there is no visual or contextual distinction between them. In this experiment, we explore the use of warning messages and the timing of the permission requirements' location relative to the install decision. We hope to encourage more secure decision-making and increase the number of safer app installations by presenting warnings prior to the install decision. This should help users recall their BYOD policy and personal privacy preferences in order to minimize risk and increase attention to the consent-based permission system.

2 Methods

2.1 Participants

The university institutional review board approved all experimental procedures. A total of twenty-two undergraduate volunteers received course credit for a sixty-minute effort. To maintain the counterbalance in our four experimental lists, the data collected from

six extra participants were excluded from further analysis. This allowed us to have an equal number of four participants represented across the four lists. The age of participants ranged from 18–35 years old with eight males and eight females. Four participants reported that English was not their first language. At the end of the experiment, participants were asked to fill out a survey regarding their general app usage. Fourteen out of 16 participants use an iPhone as their personal smartphone; the remaining two were Android users. On average, participants stated that they downloaded about one to two apps per month. 13 participants reported that they store private information on their smartphones, but only four reported that they have security or safety concerns with the device. All of the participants have never experienced identity theft in the past. Participants were also given a survey at the end of the experiment to measure their general trust in the hypothetical app store system. The survey is comprised of five negative and seven positive semantic statements (Jian et al. 2000). Overall, participants reported that they trusted the system ($M = 4.99$, $SD = 1$).

2.2 Apparatus

The study was created and run within Paradigm (http://www.paradigmexperiments.com/), an experimental presentation software employed for precise timing and data recording. Participants played Bejeweled (http://www.bejeweled.com) as a distraction task to pass time. The design of the hypothetical app store was modeled after the Android interface with slight modifications to the layout, iconography, and color scheme (see Fig. 2 for examples). In the experimental conditions where permission requirements are presented before the install decision, we introduced a tab-based menu to separate permissions, reviews and screenshots on the description page of the app. Permission requirements are defaulted to the first tab. The trials were created based on 10 real-world app types from the productivity category in the Google Play app store (e.g., calendar, calculator, reader, dictionary, flashlight, notes, reminders). Permission requirements, descriptions, and screenshots were taken directly from the apps. App logos, developer brands, and the name of the apps were customized to avoid confounds tied to familiarity.

2.3 Procedure

Participants were asked to fill out a demographic survey prior to beginning the experiment. They were then told to imagine they have just started employment at a new company and would be presented with a BYOD policy. A scenario was given to them explaining that they are employing an Android smartphone for personal and business purposes. They were prompted to study the hypothetical company's BYOD policy, then asked to play five minutes of Bejeweled. This ensured they were dependent on long-term memory for access to the BYOD policy. They were presented with one of four possible experimental condition blocks, ordered by using Latin square. After each block, participants were asked to reflect on their decision making process and prompted about their experience or familiarity with any of the apps. At the end of the experiment, two surveys regarding their application usage and level of trust with the hypothetical app store were given.

