



**UNIVERSITY OF
PLYMOUTH**

**A Privacy-Enhancing Framework for Mobile
Devices**

By

Aziz Abdullah Alshehri

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Engineering, Computing and Mathematics

August 2020

COPYRIGHT STATEMENT

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

Copyright © 2020 Aziz Alshehri

Acknowledgements

First and foremost, all praise and gratitude are due to Allah the All-Compassionate and All-Merciful for everything He has provided me throughout my life, in general, and for giving me the potential and patience to persevere and reach this stage of my PhD research, in particular. Without Him, I would not have achieved anything or even existed.

I also owe a debt of gratitude to my beloved parents for their considerable encouragement and support, and passionate love and prayers for my success even though I have fallen short of being worthy of all what they do and have done for me. Any success that might be resulted, hopefully, should help me make them proud and happy of me. May Allah reward them the best.

My unreserved love, thanks and appreciation must go to my wife (Nadiah) and children (Raghad, Ahmad, Rima and Anas”) who have been very patient, understanding, and inspiring to me throughout this endeavour, spending days, nights, and sometimes even holidays without me. Hope that the potential success of this research will compensate some of what they have missed. May Allah bless them.

I should not forget my dear siblings who have been always supportive to me whenever I am in need and without any reservation. Many thanks to them.

This thesis would not have been completed on time without the invaluable guidance, wholehearted support, timely feedback and utmost professionalism from my Director of Studies Professor Nathan Clarke. I would like to express my special thanks and admiration to him. It has been really a pleasure and an incredibly rewarding experience to work with him and I am looking forward to continuing doing so in future. Thanks must also go to my other supervisor: Dr Fudong Li who has spent a lot of time and efforts proofreading papers and my thesis, in addition to providing helpful advice throughout my studies.

I would like to thank all my friends and colleagues, either in the UK or in the KSA, who have contributed positively towards my progress by any means even if it was just a smile. Many of them deserve mentioning but it is difficult to state all the names.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without the prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

This study was financed with the aid of a scholarship from the Kingdom of Saudi Arabia - Royal Embassy of Saudi Arabia Cultural Bureau in London.

Publications:

1. Alshehri, A., N. L. Clarke, and F. Li. "A holistic framework for enhancing privacy awareness." 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018.
2. Alshehri, A., N. L. Clarke, and F. Li. "Privacy Enhancing Technology Awareness for Mobile Devices", International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019).

Word count of main body of thesis: 43,366 words

Signed:

Date:.....

Abstract

A Privacy-Enhancing Framework for Mobile Devices

Aziz Abdullah Alshehri

The use of mobile devices in daily life has increased exponentially, leading to them occupying many essential aspects of people's lives, such as replacing credit cards to make payments, and for various forms of entertainment and social activities. Therefore, users have installed an enormous number of apps. These apps can collect and share a large amount of data, such as location data, images, videos, health data, and call logs, which are highly valuable and sensitive for users. Consequently, the use of apps raises a variety of privacy concerns regarding which app is allowed to access and share; to what degree of granularity, and how to manage and limit the disclosure of this data. Accordingly, it is imperative to develop and design a holistic solution for enhancing privacy on mobile apps to meet users' privacy preferences.

The research design in this study involved an attempt to address the problem in a coherent and logical way. Therefore, the research involved different phases, starting with identifying potential user requirements based on the literature, and then designing a participatory study to explore whether the initial requirements and design meet users' preferences, which in turn led to the design of a final artefact. Design science requires the creation of a viable artefact for the current problem in the field. Thus, this study reviews the current use of privacy technologies and critically analyses the available solutions in order to investigate whether these solutions have the capability to meet personal privacy preferences and maximise users' satisfaction. It is evident that most of the prior studies assume the homogeneity of privacy preferences across users, yet users' privacy preferences differ from one user to another in the context of how to control and manage their data, prioritisation of information, personalised notifications, and levels of knowledge. Moreover, solutions with a user interface designed according to the users' perceptions and based on HCI principles are not readily available. Therefore, it is paramount to meet and adopt user's need and requirements to enhance privacy technology for mobile apps.

A survey of 407 mobile users was undertaken to discover users' privacy preferences. The outcome of the survey shows that it is possible to prioritise information into 10 unique profiles. Each profile effectively represents a cluster of likeminded users and captures their privacy-related information preferences. The outcomes of the analysis also revealed that users differ not only in the context of prioritisation of their information, but also regarding design, protection settings, responses, and level of knowledge. This, in turn, emphasises the need to develop and design a holistic solution for users, considering all these dimensions.

As such, the thesis proposes a novel framework for enhancing privacy technology in a modular and robust manner that would support such a system in practice. This system provides a comprehensive solution that has been developed by considering different dimensions, and it includes a personalised response, prioritisation of privacy-related information, multilevel privacy controls, and also considers users' varying levels of knowledge. As a result, this approach should enhance users' privacy awareness and meet their needs to protect their privacy. Additionally, the proposed of the system consists of user interfaces designed according to the users' perceptions and based on HCI principles to overcome the usability issues without compromising the users' convenience. Ultimately, the evaluation of the effectiveness of the proposed approach shows that it is feasible and would enhance privacy technology as well as user convenience. This, in turn, would increase trust in the system and reduce privacy concerns.

Contents

1.	Introduction.....	1
1.1	Introduction.....	1
1.2	Research Aims and Objectives.....	3
1.3	Thesis Structure.....	4
2.	Technology and Privacy	7
2.1	Introduction.....	7
2.2	Conceptions of Privacy and the Value of Privacy	7
2.3	Mobile Privacy Usage and threats	9
2.4	Heterogeneous Privacy.....	20
2.5	Current Privacy Control on Mobile Devices.....	22
2.6	Conclusion	25
3.	Literature Review of mobile device-Related Privacy.....	27
3.1	Mobile Applications	27
3.2	Discussion.....	56
3.3	Conclusions.....	61
4.	Research Methodology	63
4.1	Introduction.....	63
4.2	Positivism versus interpretivism.....	64
4.3	Qualitative versus Quantitative.....	65
4.4	Inductive Versus Deductive.....	66
4.5	Design Science Research Methodology.....	67

4.6	Method Adopted for the Current Research	70
4.7	Questionnaires Design	74
4.8	Data Collection	77
4.9	Data analysis	78
4.10	Evaluation.....	82
4.11	Conclusion.....	82
5.	Requirements Analysis for Profiling Users’ Privacy Information	85
5.1	Initial requirements analysis	85
5.1.1	Prioritisation of privacy-related information	86
5.1.2	Adapting privacy to the user’s knowledge	87
5.1.3	Fine-grained privacy controls	88
5.1.4	Transparency feature.....	88
5.2	Methodology	89
5.2.1	Privacy related information categorisation	89
5.2.2	Privacy-related information Questions	92
5.3	Analysis of the Results	97
5.3.1	Demographic.....	98
5.3.2	Users’ Average Preferences and Their Variances	99
5.3.3	Privacy Profiling	102
5.3.4	Possible Ways to Assign Privacy Profiles	113
5.4	Conclusions	117
6.	Requirements Analysis for Privacy usability	120

6.1	Introduction.....	120
6.2	Usable Interface Design Literature.....	120
6.3	Initial Interfaces	126
6.4	Survey Methodology	136
6.5	Analysis of the Results.....	141
6.6	Conclusion	146
7.	Design and Development of a Privacy-Enhancing Framework for Mobile Devices .	149
7.1	Introduction.....	149
7.2	Essential Requirements	149
7.3	Enhancing Privacy Technology Architecture	155
7.4	Privacy Enhancing Technologies Interfaces	162
7.5	Evaluation of the Proposed Approach.....	174
7.5.1	Experts	177
7.5.2	End-Users.....	183
7.6	Conclusion	185
8.	Conclusions and Future Work	188
8.1	Achievements of the Research.....	188
8.2	Limitations of the Research Project	189
8.3	Suggestions and Scope for Future Work	190
8.4	The future of mobile phone privacy	191
	References.....	192
	Appendix A – Ethical Approval (User Survey).....	215

Appendix B: User survey consent.....	227
Appendix C: User survey	228
Appendix D – Consent Form for the System Evaluation.....	246
Appendix E –Ethical Approval for the System Evaluation (End-Users).....	248
Appendix F – End Users Questions for the System Evaluation.....	260
Appendix G– Experts Questions for the System Evaluation.....	261
Appendix H –Ethical Approval for the System Evaluation (Experts)	262

List of Tables

Table 2.1: The GDPR data protection principles.....	9
Table 3.1: A review of prior studies approaches and solutions.....	57
Table 4.1: The Differences between Qualitative and Quantitative Research.....	66
Table 4.2: Design Science and its Applications in This Research.....	72
Table 4.3: The Strength of the Relationship.....	81
Table 5.1: Data Group.....	91
Table 5.2: App categories and data types.....	93
Table 5.3 Summary of Respondents' Demographic Characteristics.....	98
Table 5.4: Clustering Error.....	103
Table 5.5: The Accuracy of Predicting Users' Preferences.....	105
Table 5.6: The Agglomerative Coefficient for Different Dissimilarity Methods.....	106
Table 5.7: Average of Each App Category and Data in Each Cluster.....	109
Table 5.8: Cluster Ranking With the Average.....	110
Table 5.9: The Correlation between Understanding the Privacy of Apps and the Three Categories.....	112
Table 5.10: The Correlation between Demographic Information and the Level of Knowledge	113
Table 5.11: Distribution of Demographic in each User Group.....	114
Table 5.12: The 13 Most Important Questions.....	115
Table 6.1: Nielsen 10 Usability Heuristics.....	121
Table 6.2: HCI-S Criteria.....	123
Table 7.1: Private Information Modified at Various Levels.....	158
Table 7.2: Characteristics of Interface.....	163
Table 7.3: Expert Participants' Background.....	175

List of Figures

Figure 2.1: Permissions dialog that Includes only This Time Option.....	22
Figure 2.2: App Permissions in Android.....	23
Figure 2.3: Example Purpose String	24
Figure 3.1: Example of Privacy Settings.....	32
Figure 3.2: Users Can Release Location Data at Different Degrees of Granularity	33
Figure 3.3: Users Can Release Pictures at Different Degrees of Granularity	33
Figure 3.4: History Interface	34
Figure 3.5: Four Level Approach.....	35
Figure 3.6: Main Visualisation Screen of Privacy Leaks.....	37
Figure 3.7: Antmonitor System Overview	41
Figure 3.8: Pop-Up Showing That a Recommendation is Available	44
Figure 3.9: Architecture of the Labyrinth System.....	46
Figure 3.10: Visual Security Configuration on iOS.....	47
Figure 3.11: Colour Coding for One Attribute – Birthday.....	53
Figure 3.12: The main solution approaches	59
Figure 4.1: Information Systems Research Framework.....	68
Figure 4.2: Research Processes	73
Figure 5.1: Average User Preferences	100
Figure 5.2 Variances in User Preferences	102
Figure 5.3: Average of Each Cluster.....	104
Figure 5.4: The Resulting Dendrogram Produced by Hierarchical Clustering	107
Figure 5.5: Visualisation the Clusters Result in a Scatter Plot.....	108
Figure 5.6: The Percentage of Novice, Intermediate and Advance.....	111
Figure 5.7: Answers Distribution between Novice, Intermediate and Advance to the Question (Understanding Privacy Settings)	112
Figure 5.8: Feature Selection Methods	115

Figure 5.9: The Results of Accuracy from SVM Algorithm	116
Figure 5.10: The Results of Accuracy from Different Algorithms.....	117
Figure 6.1: The Small Icon in the Status Bar	127
Figure 6.2: Short Interface Notification	128
Figure 6.3: Full Interface Notification.....	128
Figure 6.4: Three Levels Privacy Protections Settings.....	129
Figure 6.5: Four Levels Privacy Protections Settings	130
Figure 6.6: Four Levels of Privacy Protections Settings Sliders	131
Figure 6.7: Graphic User Interface	132
Figure 6.8: Text-based interface.....	133
Figure 6.9: Historical View Interfaces with Colours.....	134
Figure 6.10: Historical View Interface White and Black Colours.....	135
Figure 6.11: The Participants' View on Icons and Colours.....	143
Figure 6.12: The Participants' View on Understanding the Interfaces.....	144
Figure 6.13: Experts' Opinions about Understanding the Interfaces.....	145
Figure 6.14: Experts' Opinions about How Easy to Use Interfaces	145
Figure 6.15: Experts' Opinions about All Interfaces.....	146
Figure 7.1: Mobile Privacy Awareness framework.....	156
Figure 7.2: Adaptive Interface Components.....	158
Figure 7.3: Location Information Representation at Medium level	159
Figure 7.4: Ten-Privacy Profiles	161
Figure 7.5: User Registration Interface	165
Figure 7.6: Novice Dashboard.....	166
Figure 7.7: Advanced Dashboard	168
Figure 7.8: Sending Notification According to the Importance of Data in Cluster 9.....	169
Figure 7.9: Control the Priority of the Alert.....	170
Figure 7.10: Risk Impact Interface	171
Figure 7.11: App Settings Interface.....	172
Figure 7.12: Novice and Advance App Settings	173

Figure 7.13: Historical Interface for Novice User.....	174
Figure 7.14: Historical Interface for Advanced User.....	174

Chapter One

Introduction

1. Introduction

1.1 Introduction

The number of unique mobile phone subscribers has increased dramatically over the last few years, from 4.4 billion in 2014 to 5.4 billion in 2019, and is anticipated to reach 5.86 billion by 2025 (Internet Growth Statistics, 2019). Mobile apps are used in daily life to, for example, connect with friends, order food, send money, check emails, and play games. It has also led individuals, companies and governments to rely heavily upon on mobile phones for accessing and storing financial, medical and business information that is considered is sensitive and valuable. Therefore, the enormous amount of private and personal information that is stored on mobile technology has increased. Hence, users are becoming increasingly concerned about their personal information that is stored by these applications (Anton et al., 2010), and studies indicate that users can take responsibility if they know how their information is being used online (TRUSTe, 2016).

Regarding privacy control, Brandimarte et al. (2012) found that when users have control over their personal information, they are willing to share more. Users are also concerned about lack of control over their personal information due to often being unaware of what information an application collects about them (Hajli and Lin, 2016). These findings highlight the need to provide users with more control over their personal information, which in turn would increase trust and encourage them to share more and reduce privacy concerns.

