Towards Improving Privacy Awareness Regarding Apps' Permissions

Nurul Momen
Karlstad University
Karlstad, Sweden
Email: nurul.momen@kau.se

Marta Piekarska
Technische Universität Berlin
Berlin, Germany
Email: marta@sec.t-labs.tu-berlin.de

***Abstract*—Empirical studies show that the flow of personal information through mobile apps made devices vulnerable in terms of privacy. Cumbersome and inconvenient representation of privacy notice encourages the user to ignore it and disclose sensitive private information unintentionally. Hence, summarized permissions are presented on mobile devices and users tend to overlook them as well. Rigid structure for using a service and inherited behavior from desktop applications to accept everything are the reasons behind compelling the user to proceed without paying any attention. Complex permission based structure is also a major impediment for consumers that makes it difficult to perceive appropriate consequences of their decisions. We argue that as privacy strongly depends on individual perception, the key to educate and empower users is to providing them with transparency of what is happening on their smartphones. In consequence we suggest a convenient, transparent and proactive approach to help in understanding and deciding upon privacy implications of apps. We propose a scale that has scalability within itself. We implement this method within a tool, named Aware, that presents the summary of what applications are installed on a smartphone, which resources they access, and what are the reasons for that. Moreover, the tool is capable of nudging the user when certain sensitive data is accessed.**

Keywords–Mobile Operating Systems; Mobile Phone Privacy; Control and Management of Privacy.

I. Introduction

Smartphones are part and parcel of our daily life: we carry them, store all sorts of personal data on them and even sleep right next to them. Gradually, more and more dimensions are being added to smartphones due to adoption of ubiquitous computing in many sectors. They have become a universal interface for many services operating around us. Significant amount of data is required and collected in order to maintain a real time interaction with the surrounding environment. Additionally, commercial incentives play an important role here. It allows the business entities to offer better services through consumer-centric analysis. A diverse revenue stream is generated by this large data pool for numerous businesses and users are benefited by better product recommendations. However, there is a certain trade-off introduced by giving away personal information—risking individual privacy. As installing an app has become a general solution to many of our problems, it has brought a great deal of privacy concerns. It is indeed necessary to look for smart privacy protection, for example the one that preserves good usability while protecting sensitive data.

As opposed to many other concepts, like network latency or power efficiency, privacy is a topic that is fuzzy to address. Keeping aside the technical aspects, decision making is hugely influenced by emotion, feelings and cultural background of individuals [1], which makes privacy a difficult entity to protect. The problem regarding smartphone privacy is two folded. From the technological perspective, we need to overcome lack of knowledge, transparency and simplicity. On the other hand, there are the social, cultural and psychological aspects. Moreover, depending on the person asked, the tolerance threshold will be different. Also time and context both can play vital roles behind personal preferences. Individual tolerance may fluctuate for same piece of information during variable situation and time.

In general, mobile operating systems offer a permission structure for the apps and an app gets access to user data through it [2]. Users are asked for their consents in order to proceed with the app. They are also expected to understand the consequences and make informed decisions, which is in fact very unlikely to be right [3]. Though apps require explicit consents from users, given justifications have proven to be ineffective to initiate privacy-aware behaviour [4]. Decisions are being made with misunderstanding and wrong perception about privacy implications, which lead the user to disclose privacy sensitive information unintentionally [3], [5]. It is quite alarming that the user-consent relies on usual bad practice to press the *Agree* button after scrolling down the list of permissions.

An alternative solution is required to simplify the representation of personal data usage that should have the ability to ease the decision making dilemma by offering a clear and conclusive notification with consequences. We would like to bisect the problem into two parts. First, the permission usage is provided to the user assuming that she possesses proper knowledge to understand it, which is in fact overlooked by majority. It encourages the user to ignore it and carry on without paying attention. We conduct a survey to determine user awareness regarding app permissions. Second, even if we are able to educate users in an easy to understand way, tolerance threshold varies from person to person and is non-quantifiable. We introduce a method for measuring users' preference and implement it within prototype apps in pursuance of nudging toward privacy.

Our contribution to the field has multiple facets. A theoretical method is proposed to quantify individual privacy preference for sensitive data usage on mobile phones. The method is capable of offering a flexible and easily adoptable structure. User convenience and ease of understanding are the prime benefits of it. A tool, named Aware, is introduced which is implemented on both Firefox OS and Android, to provide convenient, proactive and efficient interface for an overview of personal information usage by installed apps. Based on user preference, the app is able to produce nudges in the form of notifications.