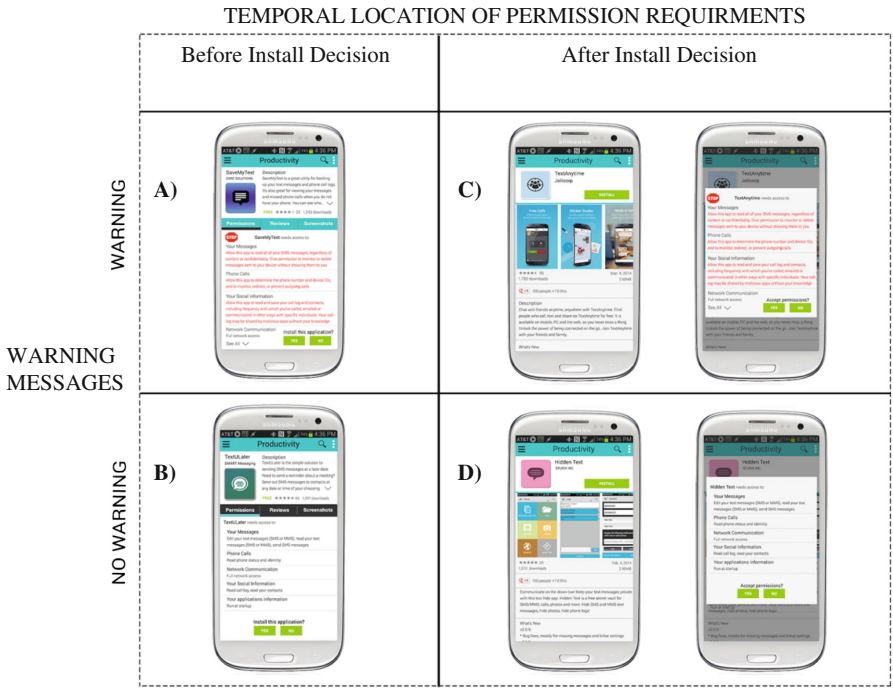

Fig. 2. Examples of the experimental conditions

Figure 2 shows the four experimental conditions stemming from a within-subjects design: Warning Messages 2 (present or absent) X Temporal Location 2 (before or after install decision). The four experimental condition blocks contained 10 trials each. Therefore, there were a total of 40 trials. We labeled the conditions as A, B, C, and D (denoted in Fig. 2). The order of the conditions was counterbalanced across participants: list 1 -ABCD, list 2 - BCDA, list 3 – CDAB, and list 4 - DABC. In each block of 10 trials, participants were asked to determine whether or not they would install the app. We measured the number of correct responses for each condition. 70% of trials were set up to have NO as the correct response, which meant that these apps are considered too risky to install. The NO trials represent risky apps that contain "dangerous" permissions that may store, capture, and share the user's data with remote third parties (Barrera et al. 2010; Mylonas et al. 2014). The permission requirements for these apps violated at least one of the company's BYOD policy given at the beginning of the experiment. The remaining 30 % of the trials was set to YES as the correct response. The YES trials represent apps that have limited access or fewer permission requirements that do not pose as much of a threat to the user. Therefore, users are safe to install these apps even though there may be warning message(s) present.

3 Results

A repeated measures ANOVA was employed to examine Warning Messages 2 (present or absent) X Temporal Location 2 (before or after install decision) on the portions of correct decisions to install. We separated the data according to the NO trials, when the user should not install the app, and YES trials for when the user should install the app.

3.1 Should not Install - Risky App

The analysis revealed that providing warning messages with the permission requirements significantly discouraged users from installing risky apps ($M = .80$, $SEM = .03$) compared with not having a warning message ($M = .61$, $SEM = .05$); $F(1,15) = 7.68$, $p = .014$, $\eta_p^2 = .034$. Unfortunately, users still installed dangerous apps approximately 20 % of the time even with relevant warning messages. The temporal location of permission requirements did not have a statistically significant impact on performance when presented before the install decision ($M = .70$, $SEM = .02$), or after ($M = .72$, $SEM = .05$); $F(1,15) = .15$, $p = .71$, $\eta_p^2 = .01$. Contrary to previous findings (e.g., Kelley et al. 2013), it appears the placement of the privacy information in relation to the install decision is not critical when it comes to identifying risky apps. There was also no statistically significant interaction between warning messages and permissions location $F(1,15) = .15$, $p = .71$, $\eta_p^2 = .01$.

3.2 Should Install - Safe App

The analysis showed no main effect of warning messages. There was no difference when warnings were present ($M = .57$, $SEM = .06$), or when there were no warnings ($M = .59$, $SEM = .06$); $F(1,15) = .09$, $p = .77$, $\eta_p^2 = .01$. However, there was a significant main effect for the temporal location of permission requirements on appropriate app installation; more appropriate decisions were made when the permission requirements were presented before the install decision ($M = .71$, $SEM = .05$) compared to after ($M = .46$, $SEM = .07$); $F(1,15) = 12.73$, $p = .003$, $\eta_p^2 = .46$. However, these findings were qualified by a significant interaction between warning messages and temporal location, $F(1,15) = 9.48$, $p = .01$, $\eta_p^2 = .39$ (see Fig. 3). Paired-samples t-tests were employed to further explain the interaction. When looking at the comparisons between the two temporal locations, warning messages presented before the install decision significantly increased safer installations ($M = .81$, $SEM = .05$) compared to when there were no warnings before the install decision ($M = .60$, $SEM = .07$); $t(15) = 2.43$, $p = .028$. However, when the warning messages were presented after the install decision, the opposite result occurred where warnings actually decreased safer installations ($M = .33$, $SEM = .09$) compared to when there were no warnings ($M = .58$, $SEM = .09$); $t(15) = -2.16$, $p = .048$. This suggests that meaningful warning messages increase trust of safe apps when placed on the description page. Interestingly, placing a warning message after a decision is made to install creates distrust.