The problem is further magnified as users are now in possession of an ever-growing number of apps that deal in large amounts of data. Furthermore, the Information Commissioner's office indicates that it is undesirable to present a user with large privacy information or a large number of requests (CIO, 2013). Therefore, it would be difficult for the average user to assert control over such large amounts of data. The problem is exacerbated when it comes to privacy-related information preferences where the most current solutions assume that

privacy-related information preferences are the same and can be captured by a one-size-fits-all approach. Whilst, Madden et al. (2013) indicate that users' privacy-related information preferences differ from user to user, there is another dimension to preferences highlighted by Wisniewski et al. (2016) regarding existing users' expertise, which is a key factor in educating users so that they can take appropriate privacy protection measures (Wisniewski et al., 2016). However, the current solutions and tools still suffer from not accommodating novice but expert users. Therefore, there are various aspects of user preferences and desires regarding privacy that current solutions and tools are still far from meeting.

Due to their concerns about privacy protection, most mobile operating systems, such as Android and iOS, provide some privacy safeguards for users. However, Kelley et al. (2012) found that users struggle to understand the permissions in Android due to the lack of usability. Also, several studies have shown that privacy interfaces, whether for iOS or for Android, do not provide users with sufficient information or control (Felt et al., 2012; Gerber et al., 2016; Kulyk et al., 2016). The Federal Trade Commission (FTC) suggests that privacy controls need more improvement to protect users' privacy (Federal Trade Commission, 2013). The aforementioned studies also indicate that current operating mobile systems suffer from several issues related to usability, and reflect an essential connection between usability and privacy.

Accordingly, it is not realistic to assume homogeneous privacy preferences and requirements across whole users. Therefore, it is paramount to explore current users' privacy preferences in the context of usability, privacy control, prioritisation information and the level of users' knowledge in order to allow users to dynamically change their preferences and meet their needs without overly burdening them. This, in turn, emphasises the need for a holistic solution for users, considering all these dimensions on mobile devices. The term "mobile device" has been used to convey varying meanings in different contexts, mainly with reference to the technology of wireless devices though. Authors across relevant literature

appeared to have used the term to mean “mobile phone”. This is, perhaps, because the mobile phone is the most common example of a wireless mobile device. Accordingly, this research would use the term “mobile device” to refer to “smartphones”. Although the mobile phone is the focal point of this study, the research outcome is intended to be applicable to all mobile devices.

1.2 Research Aims and Objectives

This research builds upon the current use of privacy technologies and the available solutions in order to explore whether these solutions have the capability to meet personal privacy preferences, enhance privacy technology and maximise user satisfaction. Key to answering this question is to better understand the nature of the technologies and services users utilise, in order to develop an understanding of what privacy-related information means for users (in terms of its identification and impact), and how best to interact with such information in order to inform and react.

In order to achieve this, the following research objectives have been established:

- To identify and understand the potential privacy concerns that users have across the internet, social media, mobile devices and the internet of things.
- To review the privacy techniques and solutions available to protect users’ information and reduce their concerns across a range of platforms, including computers and mobiles.
- To explore users’ privacy-related information preferences in order to develop a new technique to manage and prioritise a large volume of information on mobile devices.
- To investigate end-users’ perceptions and attitudes towards usability in order to develop usable and adaptive interfaces that maximise user satisfaction.
- To develop a novel and holistic framework that will enhance privacy technology on mobiles to meet users’ privacy preferences.

- To design mobile privacy awareness interfaces that exemplify the enhanced privacy technology framework to better understand how the architecture would work in practice.
- To conduct an evaluation of the aforementioned model to determine its effectiveness.

1.3 Thesis Structure

This thesis is organised into eight chapters and each chapter address the particular objectives as follows:

Chapter 1 introduces the research problem and outlines the overall research objectives and the structure of this thesis.

Chapter 2 provides background information about the concept of privacy and how users value it within their technology use. The chapter continues by providing an overview of the potential privacy concerns that users have and how they are perceived in different applications.

Chapter 3 presents a comprehensive literature review of current privacy solutions for mobile applications, participatory sensing, web applications and social networks. This chapter concludes with a discussion on identifying the gap that exists in the literature.

Chapter 4 provides an overview of the research methodologies, including highlighting the philosophical systems and paradigms of scientific research. It also presents and discusses the specific research methodology adopted in this research.

Chapter 5 demonstrates the design of the initial requirements based on prior studies in order to enhance privacy technology and meet users' privacy preferences. The initial requirements have been utilised in the survey to verify and explore the current privacy preferences regarding the prioritisation of privacy-related-information and how to manage it. Moving

forward, the outcomes of the survey are discussed in this chapter, which in turn involves an analysis of how to cluster the entire user population into a number of subgroups.

Chapter 6 sets out the design of the initial interfaces based on Human-Computer Interaction (HCI) principles to overcome the usability issues without compromising the users' convenience. The initial interfaces have been used to investigate the end users' perceptions and attitudes towards usability in order to develop usable and adaptive interfaces that maximise user satisfaction.

Chapter 7 builds upon the knowledge resented in Chapters Five and Six to develop a novel privacy technology framework that considers current privacy preferences, followed by detailed practical architectural specifications designed in a modular and robust manner. The chapter then presents Mock-Up interfaces to prove that the concept of the proposed framework would work in practice. It also provides a focus group evaluation conducted with two separate groups (experts and end-users) in order to investigate users' acceptance of, and satisfaction with, the proposed approach.

Finally, Chapter 8 summarises the conclusions arising from the research, and highlights its achievements and limitations. Future research and developments related to this project are also suggested.

Chapter Two

Technology and Privacy

2. Technology and Privacy

2.1 Introduction

This chapter provides background information on the concept of privacy and how users value it within their technology use. The chapter continues to provide an overview of the potential privacy concerns that users have and how they are perceived in mobile applications. Therefore, the first section discusses the emergence of privacy in digital information and how it is important to protect privacy. The second section proceeds to discuss the impact of information technology on user privacy, and the consequences of privacy violations on these technologies. Additionally, it presents the potential privacy concerns that users have and how they are perceived. The third section explores the concept of heterogeneous privacy to highlight and the point that users have different privacy concerns and requirements. The final section describes some of the privacy safeguards available for users on mobile platforms.

2.2 Conceptions of Privacy and the Value of Privacy

The concept of privacy, in general, exists in various topics such as the media, digital data communication, and bodily privacy. However, with the increasing collection and storage of digital data, information privacy has become a majorly important issue now (Anton et al., 2010). Therefore, it is essential to highlight the concept of information privacy and how important it is to individuals. From a historical viewpoint, in 1968, Westin defined privacy as "*the right to select what personal information about me is known to what people*" (Westin, 1968). Although this concept refers to non-digital data, it can be extended to digital information. This definition enhances the concept of autonomy and the protection of human rights. Autonomy is a core value of privacy, which allows the user to make independent decisions according to his or her ideals (Levin and Abril, 2009). Therefore, Laas-Mikko and Sutrop (2012) indicate that the primary task of privacy with

respect to the individual is to protect his or her autonomy. Protecting autonomy represents the deep need to develop a self-identity and an individual lifestyle (Michelfelder, 2001).

Regarding the right to control access, Altman (1977) defines privacy as “*selective control over access to the self*”. Moreover, Himma and Tavani (2009) see privacy as “*control and self-determination over information about oneself and over the access to one’s personal affairs*”. Similarly, Fuchs shows that privacy is based on human action and users may choose to prevent or disclose a lot of information about themselves (Fuchs, 2011). In this case, privacy is variable, dynamic, and flexible, depending on individual action and choice. Because the concept of privacy is based on individual action, empowering users to control their personal information is an important feature. Furthermore, control over personal information may be seen as a state that enhances personal growth.

Subsequently, internet privacy ought to be an integral part of fundamental human rights. As such, a number of developed countries have adopted broad laws intended to protect individual privacy. For example, in 2016, the European Union’s General Data Protection Regulation (GDPR) adopted new legislation on data protection (European Commission, 2016). The GDPR specifies six data protection principles that everyone must follow when collecting, processing and storing personal data. These principles identify the lawful purposes for utilising users’ data, as shown in Table 2.1.

The new law enhances users’ privacy and requires companies to be more transparent, provide users control over their personal data, and such data can only be gathered legally under strict conditions, for a legitimate purpose (Allen and Overy, 2016). However, as technology constantly changes, these laws may not adequately protect users’ privacy. Therefore, technological solutions will play an important role in order to protect individual privacy.

Principle	Description
Lawfulness, and transparency	processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
Data minimisation	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate
Storage limitation	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes
Integrity and confidentiality	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing

Source: (European Commission, 2016)

Table 2.1: The GDPR data protection principles

2.3 Mobile Privacy Usage and threats

The mobile applications collect and process a large amount of data that is really valuable and sensitive to users. Therefore, it is imperative to study these aspects, and to explore potential privacy concerns and threats. Understanding users' concerns about their privacy would help designers and researchers to develop more effective solutions. Moreover, solving privacy concerns will enhance users' acceptance of the technology.

A mobile application typically has direct access to different sensor information and a variety of private information residing on smartphones, such as device ID, call information, location, calendar events and photographs. Amongst the most popular platforms are Android and Apple's iOS. However, Android and iOS are quite different in how they manage privacy. The App Store on iOS is a centralised, curated marketplace for downloading iPhone applications and it inspects apps in order to check whether the apps follow the privacy guidelines of the Apple company or not. While there are several

marketplaces for Android users to download applications (Chin et al., 2012). In order to protect users' privacy on Android, Google has included app permissions that allow users to selectively grant or restrict permissions for installed apps (Felt, Egelman and Wagner, 2012). Unfortunately, some permissions on Android may cause potential risks for users. For instance, the user has no choice to grant access only to permissions that are related to the functionality of the app. The problem is exacerbated when the user is unaware of what permissions mean and the lack of information on the risk of permissions confuses the user with regard to determining whether to install the app or not (Kraus et al., 2014). Thus, it is difficult for an average user to determine what data is at high or low risk. Felt et al. (2012) recruited 308 participants from among Android users to answer an online survey regarding Android permissions, and they found that only 17% of the participants paid attention to permissions during installation, and only a minority of users demonstrated both awareness of permission warnings and reasonable rates of comprehension.

In addition, some apps may contain advertising, especially because advertising on apps is an essential revenue source for developers. The apps that contain advertising have an embedded specialised code called advertising libraries, or ad libraries, which often require permission in order to collect private information such as network connectivity and location information (Lin et al., 2014). Pearce et al. (2012) found that 49% of Android applications contain at least one advertising library. Advertising libraries over-privileged 46% of the applications. Moreover, 56% of the applications with advertisements requested permission to access the users' location (34% of all applications) (Pearce et al 2012). This study indicates that many advertising libraries often request sensitive permissions, or permissions not related to the application's functionality. Therefore, advertising libraries allow applications to track the user's location without their knowledge.

Another privacy threat on mobile devices is related to the exposure of information in sensors, because modern mobile phones come with a rich set of embedded sensors such as an accelerometer, digital compass, gyroscope, GPS, microphone, and camera. Several studies have emphasised that there are privacy concerns from personal sensing applications (Iachello et al., 2006; Klasnja et al., 2009). One of the concerns is regarding accessing the sensor information that can include the recording of intimate discussions, photographs of private scenes, or tracking a user's path and monitoring the locations they have visited (Christin et al., 2011). Iachello et al. (2006) examined privacy concerns regarding the audio capture of conversation and they found that users were concerned with the potential misuse of their recordings by third parties. In addition, Raij et al. (2011) focused on the concerns of users whose conversation episodes may be inferred without any recording of the audio, such as an innocuous respiration sensor. Furthermore, Klasnja et al. (2009) examined privacy concerns when participants are using a physical fitness system and found that 42% of the participants had concerns about GPS being recorded all-day, every day. Although there are many advantages of using GPS on mobile devices, for instance, GPS allows users to search for the nearest restaurants, having one's location constantly sensed can enable an unwanted person to learn where and when a user spends their time. Furthermore, users may simply be uncomfortable with others knowing their location (Klasnja et al., 2009).

Moreover, several health applications, such as Hospital Information Systems (HISs), Electronic Medical Record (EMR) systems, Clinical Decision Support Systems (CDSSs), and so on, collect personal information from sensors (Ventola, 2014). Therefore, many studies have examined sources of concerns about informational privacy and the confidentiality of health-related information. Chin et al. (2012) found that users are less willing to perform tasks that involve sensitive data such as health records on their phones compared to their laptops, because the users were more concerned with privacy on their

phones than on their laptops. Therefore, access to health information by some applications without the user's knowledge could reduce their trust about using these health applications.

Shopping applications also have direct access to sensitive information such as credit card number and expiration date, which represent sensitive information for users. Chin et al. (2012) interviewed 60 participants and found that smartphone users are concerned that using mobile payments could put their financial and personal security at risk. Therefore, participants are significantly less willing to make shopping purchases on their smartphones than on their laptops. This result highlights that there is a difference between users' behaviour on mobile phones and laptops regarding the privacy issue. Therefore, it is important to protect the users' privacy on these applications in order to increase their trust in mobile shopping online.

When it comes to multimedia content, taking and sharing photographs or videos has become easier with mobile devices and high-bandwidth mobile networks. Moreover, several studies have shown how multimedia content is sensitive or valuable to users. Muslukhov et al. (2012) found that some of the participants consider photographs and videos on mobile phones as both sensitive and valuable. Therefore, disclosing this information could cause confidentiality to be at risk. Moreover, another study conducted by Ben-Asher et al. (2013) surveyed 465 smartphone users and found that multimedia was ranked by 60% of the respondents as sensitive, and they fear unauthorised access, which will violate their privacy.

Mobile web browser can access personal information, often referred to in the literature as Personally-Identifying Information (PII). PII includes a visitor's behaviour on a website, contact numbers, login credentials and credit card information, which is critically important to users. As a result, numerous studies have already highlighted many of the

online privacy concerns that have arisen (Chung and Paynter, 2002; Anton, Earp and Young, 2010; Zhao, 2015). These concerns include whether personal information can be collected by websites without consent, or whether third parties can track a user's browsing activity across a website. With the increase in online shopping, cloud computing and social networks, there has been an increase in individuals' level of concern about information (Yaprakli and Unalan, 2017).