The rest of this paper is organized as follows. the problem is outlined through a discussion of related literature in Section 2. A survey was conducted in order to realise the lack of privacy awareness, which is described in section 3. Solution

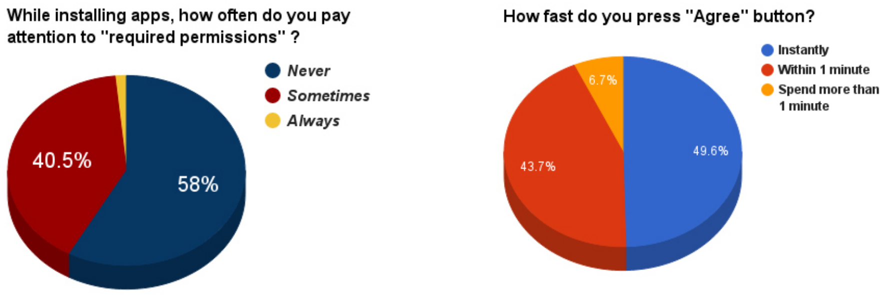

Figure 1. Statistics regarding user behaviour: a survey conducted in Berlin where N=252.

architecture and implementation strategy are described in Sections 4 and 5, respectively. Our prime observations as well as limitations are discussed in Section 6. We concluded with a forecast about future work in Section 7.

II. Related Work

Previous works have ignited several debates within privacy research arena. One of the ongoing debates is whether to introduce more control to user-interface or not [6][7]. Decision making for important private data based on a cumbersome method could result into a complete rejection from the subscribers [3]. Absence of transparency offers difficult hurdle for the user and results into lack of proper attention during decision making process [5]. Misunderstanding and lack of knowledge are often accountable for blindfolded positive consent of a user [3][5].

Privacy-unaware behaviour has the potential to result into passive expenses for the user. In [8], McDonald and Cranor presented a theoretical approach to determine the cost of sacrificing user privacy. They argued about the need for simple and usable transparency for convenient user experience. Jung et al. [9] conducted a survey on different mobile OS users and concluded that an “expectation gap” is present between perceived and actual usage of their agreed permissions. Furthermore, Acquisti and Grossklags [10] pointed out that users are more likely to sacrifice their privacy due to misperceived consequence and lack of sufficient information. Their findings indicate the shortcomings of current methods in order to make informed privacy decisions.

Felt et al. [2] developed Stowaway for investigating permissions on Android apps. They examined 940 apps and reported that one third of them are over privileged. Au et al. [11] developed PScout to analyse Android permissions and found out that 22% of the non-system entries are unnecessary. They went through several versions of Android (from version 2.2 to 4.0) and reported redundancies after examining 75 permissions. Their findings indicate the fact that personal information is being collected without informed consent of the user. Additionally, Rosen et al. [5] pointed out how difficult it can be to understand the privacy implications from an Android interface. They introduced a profile based solution to offer a better understanding by exposing behavioral statistics on privacy issues.

Several research works showed that user behaviour shifts toward positive direction by nudging [12][13]. Nudging is a gentle encouragement to a user for making decisions wisely. Though it does not prohibit users from taking any step, this tiny intervention has proven to be really helpful [14][15]. In case of mobile apps, nudging is also used as reinforcement for privacy preservation [16]. Almuhimedi et al. [17] developed AppOps based on nudging and emphasised on how many times personal data is accessed by apps. Franzen and Aspinall [18] developed PhoneWrap with similar views and proposed ticket based access for controlling permission usage. We developed Aware in a complimentary principle with a focus on spontaneous nudging.

Quantification of privacy aspects has always been challenging. Alohaly and Takabi [4] used Natural Language Processing (NLP) in this regard. Braunstein et al. [19] took user responses during pseudo situations in order to determine individual preferences. In contrast, we propose a flexible scale which is intended to be defined and controlled by users. In our prototype apps, we introduce a method to take user preferences into consideration and produce instantaneous nudges.

