# Privacy Enhancing Technology Awareness for Mobile Devices

A. Alshehri[1], N.L. Clarke[1,2] and F. Li[1,3]

[1]Centre for Security, Communications & Network Research (CSCAN), University of Plymouth, United Kingdom;
[2]Security Research Institute, Edith Cowan University, Western Australia
[3]School of Computing, University of Portsmouth, Portsmouth, United Kingdom
e-mail: {aziz.alshehri; nclarke}plymouth.ac.uk; Fudong.li@port.ac.uk

## Abstract

Users are often unaware of what information an app is collecting about them and with the increasing number of apps can also struggle to control and manage the large volumes of personal information. Current research into privacy often has a tendency to assume that users have uniform privacy requirements to control and manage personal information. The main problem with this approach is that research has also shown that users have different privacy attitudes and preferences. It is important to factor these requirements in a privacy-awareness model that can enhance the user's awareness to make more informed decisions and to reduce their specific degree of exposure. As a result, this paper proposed an approach that considers individual requirements in a centralised and usable manner to meet users' needs. Through prioritization of privacy-related information, based on an individual user basis, is utilised to ensure relevant and timely notifications about privacy-related information that is important to the user. Accordingly, an evaluation was conducted to identify users' privacy preferences, how they wish to control different aspects of privacy and how this relates to good usability design to maximise adoption.

## Keywords

Privacy in mobile computing; Context-aware privacy control; Usable privacy

## 1 Introduction

With the rapid growth of devices, activities, services and information, an enormous amount of private and personal information is created and stored. Users are becoming increasingly concerned about their personal information, how it is used, by whom and where it is stored (Anton, Earp and Young, 2010). For instance, a Consumer Report found that 92% of British and U.S. Internet users are concerned about their privacy online (TRUSTe, 2016). Users are also concerned about lack of control over their personal information as they are often unaware of what information an application collects about them (Hajli and Lin, 2016). Due to their concerns about privacy protection, most mobile operating systems such as Android and iOS provide some privacy safeguards for users (Kelley *et al.*, 2012). However, despite these provisions, there are several usability issues related to the functionality and interface. For instance, Kelley et al.(2012) found that users struggle to understand the permissions in Android due to the lack of usability. Therefore, the Federal Trade Commission suggested that privacy controls need further improvement to protect users' privacy (Federal Trade Commission, 2013).

The focus has been given to the development of policies, procedures and tools that aid an end-user in managing and understanding their privacy-related information(Nadkarni and Enck, 2013; Bal, Rannenberg and Hong, 2014)(Bal, Rannenberg and Hong, 2014)(Bal, Rannenberg and Hong, 2014)(Bal, Rannenberg and Hong, 2014)(Bal, Rannenberg and Hong, 2014)(Bal, Rannenberg and Hong, 2014). However, these approaches assume that users can correctly configure all resulting settings and they have uniform privacy requirements. In reality, users do have different privacy concerns and requirements as they have heterogeneous privacy attitudes and expectations (Alaggan, Gambs and Kermarrec, 2015).

From a usability perspective, the user plays an essential role in controlling their personal information. Directly linked to their ability to manage privacy-related information is their awareness and knowledge of the issue. Aldhafferi et al. ( 2013) suggested that empowering users to control their personal information is essential to increasing the users' confidence in their social network providers. Therefore, a privacy enhancing solution needs to address the dual requirements of controlling the data and providing the necessary knowledge and awareness for users to make informed decisions.

Traditional solutions within the domain typically assume that users are identical in context, in terms of their prior knowledge and in how they interact with the technology. However, research has also highlighted differences between users – particularly between those that rate themselves as expert versus novice (Chua and Chang, 2016). Accordingly, there is a need for an approach that considers individual requirements in a usable manner to meet users' needs. This paper proposes a novel approach to privacy awareness and management for mobile applications that provides a tailored and individualised solution for users, taking factors such as current awareness and knowledge, the need to enhance awareness, the needs of the individual and their desires to control different aspects of privacy and good usability design to maximise adoption.

The remainder of this paper is organised into five sections. Section 2 presents an analysis of background literature. The proposed system is presented in Section 3. Section 4 presents the result of the evaluation of the proposed system. A thorough discussion of the results is presented in section 5. The conclusions and future work are presented in Section 6.

## 2 Background Literature

Numerous techniques have been proposed to monitor personal information(Agarwal and Hall, 2012; Balebako *et al.*, 2013; Enck *et al.*, 2014). The majority of existing techniques has focused upon the technical aspect to protect the privacy of users. They have shown that is possible to monitor sensitive information for users in real time. Some of the tools used a dynamic approach to monitor personal information for users. Whilst, a few studies used a network approach to detect information leakage in the mobile as shown in Table 1.