One of the essential concerns of internet users is regarding sharing their information with third parties for marketing or other purposes without permission, or even having their details published on the Internet (Sipior, Ward and Mendoza, 2011). In order to collect users' data, many websites employ cookies. These are small amounts of information used by a website and stored on the user's computer in order to identify users and capture the user's preferences when using a particular site. As a result, websites may share personal information such as gender, age, buying preferences, or even the user's email address, with a third party. Therefore, the GDPR requires each company in the EU to gain explicit consent from online users before collecting any personal data (European Commission, 2016). Despite the fact that obtaining consent has been utilised widely in many companies, there many issues still exist, for instance, the collection of personal information from social media that is connected to a web page. Ali et al. (2018) have shown that some social networking profiles are connected to cookies, allowing the social networking profile to know the viewing habits of some users. Moreover, online users may be unaware of how to make informed consent, and not fully understand the facts, implications and consequences of an action (Politou et al., 2018). Due to these concerns regarding using cookies, 27% of online users in the world use an adblocker tool to disable all unwanted tracking or delete cookies (Statista, 2018). The outcomes of these studies emphasise that the tracking of users' activities in the browser would raise privacy concerns, especially when the users' profiles can be connected to their identity.

Search engines are another tool on the web browser which collect personal information about users such as their IP address, cookie-based unique ID, the time of the user's visit, personal interests, search histories, and the links that users choose, through the most important tools for finding information like Google, Yahoo, and Microsoft Live Search. Arguably, users' personal information has to be collected and analysed to provide users with the relevant result that meets their intention. However, malicious servers may intercept and alter search engine requests in order to change the links that appear alongside a result. For example, one study found 349 malicious servers that were modifying content inflight (Ross and Maltz, 2011). However, intercepting communications is prohibited in many countries. For example, the law in the UK, the Regulation of Investigatory Powers Act (RIPA), prohibits the interception of communication without the user's knowledge (Regulation of Investigatory Powers Act, 2012).

Due to search engines storing personal data related to a user's private life, disclosing of this information by these applications could cause a serious issue for users. For instance, in 2006, twenty million queries made by 658,000 users of the AOL search engine were released (Romero-Tris et al., 2015). In 2018, 500,000 users' accounts were breached in Google+ which allowed attackers to access the personal details of users (zdnet, 2018). These incidents show that Web Search Engines (WSEs) are not always capable of protecting users' privacy. Arguably, despite these tools having many advantages for users, they may pose a privacy threat to users due to storing past searches submitted by each user.

Personal information in online patient health records is another concern for users. For instance, one study showed that 100% of patients would like to know and be able to control their health information because they are concerned about the sharing of that health information (Caine et al., 2015). Moreover, when patients find out that their health

data has been revealed to third parties, many feel this violates their privacy. Hence, some patients may avoid healthcare or withhold data from physicians due to privacy concerns (Appari and Johnson, 2010). This indicates that the patients' desire for more transparency and more privacy control over their health information.

In general, these studies highlight that users are concerned about a wide range of privacy issues regarding the type of information being shared without their knowledge and who has access to it. Therefore, this section draws attention to the need to reduce these privacy concerns in the web browser.

Online Social Networks (OSNs) allow users to share personal information, photographs, videos, and opinions (Statista, 2016). Therefore, it is important to understand how personal information is used on OSNs and how OSNs vary in their levels of privacy.

Indeed, the personal information that can be stored on OSNs varies from site to site. For example, the profile of the user on Twitter contains some personal information such as date of birth, current address, and telephone number(s). Whilst some sites such as Hobbyearth and LifeKnot encourage users to provide more information about themselves such as hobbies, favourite cars or movies and relationship status.

Numerous privacy risks exist in these networks, such as privacy violations, identity theft, fake accounts and sexual harassment (Fire et al., 2013). Some of the threats specifically target users' personal information such as relationship status, date of birth, school name, email address, phone number, and even home address. Using personal information allows an attacker to create a new account or use the information from employee profiles in order to establish trust over time. It has been reported that 1.5 million fake Facebook accounts were on sale during February 2010 (Richmond, 2010). Fake accounts can be used for different reasons, for example, to spread misinformation and rumours, to attract new followers that can later be spammed, or waste an OSNs advertisement customer resources

by making them pay for online ad clicks or impressions from or to fake profiles (Cao et al., 2012). Many researchers have addressed the risk from the fake account that could be spam (Fire, Gilad and Elovici, 2012; Krombholz, Merkl and Weippl, 2012; Yang et al., 2016). Fire et al. (2012) have presented an algorithm for identifying fake profiles and spammers using the social network's own topological features. They evaluated their methods using three directed OSNs - Academia.edu, Anybeat, and Google+ and they detected 46%, 33% and 32% of the profiles were considered spammers. The outcomes of this study reveal high percentages of fake and spammer profiles across the various social networks.

Another purpose of using fake accounts is that attackers can use the victim's personal information to ask the user's friends for assistance – typically in the form of transferring money to a bank account. The Sunday Times revealed that Abigail Pickett is one such example, where someone in Nigeria had hijacked her account on Facebook and used her account to send requests for money to her network of friends on the pretext that she was “stranded” (McGinnes 2010).

Healthcare can use social media to potentially improve health outcomes and interact with patients. The social media site QuantiaMD found that 65% of physicians use these sites for professional reasons (Ventola, 2014). Therefore, some social media sites may store health information about physicians and patients. Patients can connect with each other around common problems and share relevant health data using Health Social Networking Sites (HSNS). Although many benefits exist from sharing personal health information, such as information about diagnosis and treatment, it also presents risks; for instance, disclosure may negatively affect relationships, job opportunities, and insurance options (van der Velden and El Emam, 2013). Some social networks may send health information to third parties without the explicit consent of the information owner. Li indicates from an analysis of the end-user license agreement that checkMD websites

(<http://www.checkMD.com>) may disclose users' personal information to its business partners and other third parties (Li, 2013).

These risks increase when users are children because they are more exposed and vulnerable than adults (Fire, Goldschmidt and Elovici, 2013). Therefore, there are also threats that intentionally and specifically target younger users of OSNs. For example, an Internet predator may pretend to be a friend of an innocent young boy or girl through whom he collects personal data. Wolak et al. (2010) found that most victims of Internet-initiated sex crimes were teenagers (aged 13 to 17).

Another privacy issue is related to the exposure of multimedia content on OSNs. Users may not typically be careful when disclosing and sharing multimedia content, revealing a lot of sensitive information. For example, a Microsoft survey noted that 70% of recruiters in the US have not accepted candidates due to information, including photographs, that they found on the Internet (Stuart J. Johnston, 2010). Users may share photographs of houses, concerts, vacations, and so on, which indicates that the house is 'open' to thieves (Ilia et al., 2015). Therefore, some users may be unaware of the implications of their actions on social networking sites.

In addition, most social networking sites, such as Facebook and Twitter, allow users to keep others aware of their location at all times, which is not an issue in itself, but this information may be misused and could pose many potential threats to users who share their locations with a large number of users. Several studies have demonstrated that it can be easy to identify a person's location from a social network (Humphreys, Gill and Krishnamurthy, 2010; Mao, Shuai and Kapadia, 2011). Mao et al. (2011) demonstrated that classifiers can be trained to identify Twitter users' locations in real time. Additionally, Humphreys et al. (2010) found that 20% of Twitter tweets examined included information on when people were engaging in certain activities, and 12% of the tweets mentioned the

person's location. Although users can derive benefits from sharing where they are in public and when, disclosing their location may raise concerns about who has access to the location. However, protecting users' privacy may help them to gain the benefits from sharing information through social media while protecting them from unwanted exposure.

When it comes to the Internet of Things (IoT), the mobile device can create a very smart environment using smart devices. Connected with mobile applications enable users to control these devices remotely. Some applications of the IoTs require access to sensitive information in sensors such as the user's movements, habits and interactions with other people (Rose, Eldridge and Lyman, 2015). For instance, sensor data (e.g., accelerometers and gyroscopes) can send data to healthcare systems in order to evaluate and improve gait or physical activity levels. Another example is AutoWitness system, which can also track location and movement patterns by using sophisticated tracking algorithms (Guha et al., 2012). These examples demonstrate that some IoT applications can gain access to sensitive information related to dietary habits, psychosocial stress, addictive behaviours (e.g., drinking), exposure to pollutants, social context, and movement patterns (Raij et al., 2011). Therefore, IoT applications may reveal sensitive information about users' daily lives.

Accordingly, some studies have focused on understanding the privacy concerns emerging from sensory data, such as location traces, while others studies have focused on new privacy concerns that emerge from the disclosure of measurements collected by wearable sensors. For instance, AutoSense, an experimental unobtrusive wearable sensor, can be worn for weeks in order to collect important information such as electrocardiogram, respiration, accelerometer, temperature, and skin conductance data. This information can be unique and should not be shared with others due to fear of unknown threats to privacy (Raij et al., 2011).

One of the particular technologies in IoTs that needs more consideration regarding privacy is wearable technologies, as they are among the fastest-growing segment of IoTs (Thierer, 2014). According to CCS Insight, the wearables market is set to treble in size over the next five years and grow from 84 million units in 2015 to 245 million units in 2019 (Insight, 2019). However, there are already many types of wearables available, such as smartwatches, fitness trackers and eyewear (Nguyen, 2016). The impact of wearable technology is evident in many areas such as education, entertainment, and healthcare. Wasik (2013) states that the wearables revolution could take shape much faster than the mobile revolution that preceded it.

Moreover, wearable technologies collect and store a large amount of data - they do not store only a user's personal information, but also data on how they live their lives and their current location. Consequently, wearable devices will and do store more uniquely personal properties than the broader IoTs. Therefore, these technologies raise a variety of privacy concerns regarding how the wearable devices collect information about users, how long the data be retained for, and who else might have access to that information (Jamie Carter, 2014).

Some wearables devices such as Google Glass and the Narrative clip-on camera allow users to automatically take snapshots of their daily activities every 30 seconds (Liu et al., 2016). Other types of wearable devices such as Butterfleye, Autographer, and CA7CH Lightbox, allow users to snap pictures at regular real-time stages (Page, 2015). Because these real-time tools and activities collect and store sensitive information, disclosing this information may cause the user's privacy to be at risk. Therefore, others studies have highlighted various privacy issues related to surreptitious footage and sound recordings that can be sent to the cloud and distributed without the subjects' knowledge or consent using this aspect of the technology (Talebi et al. 2016; Page 2015). Moreover, Motti and Caine (2015) found that users have different levels and types of privacy concerns, such

as privacy for augmented reality systems and surveillance concerns among Google Glass users. They indicate that the variety of concerns about wearable devices depends on the type of wearable they use (Motti and Caine 2015).

In general, prior studies have revealed that mobile phone users have a variety of concerns due to the diversity of data stored on these devices, which include (but is not limited to) payment information, personal information, patient information and multimedia content. The problem is further magnified as users are now in possession of an ever-growing number of apps that deal with a rich set of embedded sensors, which in turn increase their concerns.

2.4 Heterogeneous Privacy

Different studies have highlighted that users' privacy concerns are varied, for instance, Sheehan (2002) found that users with lower levels of education are less concerned about their privacy online than users with a higher level of education. Another study demonstrated that there is a significant correlation between level of education and privacy concerns (Lin et al., 2014). They found that users with higher levels of education are more concerned about their privacy. This means that education level could be one of the factors that affects users' privacy preferences.

In terms of age, one study found that older age groups tend to be more concerned about privacy on Facebook than younger users (Kezer et al., 2016). Another study found that older teen social media users are significantly more likely to share some types of information on their profile than younger teens (Madden et al., 2013). These studies indicate that there is relationship between age and concerns over the level of privacy. Moreover, it is apparent that the variation in privacy requirements is not only between elderly and young users but also exists between those of the same age group.

From a national perspective, Wang et al. (2011) focused on the citizens of three countries and explored American, Chinese and Indian social networking site (SNS) users' privacy. They found that American respondents were the most privacy concerned, followed by the Chinese and Indian respondents. However, the US sample exhibited the lowest level of desire to restrict the visibility of their SNS information to certain people (e.g., co-workers). The Chinese sample presented higher concerns regarding disclosure of their identity on SNS. Another study conducted by Krasnova and Veltri (2010) found that German users are often more worried about their privacy than American users because German users expect more damage and attribute higher probability to privacy-related violations on Facebook, such as the sharing of Facebook information with employers or governmental agencies (Krasnova and Veltri, 2010). Therefore, it can be deduced that the level of privacy also varies from country to country. Hence, Zhang and Zhao claim that it is unrealistic to assume homogeneous privacy requirements across the whole population (Zhang, Nan and Zhao, 2007).

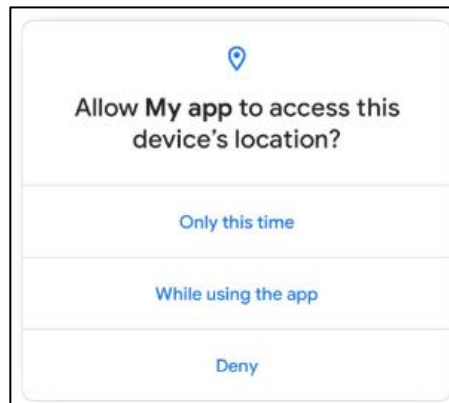
Furthermore, the differences in attitudes towards privacy may be due to differences in the data types, as many studies have emphasised that the users' preferences regarding privacy-related information are varied, and the level of privacy for individual users may change according to the type of data (Liu, Lin and Sadeh, 2013; Lin et al, 2014; Watson, Lipford and Besmer, 2015). Benisch et al. (2011) added another dimension that makes privacy preferences different, which is time. They discovered that users' preferences vary with time of day, and day of the week, and they found slightly greater preferences for sharing locations during the evening. Apple also added a feature that allows users to share their location for a period of time with someone. This feature helps the user to choose a specific person to know where he or she is without the need to call and ask (Apple, 2016).

The aforementioned studies highlight that users have different levels of privacy concerns and requirements because factors vary, such as age, level of education, legislation, and

country of residence (Alaggan, Gambis and Kermarrec, 2015). Hence, privacy preferences are diverse and it cannot be assumed that users have uniform privacy preferences across all populations.

2.5 Current Privacy Control on Mobile Devices

Due to users' concerns about the privacy protection related to mobile devices, most mobile operating systems such as Android and iOS provide some privacy safeguards for users. Android 6.0+ system displays an app requests permission at runtime, rather than at install time. In Android 10, Google introduced a new feature of the runtime permission, which allows the user to grant access only while the app is in active use as show in Figure 2.1. However, this option only works the for the location permission. In Android 11, Google offers users more fine-grained control over other permissions such as camera and microphone access called only this time. When the user selects this option in the dialog, the system allow the app to access the data for once time. Next time when the app needs similar permission again, it will have to ask for it.