III. Survey

We conducted an online survey where participants could take part anonymously. The fundamental goal of this survey was to demonstrate the current scenario regarding privacy-unaware user behaviour. Though it was a subjective test and not a controlled group, the result shown in Fig. 1 depicts lack of cognisance about mobile app privacy. The survey took place during the middle of year 2015. Therefore, responders are expected to be stranger to the latest runtime permission mechanism of Android. Background knowledge of the participants was taken into consideration while selecting two particular group of users.

Within our geographically convenient grasp, we selected two subtle groups of smartphone users in this regard: 1) students from a technical university and 2) employees from an online real estate company. We used Google Form as the medium and English as the language to carry out the survey. A brief introduction in written form was given along with the survey link describing the purpose, background, requirement and motivation behind it. We intended to perform an efficient survey by not conducting an aggravating one. Thus, participants were asked only two precise questions. Moreover, only three options were given to avoid decision making dilemma. Presumably the participants understood the context and answered the questions responsibly.

A. Demography

The survey was conducted in Berlin, Germany and the participants were residing in Berlin when the survey took

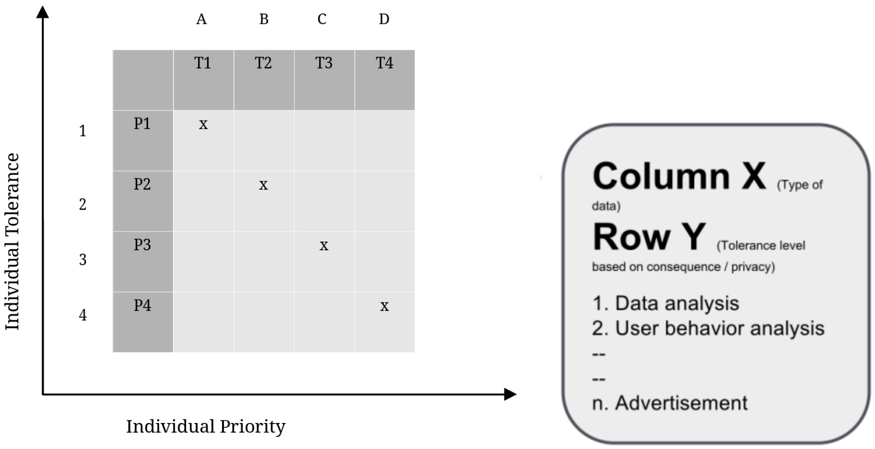

Figure 2. An instance (where columns represent data types / permissions and rows represent tolerance level) and element of the matrix solution.

place. Nonetheless, majority of the participants were expected to be internationally diverse due to the cosmopolitan nature of Berlin. During the first cycle of the survey, invitation was distributed amongst the students of TU Berlin, irrespective of their educational focus. Social media groups were used in this regard for distributing the survey request. The responders were expected to belong to their second cycle of university study. 205 responses were recorded between 08–26 April in 2015.

During the second iteration, a group of employees were requested to take part. They were working for an online real estate company named Lamudi [20]. The employee pool of this company was also internationally divergent (more than 30 different nationalities). Though they were working in different departments, all the employees were anticipated to possess substantial knowledge regarding the context of this survey. Majority of them were involved in app development, website development and data science. Presumably, they were expected to possess sublime knowledge over apps, permissions and privacy impact. Invitation was sent through a group chatting software. 47 responses were recorded between 03–31 May in 2015.

B. Result

We recorded 252 responses in total. Two brief questions were asked:

1) While installing apps, how often do you pay attention to ‘required permissions’? Options to answer: Always/Sometimes/Never.
2) How fast do you press *Agree* button? Options to answer: Instantly/Within one minute/Spend more than one minute.

We found only 1.6% responses as *Always* for the first question and 93.1% of the responding participants press *Agree* button within one minute or instantly. Presumably, a significant portion of the survey participants chose ‘sometimes’ as an answer to the first question. However, the real scenario came out by answering the second question—users hardly spend time to realize the consequences of granting permissions for an app. Despite considering an error margin, the outcome of this survey states that very few users are aware of privacy risks associated with permissions while installing an app.

C. Limitations

The survey had an uncontrolled sample at N=252. Response collection was open for a certain period of time and sample number was not taken into consideration. Also precision was missing form given options. Users could not provide precise answer to the questions. University students and employees of a company running online-based business were presumed to possess sufficient knowledge and information which leaves the possibility of having larger error margin. Regardless of international diversity, the survey lacked participants with broader age range and occupational variety.