A number of research prototypes have not only monitored sensitive information for users but also provided user control over the personal information such as AntMonitor (Le et al., 2015), ProtectMyPrivacy (Agarwal and Hall, 2012) and TISSA (Zhou et al., 2011). However, most current privacy controls support only binary and static privacy controls. A few studies such as TISSA (Zhou et al., 2011) and AppFence (Hornyack et al., 2011) provided users with multiple levels of control. TISSA provides users with empty or bogus options for personal information that may be requested by the app. Whilst, AppFence provides users with two privacy controls to protect sensitive resources: shadowing and blocking. However, the tools do not allow users to limit the disclosure of their private information in multiple levels taking factors like the level of user's knowledge to make the right choice in order to reduce the burden on users.

| N | Authors | Privacy Tool | Methods | Types of controls |
|---|---|---|---|---|
| 1 | (Enck et al., 2014) | Taintdroid | Dynamic approach to track the data through four levels | No |
| 2 | (Balebako et al., 2013) | Little Brothers Watching You | Investigation users' understanding when the data is shared | No |
| 3 | (Egele et al., 2011) | PiOS | Using static analysis to detect apps leak | No |
| 4 | (Zhou et al., 2011) | TISSA | Providing users with empty or bogus options. | Finer granularity |
| 5 | (Le et al., 2015) | AntMonitor | Analysing actual network traffic of Android using VPNService API to intercept traffic | Static control |
| 6 | (Liu et al., 2013) | Reconciling Mobile App Privacy | Analyzing people's privacy preferences when it comes to granting permissions | No |
| 7 | (Agarwal and Hall, 2012) | ProtectMyPrivacy | Developing a crowdsourcing system to help the user to make informed decisions | Static control |
| 8 | (Hornyack et al., 2011) | AppFence | Providing users with two privacy controls to protect sensitive resources(shadowing and blocking) | Finer granularity |
| 9 | (Bal, Rannenberg | Styx | Providing the user with more meaningful privacy information | No |

| | | | | |
|---|---|---|---|---|
| | and Hong, 2014) | | based on the actual behaviour of apps | |
| 10 | (Almuhimedi et al., 2015) | Your Location has been Shared 5,398 Times! | They evaluated the benefits of giving users an app permission manager and of sending them nudges | No |
| 11 | (Yang *et al.*, 2013) | AppIntent | AppIntent determines if transmission is user intended or not | Static control |
| 12 | (Song and Hengartner, 2015) | PrivacyGuard | Detecting the leakage of multiple types of sensitive data and modifying the leaked information | Finer granularity |
| 13 | (Tsai et al., 2017) | Turtle Guard | TurtleGuard helps users to vary their privacy preferences based on a few selected contextual circumstances. | Finer granularity |
| 14 | (Olejnik et al., 2017) | SmarPer | Predicting permission decisions at runtime. | Finer granularity |
| 15 | (Wijesekera et al., 2018) | Contextualizing Privacy Decisions | Contextually-aware permission system that performs permission denial dynamically | Static control |

**Table 1: A review of monitoring and privacy controls**

A few studies such as (Tsai et al., 2017), (Olejnik et al., 2017) and (Wijesekera et al., 2018) used machine learning to predict user preferences. Tsai et al. designed TurtleGuard that automatically make privacy decisions on behalf of the user. Olejnik et al. also designed a system that predicts permission decisions at runtime. These studies have shown that is possible to predict user's preferences. In order to disgned initial interface, Lin et al divided users into a small number of privacy profiles, which collectively go a long way in capturing the diverse preferences of the entire population. (Liu *et al.*, 2013). However, they do not elicit user's privacy preferences in a context where they are not just about the permissions requested by an app but also about current knowledge and their desires to control different aspects of privacy and good usability design to maximise use.

However, the aforementioned privacy solutions also assume that users are the same in the context of how to use the privacy system and how to control the large volume of personal information. Whilst the current research and available literature have highlighted differences between the expert and novice knowledge in the context of using the system and the knowledge in the domain (Chua and Chang, 2016; Wisniewski, Knijnenburg and Lipford, 2017). Therefore, it is difficult for the novice user to configure a lot of settings correctly while the expert user has the ability to manage it because he has knowledge in the domain.

# 3 Preliminary Design for a Personalised Mobile Device PET

The prior literature highlighted that privacy preferences are diverse in the context of how to control privacy-related information, the level of knowledge users have about privacy, and the prioritisation of personal information. Therefore, a preliminary design is proposed in order to provide a tailored solution for users, taking factors such as current awareness and knowledge, the needs of the individual and their desires to control different aspects of privacy and good usability design.