(Android, 2019)

Figure 2.1: Permissions dialog that Includes only This Time Option

In order to view and manage all app permissions at once is from the privacy and safety options in the settings, where the user can see a list of different categories of permissions, along with the number of apps installed that have access to that permission as shown in

Figure 2.2. Categories include Body Sensors, Calendar, Camera, Contacts, Location, Microphone, Phone, SMS, Storage, and some additional permissions. App permissions allow users to block any app permissions of certain apps on an Android mobile device, as well as grant permissions that the app is allowed to use.

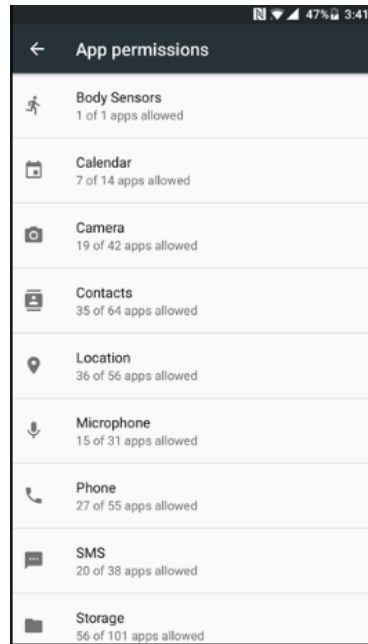
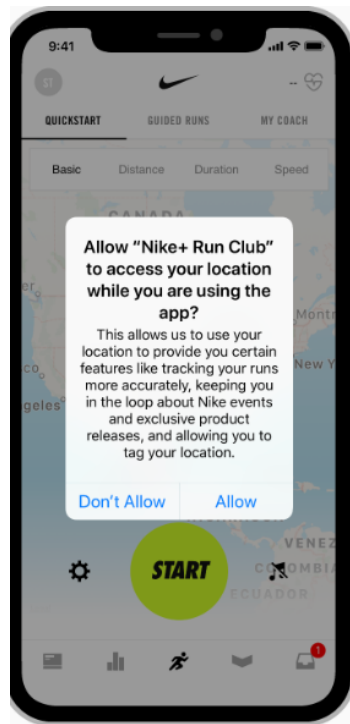


Figure 2.2: App Permissions in Android

iOS also allows users to manage their permissions. By default, an app cannot access certain user data until the user explicitly grants it. For instance, when the Facebook app wants to access the camera to upload pictures, iOS shows a notification to the user to allow Facebook to access the camera. Moreover, some iOS apps display a notification with a short description citing the purpose of the location access as shown in Figure 2.3. In order to show this message, the users need to go to the location services setting to view it. This feature is not very useful because the purpose of the location access will not pop-up by default when the app asks for the location access.



(iOS, 2019)

Figure 2.3: Example Purpose String

iOS also has privacy settings centre similar to Android settings. However, Egele et al. (2011) analysed 1,400 iOS apps and they found that many iOS apps leaked sensitive information from a mobile device to third party. This shows that iOS permissions are not sufficient to protect users' privacy because some apps may abuse these privileges. For instance, some apps may ask the user for access to their location even though that is not related to the functionality of the app. Moreover, privacy control on iOS does not provide users with information about who has access to their data. For example, once permissions are granted to an app, they may share data such as location, with a third party without informing the user. Therefore, privacy control is severely limited.

Furthermore, Walters (2014) demonstrated that users struggle to understand who has access to their data, what use is made of that data, and who has the right of access to the information (Walters, 2014). Therefore, prior studies have indicated that privacy control on mobile devices are not sufficient to protect the user's privacy. Due to these concerns, the Federal Trade Commission (FTC) has suggested that privacy controls need further

improvement to protect consumers' privacy, and they recommend that companies adhere to three primary principles: Privacy by Design, Simplified Consumer Choice and Greater Transparency (Federal Trade Commission, 2013).

2.6 Conclusion

Numerous studies have highlighted that users are more concerned about their privacy on the Internet, mobile applications, IoTs and social networks. These concerns include who has the right to access their information, when, where, and how it is accessed. In addition, users prefer to maintain strict control over the disclosure of their information, which some mobile applications provide in one way or another, but to a limited extent. However, some users are unaware of those tools and options. In addition, the tools that are provided by applications are not sufficient to meet the expectations and needs of users. Another finding from the aforementioned studies indicates that the level of the privacy is different from user to user because of numerous factors, such as age, level of education and culture. Additionally, a single change in context can trigger a change in privacy preferences. Therefore, it is essential to find ways of improving privacy options for users, particularly when it comes to sensitive data such as health, location and financial details.

Chapter Three

Literature Review of Technology-Related Privacy

3. Literature Review of mobile device-Related Privacy

Having established that users have concerns regarding different types of applications on a mobile device and that the level of concerns varies from user to user, it is imperative to explore the current solutions that can help to protect users' data and meet their privacy preferences, as this should lead to alleviating users' privacy concerns. Accordingly, this chapter presents a comprehensive review of the literature through exploring and investigating the literature on current privacy solutions for the mobile device. In recent years, many studies have been published on ways of protecting users' privacy, because privacy issues exist wherever personal information or sensitive information is disclosed. This chapter concludes with a discussion identifying the gap that exists in the literature.

3.1 Mobile Applications

Researchers have proposed many solutions in order to protect the privacy of users. Some of these solutions focus on sensing that is used by the mobile device. The majority of existing works on sensing rely on centralised servers and often involve cryptography to secure and anonymise data to protect the privacy of users. AnonySense is one of the participatory sensing systems that aims to anonymise participants' information (Cornelius et al., 2008). This is a comprehensive system for realising pervasive applications based on collaborative, opportunistic sensing by personal mobile devices. The system opportunistically sends the task to mobile nodes that choose to participate for sensing the physical and network environment around them. The mobile device retrieves tasks and submits reports through an anonymity preserving protocol. In this case, users cannot be identified within a group of users assumed to reside in the same place at the same time. This method helps to protect the user from inference attacks aimed at linking reports back to that user. For more protection, they designed a second layer that collects user reports before submitting them to the campaign administrator. In order to preserve their

anonymity, they used group signatures; cryptography schemes that enable users to anonymously sign their reports. However, using this anonymity technique in order to protect user privacy by hiding any identifying information, can threaten the trustworthiness of the system because it permits dishonest users to access the service. Moreover, the user should be more aware of the risk of revealing his or her personal information to this system.

Another solution that also uses cryptography to protect the privacy of users is Privacy Enhanced Participatory Sensing Infrastructure (PEPSI) (Cristofaro and Soriente, 2013). This is a new scheme that has been designed to protect the privacy of both data producers (i.e., mobile nodes) and data consumers (i.e., queriers). PEPSI is based in a centralised server and has been designed to protect the privacy of queries. These queries are sent to the user, who is interested in some specific sensing information. Moreover, PEPSI leverages Identity Based Cryptography. In that sense, the queries arrive at the mobile nodes in an encrypted form. Then, the client device sends reports of sensed data to the service provider, which acts as an intermediary between queriers and mobile nodes. After some processing, the service provider delivers the reports to the queriers. However, PEPSI hides the reports of sensed data and queries from unconcerned entities, and reports and queries are all encrypted. In this case, no entity can learn any information about the sensed data reported by mobile nodes. The only entity that is able to decrypt the report is the querier. However, PEPSI does not ensure privacy against the network operator before forwarding the report to the service provider because this system trusts the network operator to remove sensitive data from reports and does not provide users with control over their personal data.

To increase the trustworthiness of the collected data, Kazemi and Shahabi have proposed Trustworthy privacy-aware participatory sensing participate (TAPAS) (Kazemi and

Shahabi, 2013). This framework collects data from multiple participants to increase the validity of the collected data. The more participants that send information to the data collection process, the higher the trustworthiness of the collected data is. The system allows multiple participants assigned to each DC-point (data collection point). The server contains the list of DC-points; therefore, each participant can query the server for the locations of close by DC-points. In order to protect the participant's privacy, instead of sending their exact location, participants blur their location in a cloaked area among other participants, from which a subset of them (i.e., by utilising the voting mechanism) are selected as representatives to send cloaked regions to the server. Consequently, a malicious server cannot identify each individual participant by linking his query to the query location.

Other solutions do not rely on a centralised server, such as Privacy Enhancing Protocol for PaRticipatory sensing (PEPPeR) (Dimitriou, Krontiris and Sabouri, 2012). The PEPPeR system allows queries (mobile nodes) to have access to the data provided by participating users without the need to connect to a centralised server. The PEPPeR system aims to protect the privacy of queriers, by letting them obtain tokens from the service provider in order to have access to the data provided by participating users. The queriers can spend the token with any producer (mobile phone user) directly, but before that, the producer has to validate the token and then provide the querier with the proper amount of requested data. The token reveals no information about either the querier or the desire of the querier - the service provider just provides the token to participant. When the querier receives the token, the querier can directly contact the mobile user for data (producer). After the producer receives the token, the producer directly validates the token and then provides the querier with the proper amount of requested data without leaking the identity of the querier to the node or to the application owner. In order to know if the token has been used before, the producer will contact the witness service to attest to the

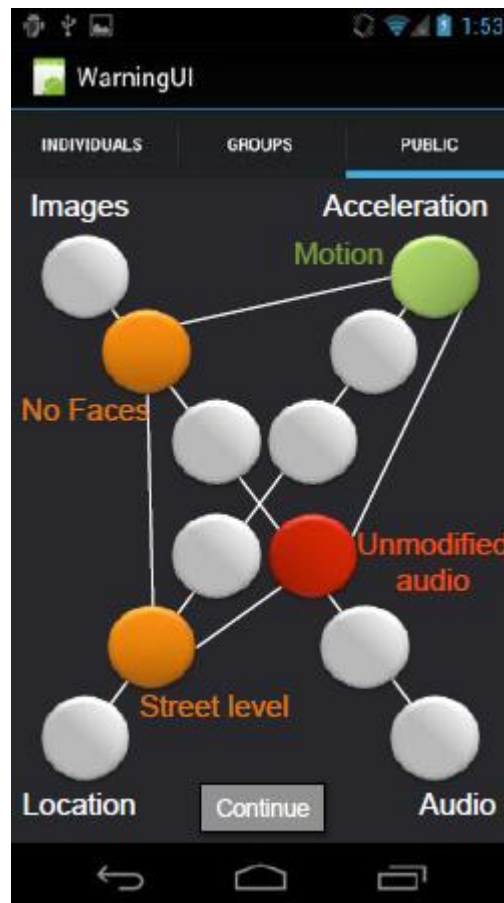
validity of the token or provide proof that the token has been used before. The final step, when the producer is convinced that the token is valid, is for the producer to provide the data requested by querier. Consequently, when the querier contacts the service provider, the system should not leak any information about the identity of the authorised querier.

A similar concept is discussed by Boutsis and Kalogeraki (2013). They propose LOcAtion-based middlewAre for TrajEctory databases (LOCATE). The system does not necessarily rely on a central server to generate and store data sensing. Instead, LOCATE allows users to locally sense and store data. The framework focuses on the participatory data that contain locations. There are many transportation applications, such as MetroSense and VTrack, which allow users to share their local traffic observations. For instance, users may submit queries in the form “*Give me the trajectories from location A and B in real time*”. In this case, all members of the community sense and contribute data to the system. The data contains the locations that a user has visited and his or her trajectories. The framework provides privacy preservation for participatory sensing systems on Android-based devices. Users can store data locally, as well as submit queries across the system. The data that is stored on the user’s local database is represented as set of the tuples. Each tuple consists of six forms of information: latitude, longitude, time stamp, point type and id trajectory. The Id of the trajectory is a unique id from among all the tuples from different trajectories. The unique id is produced through a cryptographic hash function that utilises the timestamp and the id of the user. In order to preserve the privacy, each tuple is separated from its producer (user) because it would be relatively easy for an attacker to assemble the trajectories provided for the same id and identify the user, including his/her sensitive locations. Additionally, in order to protect the user’s sensitive data, the system makes the attacker consider all trajectories as equiprobable to containing sensitive data. In this case, the leak of sensitive data is prevented. The LOCATE system distributes the user’s data trajectories among multiple user databases,

based on the local entropy. Information entropy is a method used to measure how much information there is in an event. As a result, all paths are equiprobable to be a sensitive location.

However, although many solutions have been proposed to protect the privacy of users for sensing, few of these studies provide users with control over their personal data. Yet it is important to empower participants to take control over their personal information because the participant is initially only able to choose the granularity at which sensor readings are collected and disclosed to end users. In addition, it helps users to improve their awareness and make informed decisions to reduce their degree of exposure.

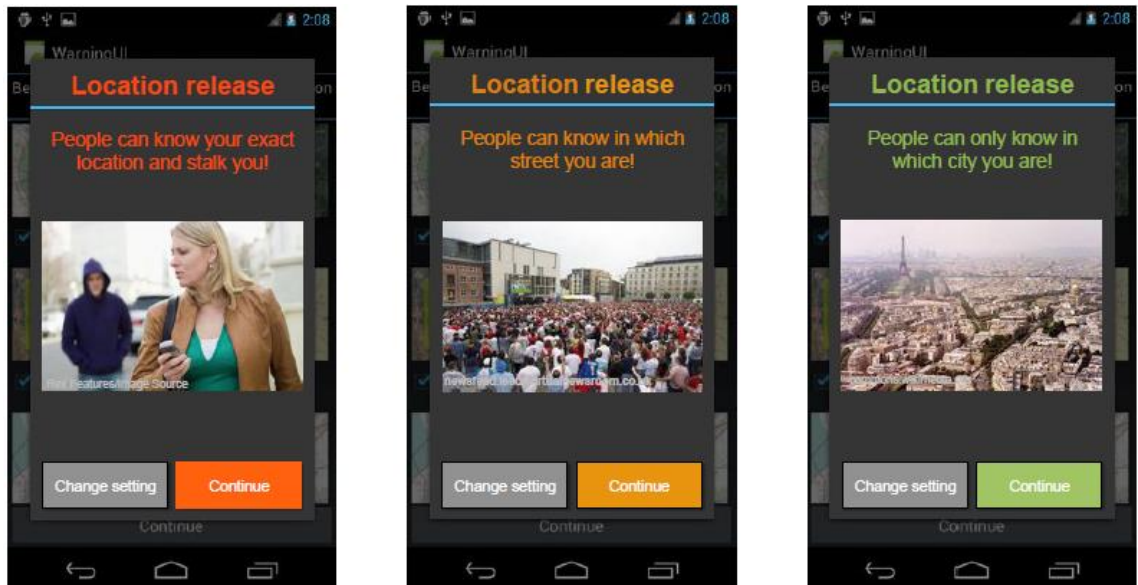
In contrast, some studies have considered usability issues in participatory sensing. One of these studies that focus on usability to increase the user's awareness in participatory sensing applications was conducted by Christin et al. (2013). They designed different graphical interfaces that allow users to apply filters, which eliminates the privacy-sensitive elements of the sensor readings prior to transmission to the application server in order to protect their privacy. The study by Christin et al. (2013) aimed to increase user awareness about potential privacy risks and display picture-based warnings. These warnings allow users to know about potential risks to their privacy, and invite them to change their settings or leave them unchanged. Picture-based warnings are inspired by pictures on cigarette packets illustrating the risks of smoking. Every warning contains a picture and a sentence about the illustrated threat. Figure 3.1 shows the colour code of the interface for the description and the continue button. The green colour indicates a coarse-granular setting, while orange indicates a moderate one, and the red colour indicates a fine-granular one.