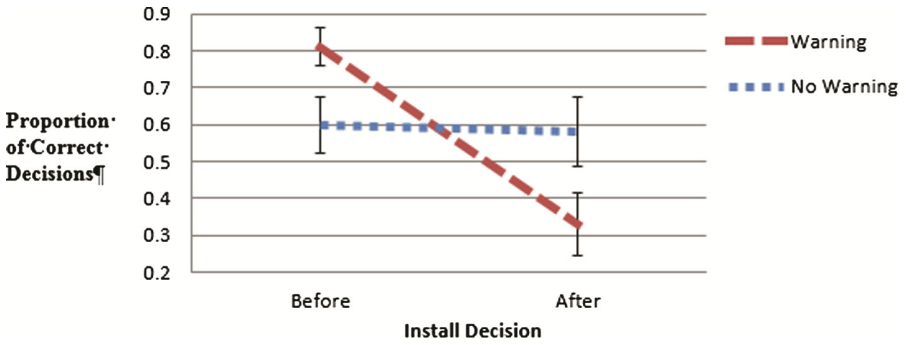

Fig. 3. Displays the interaction between Warning Message (present or absent) X Temporal Location (before or after install decision)

4 Discussion

We need to design secure systems that help users make safer decisions. Traditionally, warning messages do not account for the complexities of human decision-making (Solove, 2013). They assume cyber security expertise and are removed from the use context. We need to make the task of installing safer mobile apps relevant to a decision process and draw the user's limited attention to critical data. Current consent-based permission systems are not designed in a way that connects with users in a meaningful way. Smartphone users have a difficult time trying to identify risk using their current mental models. Further, they do not realize the degree to which they need to manage their privacy or have the ability to keep track of everything on the go (Kelley et al. 2012; Mylonas et al. 2013; Solove, 2013).

In this experiment, we explored the use of warning messages on permission requirements and the timing of when it was presented in relation to the install decision. We anticipated that users will make safer and less risky choices if warning messages are meaningful and presented as part of the decision criteria for selecting the appropriate apps to install. This experiment considered the impact of the manipulations on risky and safe app installation decisions. We found that the presence of warning messages facilitated a lower number of risky apps installations, but did not find temporal location had an impact either before or after the install decision. However, both warning messages and temporal location impacted safe app installations. We speculate that in the conditions with permission requirements presented before the install decision, warning messages were considered a part of the decision criteria, so users can factor in risk at their own discretion. However, in the conditions with permission requirements presented after the install decision, warning messages are unexpected. Therefore, we propose that warning messages given after the install decision are implicitly indicating to the user that the app may not be safe to install.

Yee (2005) explained that security interfaces could be designed in a way that helps bridge the communication between the system and the user in a cohesive and non-intrusive way by embedding the privacy needs of the user into the task at hand. The

use of recommendations, such as default button choices that hint at safer paths, can alleviate some of the challenges that make privacy self-management difficult. Although privacy management should be encouraged in the user interface to support better decisions to install safer apps while avoiding malicious ones, we need to remember that it is not a primary task that warrants the user's constant attention (Pfleeger and Caputo, 2012). Privacy self-management poses a serious concern for companies that support BYOD policies because a smartphone user's inclination is to defer privacy and security tasks onto the system; unfortunately, that system is unaware of BYOD policies and other contextual information. It is likely that users assume that the system is providing protection, therefore placement of their trust in app stores seems logical. It is also likely that they do not understand the security risks associated with sharing information. Therefore, authority is simply given to the app without any necessary validation or extra precautionary security measures (Mylonas et al. 2013). Several studies have suggested ways to communicate appropriate trust by highlighting the flaws and vulnerabilities of mobile app systems (Balebako et al. 2014; Barrera et al. 2010; Chia et al. 2012; Felt et al. 2011; Mylonas et al. 2013). We believe increased transparency supports successful risk assessments by conveying extra precautions when consenting access to personal or business data.