As a result of the analysis of the problem and the current state of the art a requirements analysis was undertaken to identify what a personalised privacy awareness and management tool should comprise. Figure 1 demonstrates the four primary requirements in order to manage and enhance mobile privacy technology. However, high-level analysis resulted in the following requirements:

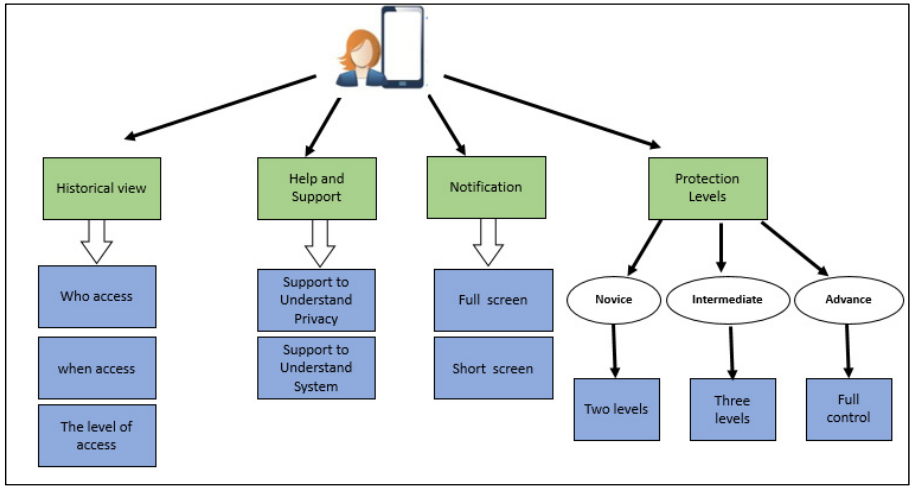



**Figure 1: Privacy management components**

- Adaptable privacy-related guidance depending upon prior knowledge and experience
- Multi-level privacy control – to provide users with a non-binary choice over privacy and thus more flexibility
- Notification support – a personalised response system to inform and control the flow of privacy-related information
- Historical auditing – to provide an overview of privacy-related information usage across apps and prior user decisions
- Prioritisation of privacy-related information.

### 3.1 Adaptable privacy

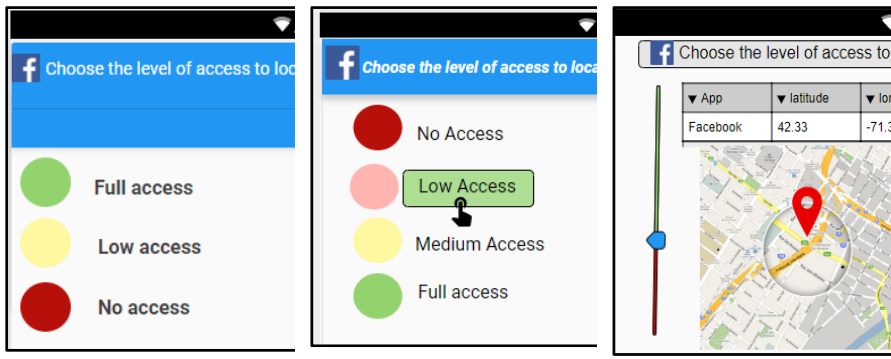
The goal of this requirement is to make the system understandable and learnable for the novice user while at the same time not hindering advance user from working productively. A novice is a user who is trying to complete the task in the system but has little or no past experience with privacy system in terms of how to manage and control a large volume of data. Therefore, they need additional help and support such as documentation, tutorial guides, and help. A novice might also need a clearer description of the alert. As the user takes more knowledge about how to use the system, the level of knowledge changes, from novice to intermediate, or from intermediate to expert; consequently the system provides the ability to automatically adapt the level of assistance and guidance provided.

### 3.2 Multi-level privacy control

A number of studies such as TISSA (Zhou et al., 2011) and AppFence (Hornyack et al., 2011) provided users with two privacy controls. However, these controls are arguably not sufficient to cater for the full range of users' needs and expectations. Therefore, the proposed system provides users with multilevel privacy controls which allow them to limit the disclosure of their private information in multiple levels taking factors the level of user's knowledge. The proposed approach suggests providing four-levels of control: full access, medium access, low access and no access. However, the full access and no access options are easy to apply because there are no modifications for the information but medium access or low access requires modification. Numerous studies have been defined methods to modify users' private information with multiple granularities across various domains (Ajam *et al*, 2010; Hornyack *et al.*, 2011). The specific information on how to apply and what these modification methods are on low and medium access settings can be determined based on the levels of access and the type of personal information. For example, the medium level for the calendar is to allow the app to access (year, month, day) while low level accesses to just (year, month). Another example, the location information can be classified into four options: full access, no access, medium access and low access. The system shares the location city in the low access level while in the medium level the system shares the approximate location if the app asks to access GPS coordinates.