Source: Christin et al. (2013)

Figure 3.1: Example of Privacy Settings

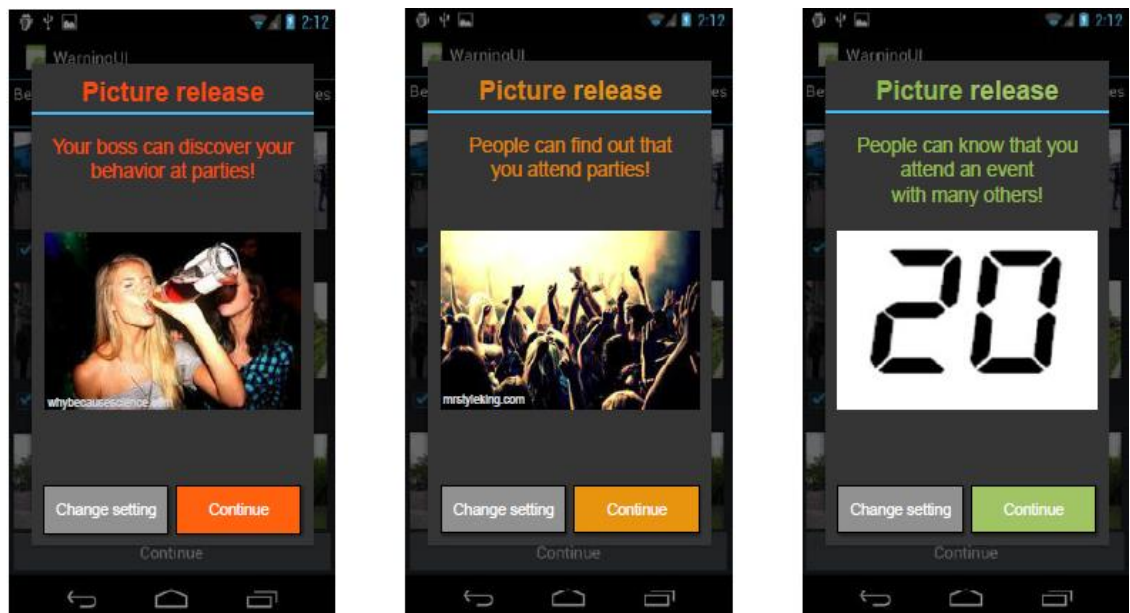
Figure 3.2 shows some examples of warning sets when publishing pictures online. These interfaces provide users with more granularity in order to control the information. Users have different levels of controls, which include fine, medium and coarse. For instance, when a user wants to change the level of a location, he has three levels: precise location, street and city. When a user-selects one of these levels, they have the ability to understand the consequences of their choices by displaying pictures and text.



Source: Christin et al. (2013)

Figure 3.2: Users Can Release Location Data at Different Degrees of Granularity

Similarly, Figure 3.3 shows the warning set when the user shares party pictures depending on the selected degree of granularity. It shows the impression that an employer may have about employees if they view the picture. On the other hand, when users choose to apply the moderate level, it will be difficult to infer the identity of the person.

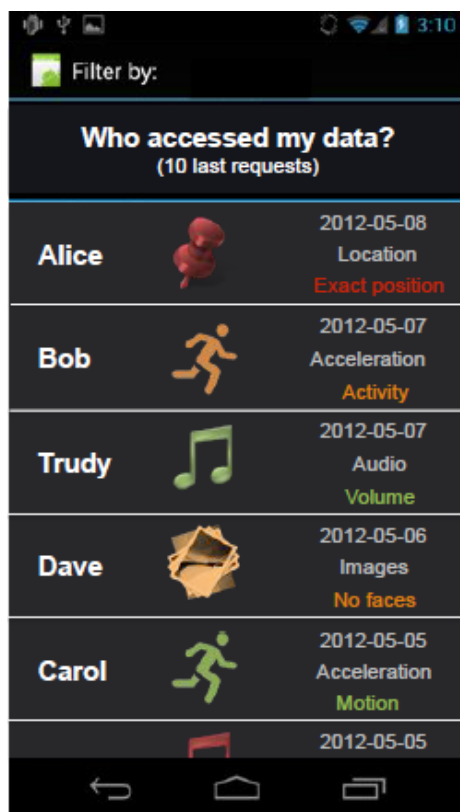


Source: Christin et al. (2013)

Figure 3.3: Users Can Release Pictures at Different Degrees of Granularity

The system reveals little information about the user, for example, whether the user is solitary or sociable. Another benefit of this proposal is introducing a history view to allow users to consult who has accessed their data, when, and to what degree of granularity.

Figure 3.4 shows that the user's history can be filtered according to different criteria, such as sensor modality, data recipients, or access dates. Viewing history will help users to verify whether their current privacy settings correspond to their privacy conceptions or not. An evaluation was carried out involving 30 participants, and 70% of participants would change their settings after having seen the picture-based warnings (Christin et al., 2013).



Source: Christin et al. (2013)

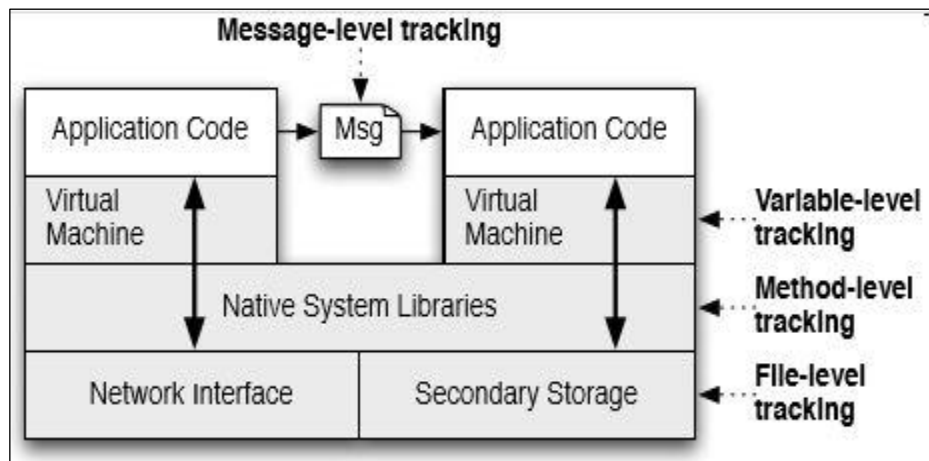
Figure 3.4: History Interface

However, Christin et al (2013) did not conduct long-term user studies to quantify their effects on user behaviour under real-world conditions. Although the proposed solution was designed with different graphical interfaces, users could not configure the user

interface settings in order to choose the size and the type of warnings. This approach empowers users to change the privacy settings, but changing the settings each time may become cumbersome for the user. Therefore, it may be difficult for novice users to make the right choice. Moreover, the history view in this proposal does not assist the system to identify the user’s preferences. Hence, the system allows the user to dynamically change their preferences in order to reduce the user burden.

Most of the current solutions focus on the Android operating system because it is the most popular mobile operating system in the world. Taintdroid is one of the most popular tainting analysis tools for Android (Enck et al., 2014). It was designed based on a dynamic approach, which is executed while a program is in operation in order to detect the sensitive data when that sensitive data leaves the system via untrusted applications. The system can track the flow of data through four levels: variable, method, message, and file.

Figure 3.5 illustrates the following four levels:



Source: (Enck et al., 2014)

Figure 3.5: Four Level Approach

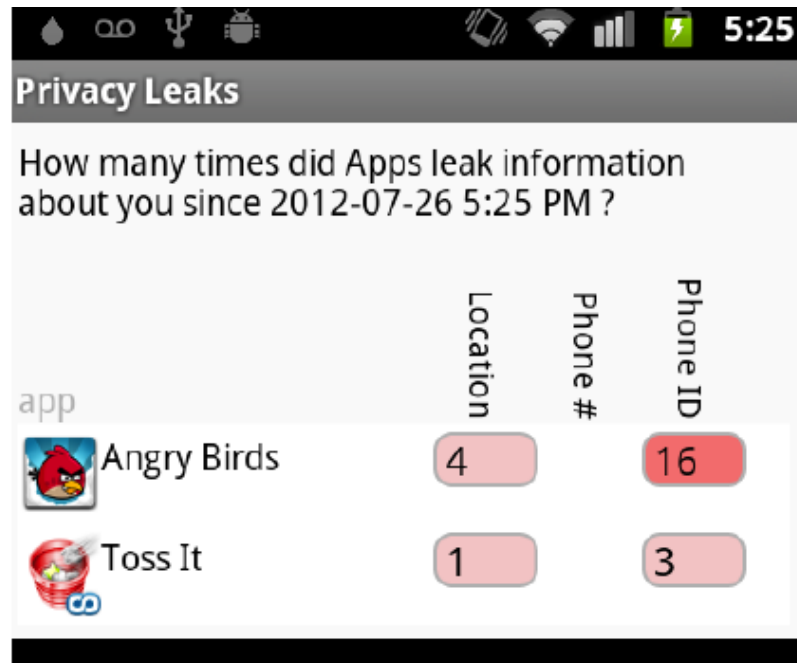
- Variable-level: in order to track the variables in the application, TaintDroid implements variable-level taint tracking within the Dalvik VM interpreter. When the system tracks variables, the system will focus on taint markings only for data and not code.

- Message-level: the message-level uses tracking between applications. The system taints on the message instead of the data.
- Method-level: in this stage, the systems patch the taint propagation on return.
- File level: the operating system may share sensor data such as the microphone and via file. Therefore, the file taints sensor data with the appropriate tag. Hence, the four levels can simultaneously track multiple sources of sensitive data.

The outcomes of the experiments revealed that TaintDroid incurs a runtime overhead of less than 14% for a CPU-bound microbenchmark. However, although TaintDroid provides users with finer control over the disclosure of their personal information, the system assumes that users can correctly configure all the resulting settings. Therefore, this approach could impose an undue burden on the user. In addition, they do not examine the usability related to the interface displayed to users.

Balebako et al. (2013) proposed another solution which was built based upon the TaintDroid platform to detect the sensitive data that leaves the system via an app. The solution aims to improve users' understanding of potential privacy leakages by designing a visualisation interface, which contains columns and cells. The columns show the type of data, and the cells in each grid show the number of times the information was sent. Figure 3.6 shows that phone ID for the Angry Birds app is red because the number of times the information was sent is high. In addition, it provides information about the data leaked by all applications over a period of time; this period is configurable by the user. The system also provides user notifications in order to notify users the moment that data is leaked by using vibration and sound. To evaluate the system, 19 users participated to investigate their existing understanding of potential privacy leakages through apps. The study shows that thirteen out of 19 participants did not know that data would be shared for advertising, and most of them were concerned about sharing data via these game applications. However, when looking at the number of the sample size, it shows that the

total number of participants is quite small. Additionally, the notification interface informs users of each data being sent, which could significantly increase the burden on, and frustration of, the user.



Source: (Balebako et al., 2013)

Figure 3.6: Main Visualisation Screen of Privacy Leaks

Indeed, the aforementioned studies have proposed solutions to improve users' understanding of potential privacy leakages, but still these solutions suffer from providing users with multi-level control over their information. In contrast, AppFence is a system that aims to provide users with privacy controls to protect their sensitive resources by utilising two level controls: shadowing sensitive data and blocking sensitive data (Hornyack et al., 2011). Sometimes users do not want to provide application access to sensitive data; therefore, AppFence sends shadow data instead of the actual data. For example, when an application requires access to a user's contacts, AppFence may provide application shadow data that contains no contact entries, and contains only those genuine entries not considered sensitive by the user, or that contains shadow entries that are entirely fictional. Another example is when applications require access to the unique

device ID, which is called International Mobile Equipment Identity (IMEI). This is frequently used for creating user profiles, and AppFence may send the device ID with a device secret and the application name. The second approach for protecting sensitive data is blocking sensitive data from being exfiltrated from the device. In order to track the sensitive data and prevent information from being transmitted from the data out of the device, AppFence utilises the TaintDroid tool, which in turn means that TaintDroid helped the researchers to monitor the user's data. However, when applications have access to an empty shadow contact list, AppFence allows the user to prevent information from being misappropriated from the sensitive data. Hornyack et al., (2011) evaluated the privacy controls for 50 applications from the Android Market which were selected based on popular and permission-hungry. The result of the evaluation shows that privacy controls reduced the effective permissions of 66% of the 50 applications. However, they only focused on four types of sensitive resources: unique device ID, contact list, network location and GPS location, and they did not consider a wide range of other data that is sensitive and valuable for users such as calendar and call log. Additionally, the system does not alert users about how applications use data and whether they will exhibit side effects if privacy controls are applied. In order to know whether side effects affect user-desired functionality, it is necessary to consult users each time. In this case, the system may place a high level of burden on users.

Similarly, the Taming Information Stealing Smartphone Applications (TISSA) provides the user with fine-grained control over the disclosure of their personal information, which includes four types of personal information: phone identity, location, contacts, and call log (Zhou et al., 2011). The fine-grained controls were two levels of control: empty level, or bogus level for personal information that may be requested by the app. The advantage of this tool is that it is a lightweight runtime system for protecting the user's private information because the implementation has low-performance overheads and requires

less than one thousand lines of code. TISSA consists of three main components, where the first one is the privacy setting content provider, which contains the current privacy settings for untrusted apps on the mobile device. It also provides users with an interface in order to query the current privacy settings for an untrusted app (e.g., a location manager). The second component is the privacy-setting manager, which allows users to manage or update the privacy settings for installed apps. The third component contains content providers or services for regulating access for four types of personal information: phone identity, location, contacts, and call log. For example, when an app requires access to private data, the system will query the privacy settings, and respond to the requests according to the current privacy settings for the app. However, the tool does not allow users to limit the disclosure of their private information on different multiple levels because blocking data or shadow data may not be sufficient for users, as users may desire more level of control over locations. Therefore, the approach could not support different multi-level privacy controls for users to achieve more flexibility.