Although our findings lack many aspects of a proper survey, a rough conclusion could be drawn from it. Though we chose two slick smartphone user groups, their answers reflected poor privacy awareness. Despite having substantial understanding of apps and permissions, privacy-unaware user behavior was observed in the survey statistics. It is indeed undiniable that broader age range, occupational and geographical diversity would enhance credibility for the survey result.

IV. Solution Architecture

By taking into account how individually defined privacy is, and how blurry the methods are that we can use to ensure respecting it, we believe that the place to start is by improving transparency. To address the aforementioned problems, we propose a theoretical solution which is based on a two dimensional matrix structure. Initially, this method was introduced in our master thesis work.

Let us consider matrix *M (m*n)*, where *m* = number of data types and *n* = number of threshold points for individuals. Depending on the granularity of a scenario, the values of *m* and *n* can be chosen. For instance, permissions are reflected as data types in implemented prototype app which is elaborated in next section. A matrix provides flexibility for the users in two different directions. Moreover, permitting the user to shuffle the columns provides an additional elasticity to the method. It allows to accommodate individually customized and prioritized privacy matrix for each user.

Column: Data types are arranged throughout the columns. Each column is accountable for signifying one particular data type. The rightmost column hosts the most sensitive data

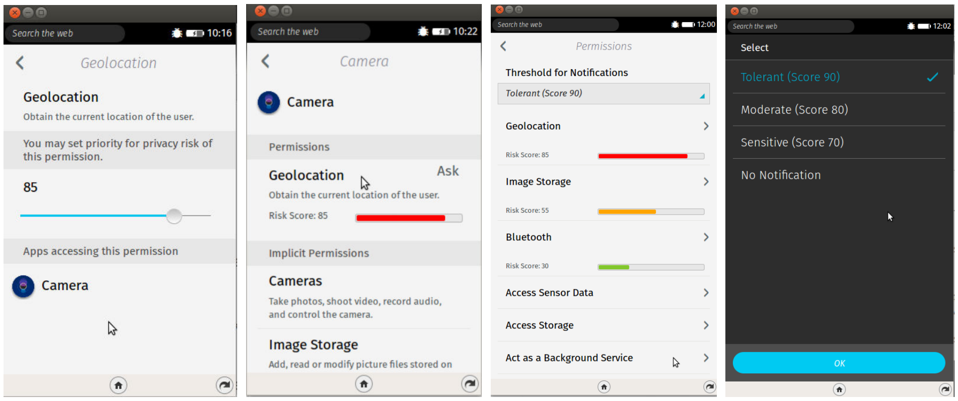

Figure 3. Interface of our prototype app on Firefox OS (from left to right): a) setting the priority for geolocation permission of camera app, b) risk score and risk bar are shown for geolocaiton permission, c) list of permissions is sorted according to user defined priority and d) setting the tolerance threshold for defining frequency of nudging/notifications.

type and the leftmost column hosts the least significant data type. User has the flexibility to rearrange default order of the columns. It allows to emphasise on individual preferences.

Row: The rows denote a personal threshold associated with each column. As the row number increases, tolerance threshold of an individual user regarding privacy decreases. Top most row (or, row 1) denotes that the user is very reluctant about the consequences. On the other hand, the bottom row (or row N) denotes her preference about certain data to be set as the most protected one. It can also be described as follows: the intersection element of the last column and last row indicates the most strict user privacy preference for the most sensitive data type.

Let us elaborate the scenario with an example, as illustrated in Fig. 2, which depicts an instance of the matrix *N (4*4)*. Personal preference of user-data or, personal priority is plotted on X axis. Y axis signifies individual tolerance. For this instance, we have four different data-types which are arranged throughout the columns (A, B, C and D) according to the preference of a user whom we can call Alice. The rightmost column signifies the most sensitive data for her. It should be noted that Alice has the freedom to shuffle the columns for changing her preferences. On the other hand, selection of rows allows to modify her own tolerance level.

Figure 2 also shows an element of the matrix. Besides knowing about data type and default tolerance level, it can describe the expected consequences within convenient description along with appropriate references. This allows the users to go in deeper explanation if they want to. It also allows them to decide upon the clauses more precisely. Moreover, users are able to revoke the settings if they do not want to agree. Suppose, Alice puts [P4, T4] as her privacy preference. This means that her tolerance level belongs to row 4 for the data type placed in column D. From an element of the matrix, Alice is able to explore more about the types of data being shared with service provider. She can also get a better idea about the consequences of sharing such data. Here, Alice has a fine grained decision making opportunity based on her own privacy preference.