As users' knowledge is different and not all users can correctly configure all settings, the proposed system allows novice users to access a minimum set of features in order to protect his privacy. For example, when the app sends the user's location out of the mobile, the system notifies the user and also provides the user with two options: allow or protected. When the user chooses to protect option, the system will display three options for the novice user: full access, low access and no access as shown in Figure 2(a). The three levels for privacy protection associated with visual icons in order to help novice users to understand each option. The three colour techniques are inspired by privacy bird system that was designed by Cranor (Cranor, Guduru and Arjula, 2006). Additionally, it is easy for the novice user to understand the privacy protection settings quickly when these settings associated with the three colours.

In contrast, the system provides the intermediate user with more options to protect the user's privacy and these options have different colours in order to assist the user to understand the function of these options and he can respond quickly as shown in the Figure2(b). Due to the advance user has more knowledge about the system, he does not need visual options to remind him about the function of each option. Additionally, he has more options to protect personal information. For example, the advance user does not only choose from the options but also can determine the longitude and latitude for location. Figure2(c) shows how the advance user has the ability to change the level of protection for the location in the Facebook app. Additionally, when the advance user changes the level of settings from the map the colour of slider will change as well to demonstrate to the advance user how the level of risk for sharing his personal information.




**(a) Novice user** **(b) Intermediate user** **(c) Advance user**

**Figure 2: Privacy protections settings for the three categories**

### 3.3 Notification support

Prior studies have highlighted that users are often unaware of what information an app collects about them (Felt *et al.*, 2012; Sarma *et al.*, 2012; Hajli and Lin, 2016). Therefore, the proposed system was designed to inform the user to receive notifications for privacy-sensitive information usage by the apps. Figure 3 shows the notification message that informs the user about ongoing privacy risks and also provides the user with mitigation options to minimize the incurred risk. It can thus improve privacy awareness and provide effective user control over their personal information. It is also important to avoid the use of technical terms in the notification which can confuse the user to understand the notification. This is particularly useful for novice users to understand what privacy notification means (Nurse *et al.*, 2011).

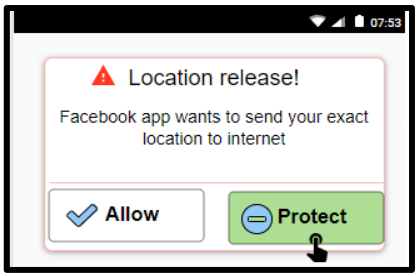



**Figure 3: A short interface notification**

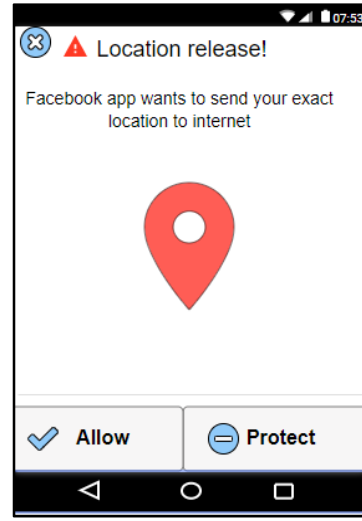



**Figure 4: Full interface notification**

A large pop-up window is another option to inform the user about ongoing privacy risks as shown in Figure 4. However, two types of notifications full-screen notification and short screen notification could be used to display the notifications. For instance, if the user is concerned about sharing the exact location with the Facebook app, the notifications would be displayed as a full-screen notification. On the contrary, a novice user is not concerned about sharing approximate location information with the Facebook app, the notifications would be displayed as a short notification.

However, the notification will be personalised according to the user's prioritisation. For instance, some users may extremely concerned about the personal information in the social media, therefore, the notification that required action from the user will be displayed the information related to social media.

### 3.4 Historical auditing

The proposed system allows users to access the date of the data that was sent out of the mobile and which app shares this data and at which degree of granularity. In order to help a novice user to understand the historical interface, the novice user could view the history of data in a high-level format without going into deep details. This allows an advance user to know who had access to which data at which degree of granularity and when without confusing the novices. The red, yellow and green colures are used in the history interface in order to allow the user to fast recognition the level of privacy when the information was shared by the app.