In order to enhance privacy controls, another study proposed DROIDFORCE to enforce privacy controls based on a user's policy (Rasthofer et al., 2014). DROIDFORCE works at the application level to target apps with static data flow analysis to identify strategic policy enforcement points, whether for a single application or for multiple applications at the same time. These policies may depend on the data available only at runtime. However, this system does not show how users can better understand these policies to make an informed decision.

Unlike previous studies that simply consider the transmission of private data as privacy leakage, AppIntent determines whether transmission is user intended or not because the transmission of sensitive data in itself does not necessarily indicate a privacy leakage (Yang, 2013). AppIntent was designed to distinguish between user-intended data transmission from the user as unintended, and Yang (2013) developed an event-space

constraint guided symbolic execution technique. This technique can reduce the event search space in symbolic execution for Android apps, which are used to determine the right inputs that ready the program to execute. The new symbolic execution technique, called event-space constraint guided symbolic execution, for Android apps aims to avoid the possibility of the path explosion problem during symbolic execution. The path explosion problem occurs when there is a large number or combination of input events. The researchers apply statistical analysis first to identify the possible execution paths that lead to sensitive data transmission under analysis (such as sending SMS). Then they use these paths to generate event-space constraints; these constraints represent all the possible event sequences for the given execution paths. Next, guided symbolic execution considers only the paths that satisfy the event space constraints. In the final step, they developed a dynamic program analysis platform to execute the app driven by the discovered event and data inputs. To evaluate usability, three Android experts were invited. During the evaluation, AppIntent was introduced to them with less than 15 minutes to examine it. Then they were asked to fill in a sheet which in each case should be classified as “user-intended” or “unintended. The results show that 98 cases match with the design of the AppIntent expectations. However, the evaluations should have been conducted with a varying number of participants in order to identify the extent of user acceptance of the system. Moreover, AppIntent does not analyse data transmissions that are not triggered by a sequences of GUI manipulations, as it focuses only on app behaviours activated by GUI events.

Other approaches such as PrivacyGuard (Song, 2015) and AntMonitor (Le et al., 2015) analyse the actual network traffic of Android using VPNService API to intercept traffic. This approach does not require root permissions and is portable to all devices with Android version 4.0 or later. The AntMonitor system consists of three components: an Android application, AnyClient, and two server applications, AntServer and LogServ, but

whether any of the installed applications are sending the personal data out to the Internet. They found that 44% and 66% of the users have applications that leak their IMEI and Android Device ID respectively. However, they did not show how the average user accepts the system. Moreover, both PrivacyGuard and AntMonitor are not easy to use for average users because they require a priori knowledge of Personally Identifiable Information (PII). For example, the user can add personal information, such as home address, ethnicity, gender and age that he wants to protect. When a user inserts the string, AntClient inspects every outgoing packet for any of the protected strings, before sending it out.

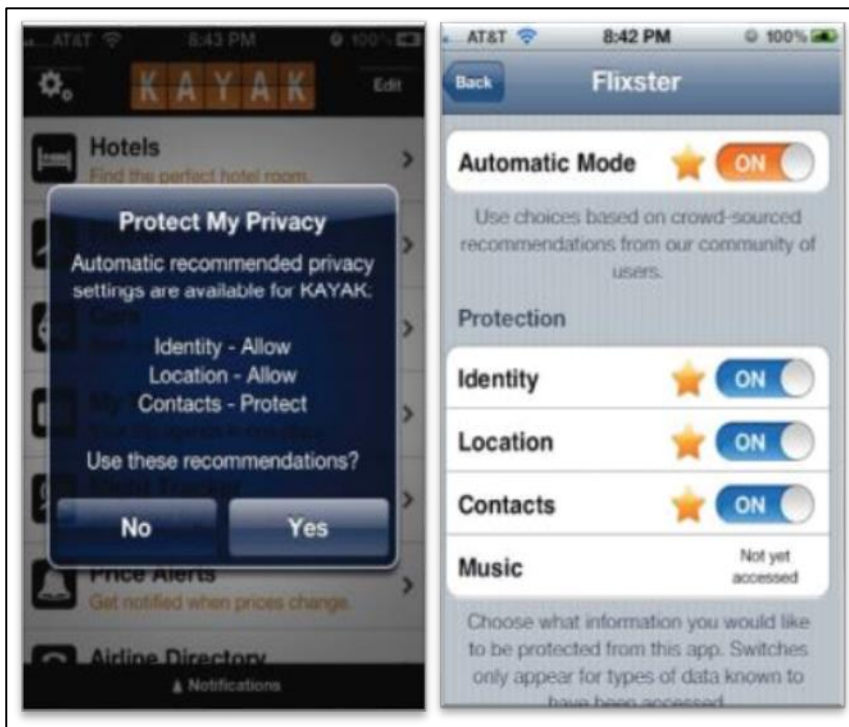
Another popular mobile operating system, iOS, has privacy controls to protect the privacy of the user's data. PIsOS allows users to protect their personal information in the fine-grained privacy policy on iOS in order to specify precisely which privileges are assigned to an application (Werthmann et al., 2013). PSiOS are completely implemented in one shared library. Based on this approach, when the enforcement framework defines the policy it will be applied to all applications. One feature of this system is allowing the user to define sandboxing for each third-party application without requiring access to the application source code. PSiOS was implemented on a number of popular iOS applications such as Facebook, WhatsApp, ImageCrop, BatteryLife, LinPack, Satellite TV and the Audi App in order to evaluate the effectiveness of the system. In order to prevent the app from accessing private user information, sandboxing profile was defined for each app and Werthmann et al., (2013) found that PSiOS successfully prevents access to the address book (for Quicksan, Facebook, and Whatsapp), to personal photos (for ImageCrop and Instagram), and to the iOS universal unique identifier, short UUID (for Quicksan, BatterLife, Flashlight, MusicDownloader, MyVideo, NewYork, and Audi). The outcomes indicate that PSiOS effectively prevents privacy breaches. However, the

framework does not show how the user can understand these policies to make informed decision information about good privacy practices.

ProtectMyPrivacy (PMP) is another solution that detects privacy leaks on iOS applications (Agarwal and Hall, 2012). It provides users with fine-grained privacy for each app in order to send anonymised data instead of privacy-sensitive information. The type of data that PMP protects is a unique device identifier (UDID), IMEI, Wi-Fi MAC and Bluetooth MAC. Another private data type that PMP protects is the user's address book, which includes names, addresses, phone numbers and emails, because some apps upload this information to a server without the user's permission. When the app wants to access the private data, PMP allows the user to deny or allow the app to access private data in real-time. Hence, PMP provides the user with two options to protect his address book: the user can allow the app to access his or her address book, or allow PMP to send an alternative address book, filled with fictitious entries (names, emails and phone numbers). Additionally, they have developed a crowdsourcing system to help the user to make informed decisions, which provides app-specific privacy recommendations. The PMP Server collects the protection decisions from users in order to generate recommendations for those users. There are three conditions for collecting protection decisions:

- The system does not generate recommendations unless there are more than five users who make the protection decisions for each app.
- The system considers decisions from only active users of an app (used for more than a week).
- PMP Server collects decisions only from users who have made decisions for a minimum number of other apps ($n > 10$ apps).

Figure 3.8 shows what type of recommendations are available. However, the user has a choice to use recommendations for this particular app or not. If the user chooses not to use the recommendations, and recommendations are available for the app, the system prompts the user to check if he would like to use them, as shown in Figure 3.8. If no recommendation is available, then the system provides the user two options: protect or allow. Figure 3.8 shows stars for what is recommended, and displays whether one of the privacy-protected features has not been accessed yet, which are the automatic recommendations.



Source: (Agarwal and Hall, 2012)

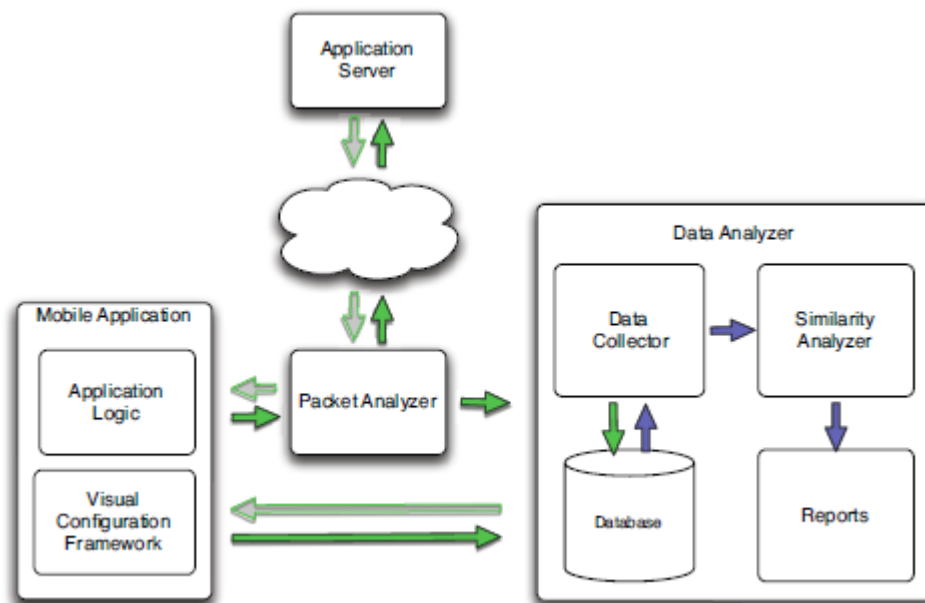
Figure 3.8: Pop-Up Showing That a Recommendation is Available

To evaluate user acceptance, the PMP has been in use for over nine months and has been used by 90,621 real users, and Agarwal and Hall (2012) found that 48.4% of apps used the access permission to the device identifier, 13.2% location, 6.2% address book, and 1.6% music library. The strength of this experiment is the fact that it was based on a large number of real users' data. Moreover, the users accepted the majority of

recommendations (67.1%), which means that the recommendations were helping them to make informed privacy choices. However, the system only deals with mere access to private data, but does not address privacy once the data leaves the app. Moreover, the system does not provide each user with personalised recommendations because each user has their own privacy preferences. Therefore, it would be helpful to take account of the user's profile when the system generates recommendations, in order to make a more personal recommendation.

Other researchers have proposed approaches that do not rely on one operating system but can run on different mobile systems. Nadkarni and Enck (2013) have proposed Aquifer as a policy framework in modern operating systems such as Android, iOS, and Windows 8, which performs two types of restrictions that protect the entire User Interface (UI) workflow, define the user task, and ensure only specific apps can export the data to the host. Aquifer provides each application with control over sensitive data, and can therefore contribute towards the security restrictions. However, Aquifer does not show users the privacy policy of an application. Additionally, it does not provide users with comprehensive tracking of the sensitive data because it just focuses on the UI workflow that sends data to another application.

Labyrinth also supports both Android and iOS to detect access to private data by using a privacy enforcement system that automatically detects the leakage of private data originating from standard and application-specific sources (Pistoia et al., 2015). It contains a Packet Analyser that collects all the data applications that are sent to any remote server, as shown in Figure 3.9.

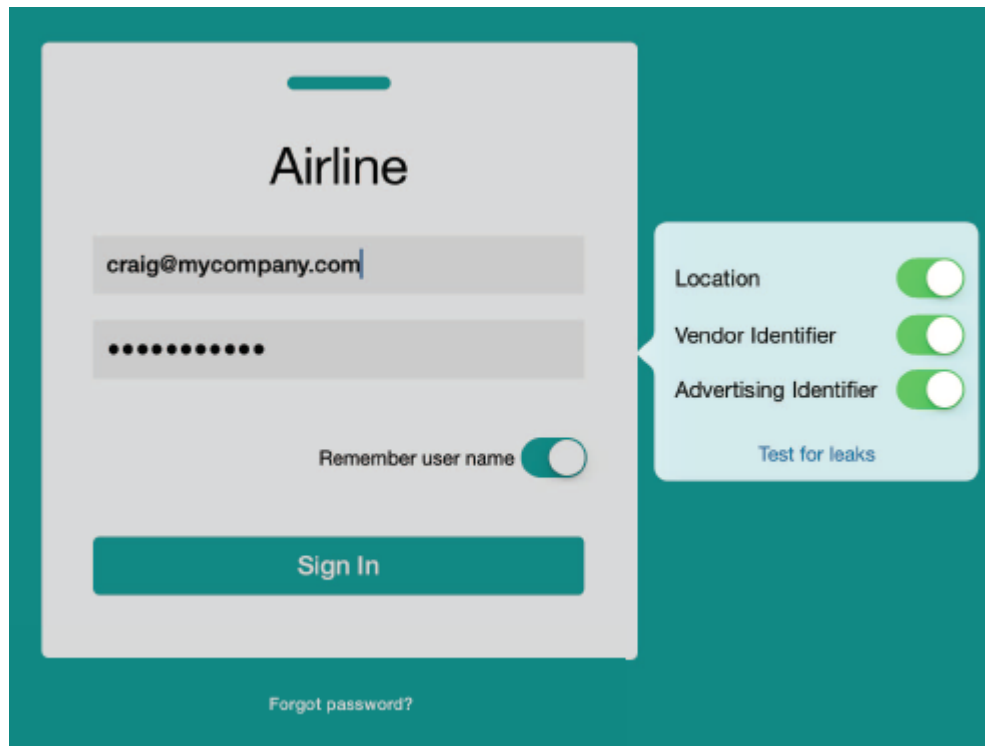


Source: (Pistoia et al, 2015)

Figure 3.9: Architecture of the Labyrinth System

When the data is collected, the Packet Analyser detects whether private data has been sent in the clear. Then the system will terminate any unauthorised communication of private data in the clear between the client and the server via the proxy interface. Moreover, Labyrinth is equipped with an integrated Visual Configuration Framework in order to identify the private information that Labyrinth should protect. Therefore, when an application accesses the private information via user input or through standard libraries, Labyrinth compares the data that is collected at run time by the Packet Analyser along with the data that is collected by the instrumentation layer. If a match is found, a confidentiality warning is reported. Regarding visually configuring, it is directly atop the application’s UI and it does not require operating-system instrumentation. Figure 3.10 shows the visual configuration of environment specific features to track at run time on the iOS platform. In order to improve the usability of the security administration of a mobile application, the visual configuration provides users with the type of data that may leak from the application at run time. However, it may not be feasible to notify users of each leak from the application at run time. Moreover, constant notifications for each leak

from the application may affect the user's acceptance of the system. Additionally, configuring the privacy policy each time may place a high level of burden on users. It would be helpful to take account of users' choices, in order to create a more personal policy.