It should be added that an extention to this solution has the potential to make room for enhanced decision making opportunity. In addition to partially aggreeable resolution, a temporal consent could reckon another dimension. For example, Alice may decide to put her consent after going throgh a trial period which would facilitate better understanding of any probable repercussion.

This solution is covering only the theoretical aspects of the problem. Dimensions of the matrix depend on the depth of the proposed solution. Value of a matrix element is also subject to specific scenario, which can be taken from a convenient interface. This method is partially realized during implementation. Certainly, there is opportunity to offer finer control. There is room for introducing further granularity to this scale, i.e., denial of certain clause or sub-clause and temporal acceptance. However, this would increase complexity which restrained us from coarse implementation.

V. Prototype Apps

We have implemented prototype apps on two different platforms: Firefox OS and Android. Having system privileges, these prototypes can show a list of installed apps along with the corresponding permissions, describe the reasons and allow users to set their privacy preferences depending on how they perceive the implications. Primarily, the prototype allows the users to take a look into two lists. Installed apps are given in the first one. The list can be sorted based on user-defined privacy risks. User may carry on to discover more details about any installed app. The app details option shows the list of permissions which are being used by that particular app. In the second list, all the permissions are being populated. Users can select one and find out more to be aware of consequences. Moreover, the user may choose to receive notifications for privacy sensitive information usage by other apps.

In order to highlight the privacy-sensitive applications, we introduce *Permission Priority*. It allows a user to prioritize the apps according to perceived consequence. User-defined priority for personal information depicts empowerment over individual privacy. We also introduce smart alert mechanism for certain permission usage. The prototype offers control over notification frequency. The user is in charge to decide on when to get notification and what to be notified about. We also introduce colored *Risk Bar* to improve awareness about consequences instantly through visualization.

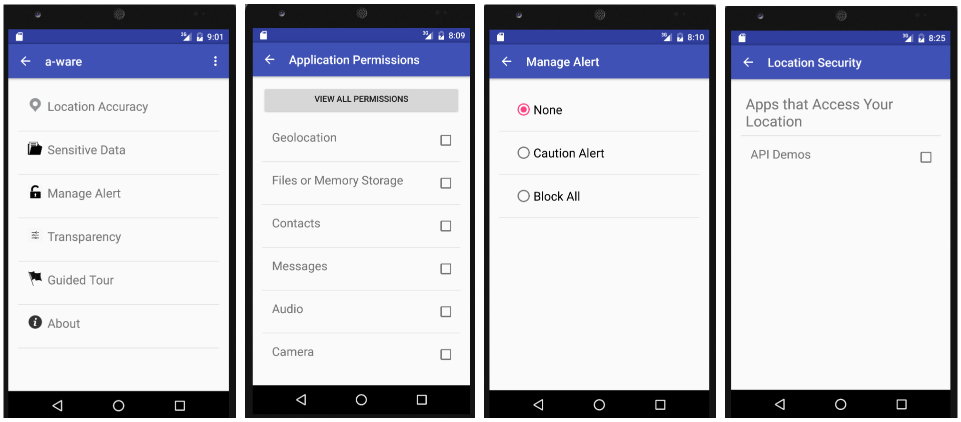

Figure 4. Interface of the prototype app on Android (from left to right): a) starting screen, b) permission list for marking nudging / notification preference, c) managing notification frequency and d) list of apps having permission to access users' location.

A. *Permission Priority*

As shown in Fig. 3 and Fig. 4, Alice can set her priority for a particular data-type which is equivalent to arranging the columns in the matrix solution. It allows to prioritize the apps according to potential risks. Additionally, she can get the summary of data types that are being accessed by an app. Also, an overview of sensitive data usage can be visualized along with their priorities. A colored risk bar helps her to be cautious by highlighting the risky permissions. It improves awareness of the consequences. It also rises curiosity to discover more in order to feel safe. Moreover, the prototype allows to set the frequency of nudges in the form of notifications. The threshold is chosen by the user. This functionality signifies the choice from rows of the matrix solution structure. Thus, Alice can choose "when" and "what" to be notified about.