### 3.5 Prioritisation of privacy-related information

As seen in the literature review, privacy preferences are diverse and cannot adequately be captured by one size-fits-all default settings because the level of privacy differs from user to user. Eventually, this needs to result in a privacy profile/configuration unique to each individual. However, understanding and adapting to an individual's specific preferences is challenging without overly burdening them at the initial setup. Therefore, in order to cater to different user preferences and expectations initially, user profiling could be utilised to cluster users into a smaller number of privacy profiles. Prior studies (Zukowski & Brown 2007; Lin et al. 2014) show that is possible to cluster users into a small number of privacy profiles, which collectively go a long way in capturing the diverse preferences of the entire population.

## 4 Evaluation

This section validates the user's requirements that were mentioned in section 3 by conducting an online survey. It also discusses how to cluster the entire user population into a number of subgroups and their desires to control different aspects of privacy and good usability design in order to provide a tailored and individualised solution for users.

### 4.1 Experimental Methodology

The proposed solution was evaluated by recruiting participants via different platforms such as mailing lists, social media and community centres for three months (26th September 2018- 26th December 2018). The survey was implemented online using the Qualtrics platform. The survey was structured to cover four parts:

- Demographic: exploring the participants' demographic characteristics, including questions related to gender, age, education and occupation.
- Users' mobile app privacy preferences: it investigated how users are concerned about such privacy-related information being shared by different categories of apps.
- Privacy control and management: it presented questions related to how to control the privacy-related information
- Usability: it investigated users thoughts regarding the design of interfaces

App privacy preferences section in the survey were organised along two dimensions: app categories and data type. Hence, eight app categories associated with various data types. Therefore, there are 46 questions were asked to participants in order to cluster participants preferences into a number of subgroups. The targeted participants were public users who are 18 years or above and has a smartphone. Participants were asked how concerned they are about such privacy-related information being shared by

different categories of mobile apps on 5 points Likert scale (from extremely concerned to Not at all concerned).

In total, 407 completed responses and the total responses are within the range of other surveys in the research domain and close to the expected and targeted figure. Demographic information was collected including questions related to gender, age, education, and occupation in order to analyse the data, though the age ratio or any other demographic composition of the participants were not specifically controlled. Among these participants, 70% of them were male; 30% were female. Almost half (47%) of the participants aged 25 to 34. The second largest age group aged 35 to 44 which represent 35%. Respondents were asked questions related to mobile privacy knowledge. These questions were rated on a 5-point Likert scale ranging from "Extremely knowledgeable" to" Not knowledgeable at all". Another part of the survey includes questions about the proposed interfaces for the three categories and system functionality.

### 4.2 Results

This section presents the results of the survey that was conducted to identify the current privacy preferences, and how to manage it. One of the requirements to design the system is the need to prioritise the users' personal information. Accordingly, the result of the questions related to users' personal information shows is possible to cluster the entire user population into a number of subgroups that have similar preferences within the subgroups. Hierarchical clustering was performed to cluster participants' smartphone app privacy preferences which identify 10 clusters as shown in Figure 5.

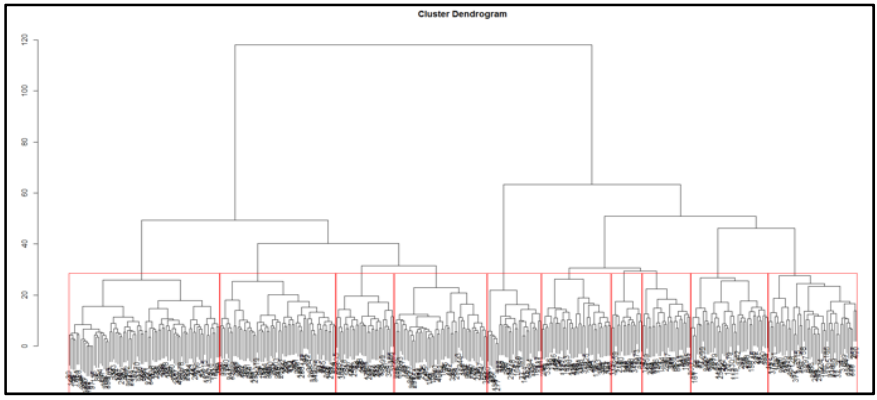



**Figure 5: The resulting dendrogram produced by hierarchical clustering**

In terms of privacy knowledge, the result shows that almost half of the participants were intermediate. Whilst 20% of them were a novice and 31% were advance users as shown in Figure 6. Regarding the question about understanding privacy settings for the apps, 26% of participants were extremely knowledgeable. The vast majority of them were advance users. On the other hand, 71% of participants who chose "Not knowledgeable at all" were novice users as shown in Figure 7.