Source: (Pistoia et al., 2015)

Figure 3.10: Visual Security Configuration on iOS

Several techniques, methods and solutions have been proposed to preserve privacy when users are surfing the web browser. Privacy Bird was an early browser privacy add-on that showed coloured icons and played bird sounds to notify users whether a website's privacy policy matched their preference settings (Cranor et al., 2006). This tool helps user to understand the policy by keeping only the relevant elements of P3P (Consortium, 2002), removing jargon, and grouping items based on the user's preferences rather than on a P3P structure. Users can see the bird icon with a song bubble in the title bar at the top right-hand corner of the Internet Explorer browser window. When a website has P3P enabled

and its privacy policy matches a user's privacy preferences, in this case, the bird changes colour and the contents of the song bubble.

However, users who want to protect all personal information such as health information, may not find many companies that provide users with sufficient P3P policy for some protection against sensitive information.

Takano et al. (2014) proposed the MindYourPrivacy system to help online users to know which companies are collecting their web browser history. It captures users' Web browsing traffic at gateways and analyses packets that contain HTTP and other traffic. In order to evaluate the usability and effectiveness of the proposed system, Takano et al. (2014) conducted two experiments: user traffic analysis and questionnaire-based use analysis for 129 participants; most of them were either IT specialists or IT students. The MindYourPrivacy system collects all the user's network traffic, including cookie and ad sites. The outcomes of the traffic analysing revealed interesting results regarding the top-five most-referred sites, which include GoogleAnalytics, Facebook, Twitter, Google+, and DoubleClick. GoogleAnalytics has the largest number of incoming links, which equals to 847. Regarding the Ad sites generally, they tend to collect user information for marketing purposes. However, the questionnaire-based user study showed that visualisation of Web tracking would help users to understand online privacy, whilst other participants are not concerned about their online privacy, which in turn emphasises that users' privacy requirements are various and this variation should be considered during the design stage.

Dhawan and Ganapathy (2009) examined the Sabre system to monitor JavaScript execution on runtime. They monitored sensitive resources and low-sensitivity sinks. Each JavaScript object is associated one label in the browser. When Sabre detects that objects contain sensitive data, the system will label this data differently. Sabre monitors all

JavaScript code executed by the browser. In addition, it monitors code on web applications, JSEs, as well as JavaScript code executed by the browser core. In order to monitor the codes, Dhawan and Ganapathy (2009) modified SpiderMonkey, the JavaScript interpreter in Firefox, to include security labels. The system will raise the alert when an object has sensitive data that is accessed in an untrusted way. However, the level of monitoring is too restrictive and can disable some useful and normal extensions. Additionally, this system only focuses on the information that is on an extension web and does not support a model to measure the users' privacy risk when users are browsing the Web.

Another approach is to modify the JavaScript interpreter and implement finer-grained enforcement mechanisms such as JSFlow (Hedin et al., 2014). JSFlow is a tool for securing information flow in the browser and provides a practical mechanism for fine-grained enforcement of secure information flow for JavaScript to ensure that the information does not leave the browser, or is not sent to a third party. The monitor will interrupt the execution of the program if a forbidden flow is detected. When the monitor detects that the information-flow policy is being violated, the tool can respond using one of these ways: simply logging the leak, silently blocking offensive HTTP requests, or stopping script execution altogether. The interpreter is implemented in JavaScript and keeps track of the security labels where each value is labelled with a security label representing the confidentiality of the value. JSFlow supports different information-flow policies, including tracking of user input and preventing it from leaving the browser. However, this approach requires implementing a new JavaScript interpreter. Moreover, this approach may be too restrictive because JSFlow tracks every instruction in the JavaScript engine and this is not efficient.

Liu et al. (2015) also proposed a solution for monitoring sensitive data, but they used a different technique to monitor the data, which is from network traffic. It automatically

detects personal information that is collected by services accessed via web browsers in network traffic. From Layer-7 flows of user traffic, the PI of users is extracted from HTTP requests, assuming that it is transferred in the form of key-value pairs. Liu et al. (2015) combined a key name with the name of the domain associated with the request. The purpose of using this method is that key names will potentially be used for the same type of information within the same domain. For example, google.com may use the keyword “gender” to collect user’s gender regardless of the specific Google service. In contrast, the same key will likely be used in the context of different domains with different meanings. For example, the key id may be used differently by Google and Facebook. The domain is extracted from the Host HTTP header, and extracted keys (and values) from three locations: (a) the query string of HTTP GET requests, (b) the query string in the Referer HTTP header, and (c) the Cookie HTTP header. Next, all of the domain-key combinations in a group are labelled PI “containers” in order to know if threshold subsets of them are found. The subset of PI containers are identified through a list of seed rules manually crafted to locate the PI of different types. The evaluation resulted in a large-scale traffic trace collected on the network of a residential service provider, and shows the technique is able to identify the rare domain keys that serve as containers for PI with low false negatives (2.7%) and acceptable false positives (13.6%). However, this approach does not distinguish between the PI the user has intentionally shared and others, although that is not because the transmission of the PI in itself does not necessarily indicate a privacy leakage. Additionally, the study does not demonstrate how to enhance the user’s awareness about the PI that is collected from user when he accesses online services. Therefore, it is important to enhance user awareness and user empowerment in order to allow them to distinguish between the PI the user has intentionally shared and others that they have not.

In context, enhancing users' privacy awareness only blocks tracking sensitive data, which may not be sufficient to preserve the privacy of web users. Hence, Starov and Nikiforakis. (2018) designed PrivacyMeter, which aims to inform users about the privacy consequences of visiting certain websites. The tool provides the user with the privacy score of any website that they visit. The score is calculated based on different factors such as the reputation of trackers, the amount of third-party content, or the presence of insecure "leaky" web forms. Moreover, it also provides users with contextual notifications regarding tracking for instance, "many aggressive trackers", or "many inputs are submitted to third parties". In order to improve the design of the notifications, they used the traffic light colours method to inform the user about the privacy risks, where green is used as "safe", yellow as "potentially dangerous", and red as "dangerous". To meet users' preferences, the tool allows users to change the score calculation settings to better reflect their privacy preferences. In terms of evaluation, however, Starov and Nikiforakis, (2018) did not conduct user studies to explore users' perceptions towards the tool and evaluate how easy it is to use and understand the output of PrivacyMeter.

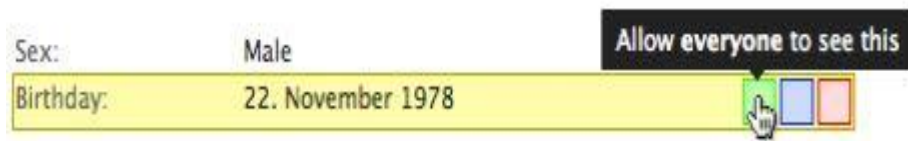
Hamed and Ayed (2015) proposed another approach that utilised privacy scoring in order to enhance users' awareness. It aimed to measure the users' privacy risk when they are browsing the Web. Two versions of a Firefox add-on were developed - one for the desktop and another one for the android version. Although this tool showed a message containing information about privacy, these messages contain too much information, which may make it difficult for the user to understand the privacy risks. Moreover, in context of the usability issue, the tool also does not help the users to know the level of risk or distinguish between a high level of risk and low risk.

Chapter 2 demonstrated that users have different privacy concerns regarding social networks due to the networks collecting and storing a large amount of personal information such as name, age, gender, profession, location, hobbies and multimedia,

which could be used for privacy violations, identity theft, fake accounts and sexual harassment. Therefore, many companies seek to protect users' information in these networks, for instance Trend Micro offers a free tool called "*Privacy Scanner*" (Trend Micro, 2015), which has been designed to increase privacy issues surrounding the use of social networks. It is an Android application that checks Facebook, Twitter, and Google+ settings for privacy risks, and can help the user to ensure that his personal information stays private. Another tool that was developed by the company is ZoneAlarm Privacy Scan (ZoneAlarm, 2015). It automatically evaluates the posts that users have created over the last month and the posts in which users are tagged. However, these tools are not sufficient to help users to protect their information on social networks. Therefore, a number of solutions have been proposed in order to overcome the shortcomings in these tools and meet users' preferences.

The C4PS privacy interface is one of the solutions that was introduced by Paul et al. (2012), which utilises a colour- coding scheme for making privacy settings more usable. The C4PS tool marks each attribute on the user's profile with a particular colour, based on the group of people who have access to this attribute. This approach applies four colour schemes for different groups of users: red – visible to nobody; blue – visible to selected friends; yellow – visible to all friends; and green – visible to everyone. This allows the user to change the privacy settings for any attribute by clicking on the edge on the right side, as shown in Figure 3.11. The right side on the edge contains three colours: green, blue and red. When the user chooses the green colour, it indicates that the user has allowed anyone to see the private information. For example, in Figure 3.11, the user chose the green colour for his birthday attribute to allow anyone to see it. Moreover, the tool allows the user to check and modify the privacy settings for photograph albums with the same colour mechanism. When the user visits his photographs on Facebook, three coloured buttons are shown on every item and this allows the user to change the privacy setting, as

described previously. However, the tool is not implemented for posts to other users' walls, and does not help the user to know the consequences of applied authorisation changes.



Source: (Paul et al., 2012)

Figure 3.11: Colour Coding for One Attribute – Birthday

Toubiana et al. (2012) designed a system to allow users to apply their tagging preferences automatically when a picture is taken. Users may not want to have a link between their identity and pictures without being able to modify them or control who accesses them. To solve the problem, the system allows users to declare their tagging preferences directly when the picture is taken, by enforcing users tagging preferences without revealing their identity. The following steps demonstrate more regarding how the system works:

- First, when a user takes a picture, the camera gets the "Tagging Profile" TP of every person present in the area and fetches their profile pictures and preferences.
- Second, the Photo-Tagging Preference Enforcement (Photo-TaPE) will recognise these faces.
- Third, when user takes a new picture, Photo-TaPE first extracts every face on the picture. When the faces match with the faces that are already stored in the local Gallery, Photo-TaPE retrieves the tagging preference of the person pictured.
- Fourth, Photo-TaPE applies a filter matching its owner's preference ("blur", "tag", "send by e-mail") for each matched face.
- Finally, the picture that Photo-TaPE delivers to the end users is a photograph respecting the preferences of every pictured person.

However, the system allows location services to inform Photo-TaPE of their presence and to disclose their location to other users in the same area. Disclosing personal location will

raise a large number of privacy issues related to the collection, retention, use, and disclosure of location information.

Squicciarini et al. (2009) discuss collaborative privacy management in a game-theoretical approach for collaborative sharing and control of images on a social network. They classified users based on their relationship as viewers, originators and owners. Viewers means users who are authorised to access the data, whilst users who post data on a given profile were defined as originator. Users who share ownership privileges with the originator were defined as the owners. This approach considers the access control policies of content that is co-owned by multiple users in an OSN. Each co-owner can select his or her own privacy preference for the shared content. The system helps the user to have control over the sharing of pictures, with automatic detection of pictures' co-owners based on id-tags, and collective privacy policies enforcement over shared pictures based on auctions. Game theory was applied to evaluate the scheme. However, the solution has usability issues because it is hard for the average user to understand the Clarke-Tax mechanism and specify appropriate bid values for auctions.

Faresi et al. (2014) focused in their research on a specific type of social network: a health social network (HSN). They examined how to protect users from other social networks because it is possible that members of an HSN are also members of other social networks such as Facebook and Twitter, which are virtual communities that allow members to connect with friends, family, and co-workers. They proposed a method for constructing a re-identification risk model using a probabilistic network. The purpose of the method is to know the risk from the re-identification of HSN members. Bayesian networks were used to identify the strength of the links between two networks when the user of these networks reuses their pseudonyms between these social networks. However, they did not apply the solution over a broad range of social network.

Some of the aforementioned studies can assist OSN users in improving their privacy settings, but users may forget to “*lock their door,*” and consequently they may leak sensitive information about themselves. Hence, Squicciarini et al. (2013) proposed Privacy Manager PriMa, which supports the semi-automated generation of access rules in order to protect the user’s privacy settings. A Multi criteria algorithm was utilised for generating access control rules from a user’s profile, which focused on two factors: user’s preference and the consequences of the disclosure of sensitive information. However, when the user changes his or her own preferences on a social network, the access control rules are updated to suggest these rules to the user, and the user to make their own decision about whether to accept these rules or reject them. In order to generate access rules, PriMa identifies each type of the information on the user’s profile as a finite set of traits; for example, the user’s age on their profile, a comment or status update, or a social relationship. Regarding the privacy control, PriMa provides the user with a fine grained approach to specify his or her privacy preferences for each individual trait, or the user can choose a general access rule. Therefore, users can specify who has access to the information, and these preferences are eventually translated into quantitative metrics for computation purposes. Then the system can automatically identify who can safely access the trait according to this coarse-grained indication. However, Squicciarini et al. (2013) only evaluated their solution on Facebook, where Facebook’s relationships between members are always bidirectional, which means both members are required to consent in order to connect; while some social networks such as Twitter do not require consent from both members. Furthermore, they have not addressed usability aspects or investigated the acceptability of the access rules generated by this solution.