The purpose of placing permission priority is to introduce a user-defined scale for privacy tolerance. Considering the theoretical matrix solution described in previous section, it symbolizes shuffling the columns through setting priority. In the detail interface of each permission, depicted in Fig. 3, we introduced a *Sliding Bar* with a range from 0 to 100. It has 20 default positions within this range which means the interval between them is 5. This scale signifies individual privacy tolerance for that particular permission. Selection of highest slider value indicates maximum privacy concern of the user.

We considered two constraints to define the scale. First, a flexible enough range is required to resolve decision making dilemma. Secondly, unexpected and fine grained transparency might result into burdensome responsibility. Thus we chose high values and less number of preference taking points in order to present an optimized solution. Chosen values are used to trigger the *notifications or, nudges*. Finally, these values are used to be visualized as the *Privacy Risk Bar*. Persuasive power of data visualization was chosen in order to achieve good practice for privacy preserving behavior. This risk bar offers a visual representation of safety zone and danger zone for privacy implications. User defined *Permission Priority* is also responsible here to define the color code: green, yellow and red zone.

For the prototype on Android, we applied a different approach to take permission priority. Instead of taking values from the range of a sliding bar, check box is placed to take users' preference.

B. *Notifications*

We introduce fine-grained transparency in our implementation. Users can get nudges or, alerts in order to be aware of privacy sensitive information being accessed. Moreover, the control to receive privacy nudges belongs to the user. It depends on the values of *Permission Priority* and user defined threshold. The notification is triggered on extreme risks (permission priority 90 or above) by default. However, users have the option to change the threshold for the notifications in order to control the frequency:

Tolerant Threshold: Notification is triggered when the current application uses a permission having user defined priority more than or equal to 90. The user is expected to receive less amount of alerts.

Moderate Threshold: Notification is triggered when the current app uses a permission having user defined priority more than or equal to 80. The user is expected to receive moderate amount of alerts.

Sensitive Threshold: Notification is triggered when the current app uses a permission having user defined priority more than or equal to 70. The user is expected to receive frequent alerts.

No notification: We understand that nudging can be annoying sometimes for a user. If this option is chosen, no alert will be triggered.

VI. Discussion

Firefox OS provides descriptive and cumbersome representation of privacy policy during the installation of an app [21]. Users are expected to go through lengthy text. It compels a user to ignore and carry on without paying any attention. Lack of knowledge makes the situation even more difficult for users to perceive proper implications. Additionally, individual emotion and judgment can play pivotal roles behind decisions regarding privacy. This is where we identify the requirement of personalized scale for convenient individual decision making. An alternative is required to simplify the representation of privacy policy which should have the ability to ease the decision making dilemma by offering a clear and conclusive notification with consequences. In comparison with the current scenario, our prototype app is eligible to offer a solution to the aforementioned problems.

Android offers a much better representation of permission usage on a mobile phone [22]. Considering Android Lollipop (version - 5.1.1) and the previous two versions, a summarized permission list is provided during installation. However, users do not have any other alternative but to accept all of them. This rigid structure encourages a user to proceed without putting further thoughts on privacy implication. The latest version (6.0.1) of Android, Marshmallow, introduced runtime permission structure. In this case, user-consent is required while a user is using the app. It is indeed convenient for the user to understand the permission structure. Our prototype is able to complement the current scenario by adding notification for certain permission usage.

Our observations have pointed out that lack of awareness is a big impediment for preventing invasion of personal data. Additionally, individual privacy remains vulnerable to unintended disclosure due to lack of proper knowledge. Often users remain uninformed about disclosing sensitive information. Misconception regarding consequences is usually responsible for privacy-unaware behavior. Absence of easy to use tools and complex representation of permission usage play pivotal roles behind these bad practices. Sometimes subscribers are compelled to compromise their personal information in order to use certain services. It is hard to convince them to use a proactive approach while only rigid binary options are provided. As a result, users tend to ignore the privacy notice which leads to uninformed decision making and unintentional disclosure of private information. Our two main observations are: (1) individual preference cannot be taken into a stiff framework, and (2) flexible transparency and personalized tolerance scale are required in order to design user friendly tools.