In addition, there was a positive correlation between the level of knowledge about the privacy of apps and understanding the privacy setting for the apps ($r = 0.525$, $p < 0.000$) which means when the level of knowledge increases, the understanding of the privacy settings increases as well. Regarding the second question related to understanding the permission of apps was a positive correlation ($r = 0.524$, $p < 0.00$) as well. Additionally, The following questions that related understanding privacy policy and privacy permissions yielded statistically significant correlation as shown in Table1. The results of these questions draw attention to the fact that the users are different in term of level of knowledge and how to manage privacy settings. This, in turn, emphasises the need to classify users. Accordingly, novice users need more assistance to understand privacy settings and how to control these settings.

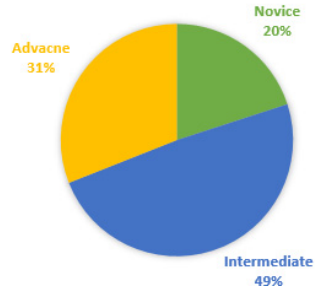



**Figure 6: The Percentage of respondents who rated themselves as novice, intermediate and advance**

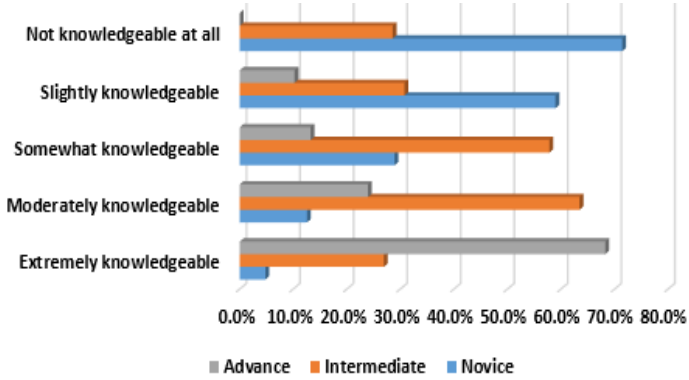



**Figure 7: Answers distribution between three levels of knowledge novice, intermediate and advance to the question (understanding privacy settings)**

Furthermore, looking at whether users' demographic information including age, gender, and education level has any correlation with the three categories(novice, intermediate and advance) in order to assign users to one of these categories. In regard to gender, the result indicates significant differences between male and female in the context of knowledge($r = -0.98$, $p = 0.04$). For the age group, the age groups were

encoded as (1= 18-24, 2= age 25-34, 3=age 35-44, 4=age 45-54, 5=above 55). A Spearman's test reveals no significant correlation between knowledge and age( r=0.96, p=0.53). a similar test on the education level of all groups of participants was also performed. The result shows that the effect of education level was a significant correlation (r=0.98, p=.04). Although there is a statistically significant correlation between education level and knowledge, This correlation is weak according to Cohen (1992) guidelines (Cohen, 1992) Table 2 shows the correlation between demographic information and the three categories (novice, intermediate and advanced) and the strength of the relationship.

| Factor | Correlation coefficient ( r ) | P-value | The strength of the relationship |
|---|---|---|---|
| Understanding permissions | 0.524 | 0.001 | Strong |
| Understanding privacy settings | 0.525 | 0.001 | Strong |
| Understanding privacy policy | 0.478 | 0.001 | Moderate |

**Table 2: the correlation between the questions related to understanding the privacy of apps and the three categories (novice, intermediate and advanced)**

| Factor | Correlation coefficient ( r ) | P-value | Strength of the relationship |
|---|---|---|---|
| Gender | -0.98 | 0.04 | Weak |
| Age | 0.96 | 0.53 | No correlation |
| education level | 0.98 | 0.04 | Weak |

**Table 3: the correlation between demographic information and the three categories (novice, intermediate and advanced)**

Regarding providing user multi-level privacy controls e.g(No access, Low access, and Full Access), 87% of participants strongly agree or somewhat agree to have this feature. The result indicates the need for providing users with more fine-grained privacy controls on mobile platforms. As mentioned earlier, the novice user can access to a few levels of privacy controls in order to avoid any confusion about how to manage mobile privacy. Furthermore, there is a statistically significant correlation between knowledge and display multi-level privacy controls. When the level of knowledge increases, the need to display multi-level privacy controls increases as well (R=-0.115, p=0.021).

Moving forward to exploring the users' thoughts regarding the design and the functionality of the interfaces, 86 % strongly agree or somewhat agree to have the ability to change privacy notification settings for different apps ($\mu$= 1.5). Regarding

the type of notifications, 56.3% of participants prefer full-screen notification. Whilst 43.7% of participants prefer the short screen.

Another requirement to help the novice user to make an informed decision for protecting his privacy is the risk impact interface. When the novice users were asked about understanding the risk impact that helps them to understand the privacy risk, the vast majority of novice users (86.7%) indicated they understood the risk impact from the interface. When the visual risk impact interface and text interface were presented to novice users, 83.1% of them chose the interface that contains visual appearance.