Acknowledgment. This research was supported by the Psychology of Design laboratory. We thank Auriana Shokrpour, Dorian Berthoud, Felicia Santiago, Jarad Bell, Michelle Gomez, and Peter McEvoy for their assistance collecting data.

References

Akhawe, D., Felt, A.P.: Alice in Warningland: a large-scale field study of browser security warning effectiveness. In: Usenix Security, pp. 257–272 (2013)

Balebako, R., Marsh, A., Lin, J., Hong, J., Cranor, L.F.: The privacy and security behaviors of smartphone app developers. In: Workshop 2014 Usable Security Experiments (USEC) (2014)

Barrera, D., Kayacik, H.G., van Oorschot, P.C., Somayaji, A.: A methodology for empirical analysis of permission-based security models and its application to android. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 73–84 (2010)

Bohme, R., Kopsell, S.: Trained to accept? a field experiment on consent dialogs. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems, pp. 2403–2406 (2010)

Chia, P.H., Yamamoto, Y., Asokan, N.: Is this app safe? a large scale study on application permissions and risk signals. In: Proceedings of the 21st International Conference on World Wide Web, pp. 311–320 (2012)

Choe, E.K., Jung, J., Lee, B., Fisher, K.: Nudging people away from privacy-invasive mobile apps through visual framing. In: Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., Winckler, M. (eds.) INTERACT 2013, Part III. LNCS, vol. 8119, pp. 74–91. Springer, Heidelberg (2013)

Cialdini, R.B., Cacioppo, J.T., Bassett, R., Miller, J.A.: Low-ball procedure for producing compliance: commitment then cost. J. Pers. Soc. Psychol. **36**, 463–476 (1978)

Egelman, S., Tsai, J., Cranor, L.F., Acquisti, A.: Timing is everything?: the effects of timing and placement of online privacy indicators. In: Proceedings of the Conference on Human Factors in Computing Systems, pp. 319–328 (2009)

Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D.: Android permissions demystified. In: Proceedings of the 18th on Computers and Communications Security, pp. 627–638 (2011)

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: user attention, comprehension, and behavior. In: Symposium on Usable Privacy and Security, pp. 1–14 (2012)

Jian, J.-Y., Bisantz, A.M., Drury, C.G.: Foundations for an empirically determined scale of trust in automated systems. Int. J. Cogn. Ergon. **4**(1), 53–71 (2000)

Jou, J., Shanteau, J., Harris, R.J.: An information processing view of framing effects: the role of causal schemas in decision making. Mem. Cogn. **24**, 1–15 (1996)

Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D.: A conundrum of permissions: installing application on an android smartphone. In: Conference of Financial Cyptography and Data Security, Workshop on Usable Security, pp. 1–12 (2012)

Kelley, P.G., Cranor, L.F., Sadeh, N.: Privacy as part of the app decision-making process. In: Proceedings of the 2013 ACM Annual Conference on Human Factors in Computing Systems, pp. 3393–3402 (2013)

Mylonas, A., Kastania, A., Gritzalis, D.: Delegate the smartphone user? security awareness in smartphone platforms. J. Comput. Secur. **34**, 47–66 (2013)

Mylonas, A., Theoharidou, M., Gritzalis, D.: Assessing privacy risks in Android: a user-centric approach. In: Proceedings of the 1st International Workshop on Risk Assessment and Risk-Driven Testing, pp. 21–37 (2014)

Pfleeger, S.L., Caputo, D.D.: Leveraging behavioral science to mitigate cyber security risk. Comput. Secur. **31**(4), 597–611 (2012)

Solove, D.J.: Privacy self-management and the consent dilemma. Harv. Law Rev. **126**, 1880–1903 (2013)

Yee, K.P.: Guidelines and strategies for secure interaction design. In: Russell, D. (ed.) Security and Usability: Designing Secure Systems that People can Use, pp. 247–273. O'Reilly Media Inc., Sebastopol (2005)