VII. Conclusion

Our prime objective was to help users by keeping them informed about privacy implications. In order to do so, we developed prototype apps capable of nudging. However, user preference was not taken for granted. The prototype allows a user to choose the type and frequency of nudges. As the design of apps relied on a scalable method, it can stretch resilience to accommodate individual preferences. It also allows the user to have personalized scale to determine their preferred boundaries for receiving nudges. We developed two prototype apps named 'Aware' for the Firefox OS and Android. In Aware, the user can assign priorities to each permission in order to define her tolerance threshold. Our implementation depicts proof of concept for the theoretical solution. Both apps are capable of providing privacy overview of a phone. Instant notification relieves the user from worrying about disclosing privacy worthy data. As our implementation work contained privacy threat detection only, we intend to address privacy protection in our future work. Our plan also contains empirical studies to measure usability, effectiveness and to achieve proven viability for the prototypes.

References

[1] S. Ang, L. Van Dyne, C. Koh, K. Y. Ng, K. J. Templer, C. Tay, and N. A. Chandrasekar, "Cultural intelligence: Its measurement and effects on cultural judgment and decision making, cultural adaptation and task performance," Management and organization review, vol. 3, no. 3, 2007, pp. 335–371.

[2] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 627–638.

[3] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013, pp. 3393–3402.

[4] M. Alohaly and H. Takabi, "Better privacy indicators: A new approach to quantification of privacy policies," in Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), 2016.

[5] S. Rosen, Z. Qian, and Z. M. Mao, "Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users," in Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013, pp. 221–232.

[6] S. Patil and J. Lai, "Who gets to know what when: configuring privacy permissions in an awareness application," in Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2005, pp. 101–110.

[7] A. Acquisti, I. Adjerid, and L. Brandimarte, "Gone in 15 seconds: The limits of privacy transparency and control," IEEE Security & Privacy, vol. 4, no. 11, 2013, pp. 72–74.

[8] A. M. McDonald and L. F. Cranor, "Cost of reading privacy policies, the," ISJLP, vol. 4, 2008, p. 543.

[9] J. Jung, S. Han, and D. Wetherall, "Short paper: enhancing mobile application permissions with runtime feedback and constraints," in Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2012, pp. 45–50.

[10] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," IEEE Security & Privacy, vol. 2, no. 2005, 2005, pp. 24–30.

[11] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, "Pscout: analyzing the android permission specification," in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 217–228.

[12] R. Balebako, P. G. Leon, H. Almuhimedi, P. G. Kelley, J. Mugan, A. Acquisti, L. F. Cranor, and N. Sadeh, "Nudging users towards privacy on mobile devices," in Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion, 2011.

[13] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, N. Sadeh, Y. Agarwal, and A. Acquisti, "To deny, or not to deny: A personalized privacy assistant for mobile app permissions," FTC PrivacyCon, 2016.

[14] A. Acquisti, "Nudging privacy: The behavioral economics of personal information," Digital Enlightenment Yearbook 2012, 2012, pp. 193–197.

[15] T. C. Leonard, "Richard h. thaler, cass r. sunstein, nudge: Improving decisions about health, wealth, and happiness," Constitutional Political Economy, vol. 19, no. 4, 2008, pp. 356–360.

[16] H. Fu, Y. Yang, N. Shingte, J. Lindqvist, and M. Gruteser, "A field study of run-time location access disclosures on android smartphones," Proc. USEC, vol. 14, 2014.

[17] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal, "Your location has been shared 5,398 times!: A field study on mobile app privacy nudging," in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 2015, pp. 787–796.

[18] D. Franzen and D. Aspinall, "Phonewrap-injecting the how often into mobile apps," in Proceedings of the 1st International Workshop on Innovations in Mobile Privacy and Security co-located with the International Symposium on Engineering Secure Software and Systems (ESSoS 2016). CEUR-WS.org, 2016, pp. 11–19.

[19] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys: measuring privacy without asking about it," in Proceedings of the Seventh Symposium on Usable Privacy and Security. ACM, 2011, pp. 15–29.

[20] "Lamudi website," Jan. 2016. [Online]. Available: http://www.lamudi.com/

[21] "Firefox operating system: App permissions," https://developer.mozilla.org/en-US/docs/Archive/Firefox_OS/Firefox_OS_apps/App_permissions; [Online; accessed 15-October-2016].

[22] "Android system permissions," https://developer.android.com/guide/topics/security/permissions.html; [Online; accessed 15-October-2016].