Specific questions were asked to investigate users' usability perspectives regarding the history interface, 81% of participants chose the interface that contains data history with colours to help the user to know who has accessed data, when and at which degree of granularity. 75 % of participants stated that the interface is excellent or very good to understand the history view. Regarding the colour of the interface, 71% of participants indicated the colour is excellent or very good. However, around 7% of all participants indicated that the colours in the interface need more improvement. One of the advance users stated in the comment the red colour affected his understanding of the interface. Most of the comments regarding history interface is about the red colour is so flashy and requires more improvement.

# 5 Discussion

The results of an evaluation are derived from a range of participants' with a variety of backgrounds in terms of gender, age, education, and level of knowledge. The outcomes from this study indicate that is possible to divide the users into 10 unique subgroups that have similar preferences in term of privacy-related information. This clearly represents a significant reduction in user burden while allowing users to better control information. Furthermore, the result of 10 clusters shows that is possible to prioritise information because each cluster has different prioritisation of information.

However, the study has also highlighted differences between users – particularly between those that rate themselves as novice, intermediate and advance. When the level of knowledge increases, the understanding of the following statements increase as well according to Spearman's test: understanding apps permissions, understanding privacy settings and understanding privacy policy. Therefore, novice user needs more help and support such as documentation, tutorial guides, and help systems. Moreover, visual aids could also help novice user to understand the system. Therefore, the evaluation of the interfaces shows novice user prefer visual aids on the interface to understand the system, in particular, the risk impact interface.

The results also show that there is a desire for adding multilevel privacy controls which allow them to limit the disclosure of their private information in multiple levels taking factors the level of user's knowledge. When the level of knowledge increases the need for multilevel privacy controls increases as well. This indicates that the binary and static techniques that are used in mobile is not sufficient to allow users to provide their private information at an appropriate level.

The result strongly indicates that equipping the solution with the push notification feature is effective for enhancing user's awareness especially for users with little experience with mobile. In addition, notification preferences are diverse because some of the participants prefer full-screen notification whilst others prefer the short screen.

# 6 Conclusion and Future Work

This paper proposed a system that considers individual requirements in a centralised and usable manner to meet users' needs. In order to meet users' needs, the survey was conducted to identify users' privacy preferences and their desires to control different aspects of privacy and good usability design to maximise use. This study shows that users are different not only in the context of prioritisation their information but also in the context of design, multilevel privacy controls, and the level of knowledge. This, in turn, emphasises the need for a holistic tailored solution for users, considering all these dimensions.

Further research could be sought to develop a holistic tailored solution for users considering all above requirements and user's privacy preferences. Then the solution will be assessed and evaluated. The goal is to look at the impact of the new approach on user trust and privacy concern because effective transparency mechanisms can increase trust in the system and reduce privacy concern.

# 7 References

Agarwal, Y. and Hall, M. (2012) 'ProtectMyPrivacy : Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing Categories and Subject Descriptors', *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, 6(September), pp. 97–110.

Ajam, N., Cuppens-Boulahia, N. and Cuppens, F. (2010) 'Contextual Privacy Management in Extended Role Based Access Control Model', in *Data privacy management and autonomous spontaneous security.* Springer, pp. 121–135.

Alaggan, M., Gambs, S. and Kermarrec, A.-M. (2015) 'Heterogeneous Differential Privacy ´', *Arxiv*, pp. 1–14.

Aldhafferi, N., Watson, C. and Sajeev, A. S. M. (2013) 'P ERSONAL I NFORMATION P RIVACY S ETTINGS OF O NLINE S OCIAL N ETWORKS AND T HEIR', 2(2), pp. 1–17.

Almuhimedi, H. *et al.* (2015) 'Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging', *Proc. of the 2015 ACM conference on Human factors in computing systems (CHI)*, 1012763, pp. 787–796. doi: 10.1145/2702123.2702210.

Anton, A. I., Earp, J. B. and Young, J. D. (2010) 'How Internet Users ' Privacy Concerns Have Evolved', *IEEE Privacy & Security*, 1936(February), pp. 21–27. doi: 10.1109/MSP.2010.38.

Bal, G., Rannenberg, K. and Hong, J. (2014) 'Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones', *29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*, pp. 113–126. doi: 10.1007/978-3-642-55415-5_10.

Balebako, R. *et al.* (2013) '"Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones', *SOUPS '13: Proceedings of the Ninth Symposium on Usable Privacy and Security*, p. 12:1--12:11. doi: 10.1145/2501604.2501616.

Chua, W. Y. and Chang, K. T. T. (2016) 'An Investigation of Usability of Push Notifications on Mobile Devices for Novice and Expert Users', in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, pp. 5683–5690. doi: 10.1109/HICSS.2016.703.

Cohen, J. (1992) *A Power Primer*, *Psychological Bulletin [PsycARTICLES*. Available at: http://www2.psych.ubc.ca/~schaller/528Readings/Cohen1992.pdf (Accessed: 15 February 2019).

Cranor, L. F., Guduru, P. and Arjula, M. (2006) 'User interfaces for privacy agents', *ACM Transactions on Computer-Human Interaction*, 13(2), pp. 135–178. doi: 10.1145/1165734.1165735.

Egele, M. *et al.* (2011) 'PiOS Detecting privacy leaks in iOS applications', *Proceedings of the 18th Annual Network & Distributed System Security Symposium, NDSS 2011*, p. 11.

Enck, W. *et al.* (2014) 'TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones', *ACM Transactions on Computer Systems (TOCS)*, 32(2), p. 5. doi: 10.1145/2494522.

Federal Trade Commission (2013) 'Mobile privacy disclosures - Building trust through transparency', (February), p. 29.

Felt *et al.* (2012) 'Android Permissions: User Attention, Comprehension, and Behavior'. doi: 10.1145/2335356.2335360.

Hajli, N. and Lin, X. (2016) 'Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information', *Journal of Business Ethics*, 133(1), pp. 111–123. doi: 10.1007/s10551-014-2346-x.

Hornyack, P. *et al.* (2011) 'These Aren't the Droids You're Looking for: Retrofitting Android to Protect Data from Imperious Applications', *In Proceedings of the 18th ACM conference on Computer and communications security*, pp. 639–652. doi: 10.1145/2046707.2046780.

Kelley, P. G. *et al.* (2012) 'A conundrum of permissions: Installing applications on an android smartphone', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7398 LNCS, pp. 68–79. doi: 10.1007/978-3-642-34638-5_6.

Le, A. *et al.* (2015) 'AntMonitor: A System for Monitoring from Mobile Devices', *Proceedings of the 2015 ACM SIGCOMM Workshop on Crowdsourcing and Crowdsharing of Big (Internet) Data*, 15(1). doi: 10.1145/2787394.2787396.

Liu, B., Lin, J. and Sadeh, N. (2013) 'Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?' Available at: http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/usr0/ftp/2013/CMU-CS-13-128.pdf (Accessed: 25 December 2017).

Nadkarni, A. and Enck, W. (2013) 'Preventing accidental data disclosure in modern operating systems', *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*, pp. 1029–1042. doi: 10.1145/2508859.2516677.

Nurse, J. R. C. *et al.* (2011) 'Guidelines for usable cybersecurity: Past and present', *Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011*. IEEE, pp. 21–26. doi: 10.1109/CSS.2011.6058566.

Olejnik, K. *et al.* (2017) 'SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices', *Proceedings - IEEE Symposium on Security and Privacy*, pp. 1058–1076. doi: 10.1109/SP.2017.25.

Sarma, B. *et al.* (2012) 'Android Permissions: A Perspective Combining Risks and Benefits', *Symposium on Access Control Models and Technologies (SACMAT)*, pp. 13–22. doi: 10.1145/2295136.2295141.

Song, Y. and Hengartner, U. (2015) 'PrivacyGuard: A VPN-based Platform to Detect Information Leakage on Android Devices', *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '15*, pp. 15–26. doi: 10.1145/2808117.2808120.

TRUSTe (2016) *2016 TRUSTe/NCSA Consumer Privacy Infographic - US Edition | TRUSTe*. Available at: https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/ (Accessed: 11 March 2017).

Tsai, L. *et al.* (2017) 'Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences', *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, (Soups), pp. 145–162. doi: 10.1017/S0953820800000650.

Wijesekera, P. *et al.* (2018) 'Contextualizing Privacy Decisions for Better Prediction (and Protection)', pp. 1–13. doi: 10.1145/3173574.3173842.

Wisniewski, P. J., Knijnenburg, B. P. and Lipford, H. R. (2017) 'Making privacy personal: Profiling social network users to inform privacy education and nudging', *International Journal of Human Computer Studies*. Elsevier, 98(May 2016), pp. 95–108. doi: 10.1016/j.ijhcs.2016.09.006.

Yang, Z. *et al.* (2013) 'AppIntent: analyzing sensitive data transmission in android for privacy leakage detection', *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*, pp. 1043–1054. doi: 10.1145/2508859.2516676.

Zhou, Y. *et al.* (2011) 'Taming Information-Stealing Smartphone Applications ( on Android )', *4th International Conference on Trust and Trustworthy Computing*, (2011), pp. 93–107.