Numerous studies have already highlighted many of the privacy issues related to user profiles, settings and control access. However, a few researchers have focused on the core of the shared information - the multimedia content. Ilia et al. (2015) explored the privacy

issues related to the exposure of photograph content on OSNs. They proposed an approach that can effectively handle the problem by changing the granularity of the access control mechanism for photo-sharing services that enforces the visibility of each user's face based on their respective access control lists. The approach allows an OSN to express and enforce every user's privacy setting within an image, even if the user's settings are restrictive or permissive. The system relies on face recognition to detect the faces of known users, which become objects in the access control model. Each user's face is automatically restricted based on the privacy settings of the specific user and not the content publisher. To evaluate the system, Ilia et al. (2015) used 34 participants. Each participant was shown a set of randomly selected photos of their contacts, with one friend "*hidden*" in each photo, and they were requested to identify the hidden friend. The result shows that the system effectively prevented users from identifying their contacts in 87.35% of the restricted photos. Although this approach presents a significant solution to preventing unwanted individuals from recognising users in photographs, the approach could have been extended to protect other sensitive information such as video and voice. Moreover, the user's identity might be inferred from other information and not just the photograph, such as the title of photographs and the comments. In addition, there are many more types of information that are embedded in photographs that need to be protected, for instance, ample metadata information when the photograph is created, and GPS coordinates.

3.2 Discussion

Numerous studies have been reviewed and investigated in this chapter in order to understand the current state-of-the-art of privacy methods, including both the problems and available solutions. The majority of existing studies have focussed only on the technical aspect to protect the privacy of users, especially how to monitor user data in

real-time. Some of the tools detect the sensitive data from the application level such as TaintDroid whilst others detect the data from the network level as shown in Table 3.1. Hence, the prior studies have shown that it is possible to monitor sensitive information for users in real time.

Authors	Data control	Detection	Awareness method	Profiles
Christin et al. (2013)	Coarse, moderate, fine	---	Picture-based	
Enck et al. (2014)	Off/on	Dynamic	Policy	
Balebako et al. (2013)	Off/on	Dynamic	Quantification	
Hornyack et al. (2011)	Shadow, block	Dynamic		
Zhou et al. (2011)	Empty level, bogus level	Dynamic		
Le et al. (2015)	Off/on	Network		
Song (2015)	Off/on	Network		
Lin et al. (2015)	----	Dynamic		
Werthmann et al. (2013)	Off/on	Network		Hierarchical clustering
Bal et al. (2015)		Dynamic	Risk impact	
Egele et al. (2011)		Static		
Agarwal et al. (2012)	Off/on	Dynamic	Crowdsourcing	
Nadkarni et al. (2013)	---			
Pistoia et al. (2015)	Off/on	Network	visually based	
Rasthofer et al. (2014)		Static		
Paul et al. (2012)	Off/on		Colour based	
Liu et al. (2013)	Off/on	Dynamic		K-means

Table 3.1: A review of prior studies approaches and solutions

However, the monitoring solutions that were proposed by these studies suffer from holistic monitoring of data, where most of these solutions only capture little pieces of data specifically, despite the increasing and rapidly diversifying characteristics of mobile data.

When it comes to privacy controls, most current privacy solutions support only binary and static privacy control approaches. Such approaches provide the user with two options - “allow” or “deny” - an application’s access to their private information. To overcome this limitation, a few studies such as TISSA provide users with empty or bogus options for personal information, whilst AppFence sends shadow data instead of the actual data. However, these approaches do not consider more flexible multi-level privacy controls to allow users to limit the disclosure of their private information on multiple levels, and do not take factors such as the level of user knowledge into account. It is paramount to consider the user’s knowledge because providing novice users with multi-level privacy controls may not help them to make an informed decision and may confuse them. Figure 3.12 shows a summary of the main solution approaches. Most solution approaches often assumed that users have uniform privacy requirements. Thus, current research approaches to privacy are usually fundamentally static in nature.

In contrast, personal information is dynamic because privacy preferences diverge from time to time. For instance, some users are willing to share their location for a period of time with some groups, such as close friends, family, Facebook friends and friends at work. Another example is that some users may share their location during certain hours of the day or days of the week. Therefore, there are a number of critical dimensions to these preferences, including the time of day, day of the week, and relevant groups.

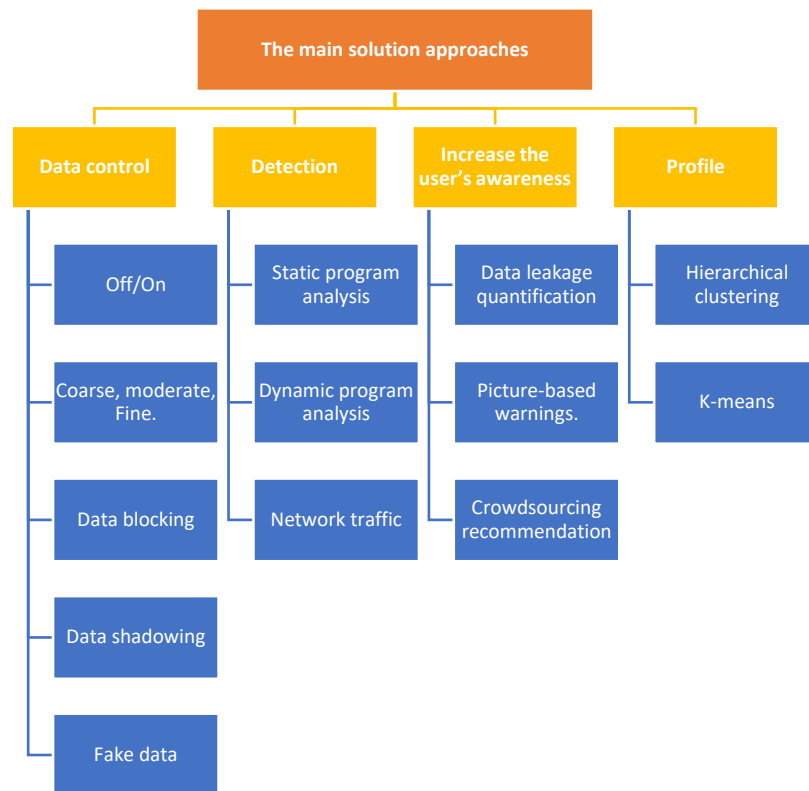


Figure 3.12: The main solution approaches

Another dimension that has not been considered by the current solutions is privacy preferences related to users' information where most of the approaches assume that users have uniform privacy concerns across all their data. Whilst some users may be concerned about some categories of apps such as social networks, they may not be concerned about others. This further indicates that prioritisation of a user's information differs from user to user.

However, a few studies have sought to measure the user's privacy risk when they use applications. In order to achieve that, they have implemented a variety of different methods, for instance, some have used the scoring method to identify the level of the privacy risk. However: Firstly, it is very difficult to quantify and measure the privacy level without returning to the user because this method only relies on the machine to calculate the level of the risk. Secondly, a user's preferences may change over time which indicates that it is difficult to use a static approach to protect users' privacy. In addition,

the prior art has not presented a holistic assessment, but rather focuses on one aspect of privacy such as web and mobile applications. This makes privacy measurements more challenging. Moreover, some approaches allow users to know the potential risk to their privacy and invite them to change their settings, such as Boutsis and Kalogeraki. (2013), Zhou et al. (2011) and Irvine et al. (2015). Despite these solutions providing users with settings to change the level of privacy, inviting users to change the level of privacy each time for each piece of data could place a burden on users, and could have a negative effect on the initial adoption of these solutions.

From a usability perspective, a few studies related to privacy focus on usability issues in order to increase user awareness. An interesting study conducted by Christin et al. (2013) aimed to increase user awareness about potential privacy risks and display picture-based warnings. Another benefit of this proposal is introducing a history view to allow users to know who has accessed their data, when, and to what degree of granularity. Paul et al. (2012) introduced the C4PS privacy interface, which uses a colour-coding scheme for making privacy settings more usable. However, the current approaches present the same content of the interface to all users. Therefore, current approaches have involved designing static user interfaces for all types of users, and they have not considered the level of users' knowledge during the design in term of how users understand the interface. Some users may want to know more information about the potential privacy risks and more control, while others may not want to.

Regarding the notification method, the most prevalent method for privacy alerts is to inform users about each potential single data leakage, but this method may significantly increase the burden on, and frustration of, the user. Additionally, they have not helped users to understand the consequences of the disclosure of sensitive information, which in turn would increase users' knowledge and help them to make an informed decision.

The evaluation of these studies shows that they have not been conducted with varying groups of participants in order to explore end-users' perceptions and attitudes towards the design, and identify the current users' preferences, which would enhance users' acceptance of the system and help to overcome the usability issues without compromising the user's convenience.

3.3 Conclusions

As presented in this chapter, several methods and systems have been proposed in order to protect individual's privacy. However, the utilisation of these techniques requires a number of considerations in regards to user acceptance, usability and holistic privacy solutions, to take factors related to different dimensions into account during the design; for example, users' desire to manage privacy and gain knowledge, prioritisation of users' information, and their current level of privacy knowledge. In addition, none of these studies have considered that sharing personal information differs from time to time and from person to person. Users have different privacy concerns and requirements because they have heterogeneous privacy attitudes and expectations. Assuming that users have uniform privacy requirements would be ineffective, and it could significantly increase the burden on, and frustration of, the user.

Therefore, there is a shortage of literature available on ways of increasing user awareness about potential privacy risks. These few works have focused on certain types of personal information among users, rather than presenting various types of information that can help users to manage their privacy across a range of apps on an individual basis. Moreover, none of these approaches have included designing an interface that overcomes the usability issues and meet users' privacy preferences.

Chapter Four

Research Methodology

4. Research Methodology

4.1 Introduction

This chapter provides an overview of the research methodologies, including highlighting the philosophical systems and paradigms of scientific research. It also presents and discusses the particular research methodology applied in this study, accompanied by a description of the scientific methodology used to design the questionnaire, collect data and analyse it. Moreover, this chapter does not only describe the paradigms of research, but it also goes beyond that to identify the differences between each approach that was utilised in the research. This has helped to guide the researcher towards determine the characteristics and the strengths of each approach. These comparisons begin with section two, which is about positivism versus interpretivism. Then moving forward, research methodologies and approaches to analysis are discussed in sections three and four, along with a comparison between each approach and paradigm.

The definition of research paradigms according to Guba, is “*the set of common beliefs and agreements shared between scientists about how problems should be understood and addressed*” (Kuhn, 1962). Therefore, research paradigms help to build a method and strategy to seek answers to research questions. By looking at the essential elements in a paradigm, according to Lincoln and Guba (1994), it should contain three primary elements, which are ontology, epistemology and methodology (Guba, and Lincoln, 1994). Ontology can be defined as “*the nature of our beliefs about reality*” (Richards, 2003). It focuses on what exists and what does not exist, and it is a theory about the nature of reality. It leads the researcher to investigate what kind of reality exists.

Regarding the term epistemology, it can be defined as “*the branch of philosophy that studies the nature of knowledge and the process by which knowledge is acquired and*

validated" (Gall, Borg and Gall, 1996). It focuses on how to gain knowledge and the sources used to obtain knowledge. Specifically, epistemology deals with the nature and limitations of knowledge in the area of research. In this case, the researchers would identify criteria to determine what does and does not constitute knowledge.

The third primary element in the research paradigm is the methodology, which helps to identify the method that should be utilised to obtain knowledge. It leads the researcher to determine the type of data that is required for the research, and to identify the method that will be performed to collect the data. It guides the researcher to address the question regarding how the world should be studied.

These three elements form a holistic view of how researchers view knowledge, the relationships between this knowledge, and the methodological strategies that are used to discover it. These elements also comprise the fundamental assumptions, beliefs, norms and values that each paradigm holds. However, there are many paradigms that are used in scientific research, which include positivism and interpretivism, qualitative and quantitative, inductive and deductive, as well as exploratory and confirmatory.

4.2 Positivism versus interpretivism

There are some differences between the two paradigms of positivism and interpretivism in terms of ontology, epistemology and methodology. In terms of ontology, positivism posits that there is a single reality, whilst interpretivism posits there is no single reality or truth (Stahl, 2007). Positivists view reality as stable if the results are the same if and when the same research is done by others. Regarding epistemology, positivism focuses on discovering absolute knowledge about objective reality. The role of the researcher and the researched are restricted to data collection and interpretation in an objective reality. According to the interpretivism paradigm, the knowledge obtained in this approach is

socially constructed rather than objectively determined (Carson, 2001); the role of the researcher and the researched are interdependent and mutually interactive.

With regard to the research methodology, positivist research involves acquiring data from different methods such as laboratory experiments, and survey and field experiments, as the research methods. The data, in this case, can be measured and known, and therefore they are more likely to use quantitative methods to measure this reality. In comparison, interpretivism involves using diverse approaches, including social constructivism and phenomenology. Social constructionism studies how people perceive the knowledge of the world from within a social context, whilst phenomenology is another methodology of interpretation that aims to interpret the world via directly experiencing the phenomena. However, in the end, the goal of different research methods and data analysis techniques is to provide information that is beneficial to the domain.

4.3 Qualitative versus Quantitative

There are two main approaches of research methodologies: quantitative and qualitative. The goal of qualitative research is to observe human behaviour and try to answer the whys and hows of human behaviour, opinion, and experience (Tong et al., 2012). The essential characteristics of qualitative research are:

- It does not use numerical measurements or statistical methods as key research indicators and tools.
- It uses the description as the unit of analysis.
- It is appropriate for situations in which detailed understanding is required.
- It is used to analyse small-scale studies and look at issues from a holistic perspective.

Despite these aforementioned characteristics, this approach has some limitations, which include not always being generalisable due to small sample sizes and the subjective nature

of the research, and also the outcomes could be different on a different day/with different people.

Quantitative is another approach to research methodology, which differs from qualitative approaches in terms of the type of data, the sample size, methodology and the outcomes of the results. Table 4.1 summarises these differences between qualitative and quantitative research.

	Qualitative research	Quantitative Research
Sample	Small and narrow	Large and abroad
Methodology	Focus groups, interviews, case studies, expert opinions, observational research	Surveys, structured interviews & observations, and reviews of records or documents for numeric information
Data Analysis	Non-numerical data	Numerical data
Reporting Outcomes	Directional in nature Not projectable to the total target audience	Reports are graphical Representative of the target audience

Table 4.1: The Differences between Qualitative and Quantitative Research

Each approach has its advantages and disadvantages regarding the time of data collection, cost and ease of data collection. Ultimately, the selection of a research approach is dependent on the core purposes of the research.

4.4 Inductive Versus Deductive

Inductive and deductive are significant approaches used in research to analyse the data. Deductive has a top-down logic and begins from one or more general statements regarding a phenomenon, and then moves towards an extracted specific conclusion. Whilst induction has a bottom-up logic, which begins with a general statement that is derived from specific examples (Bryman and Bell, 2011).

Accordingly, the deductive approach would start by identifying hypotheses or theories and then gathering data and analysing it to test these theories through observation. The

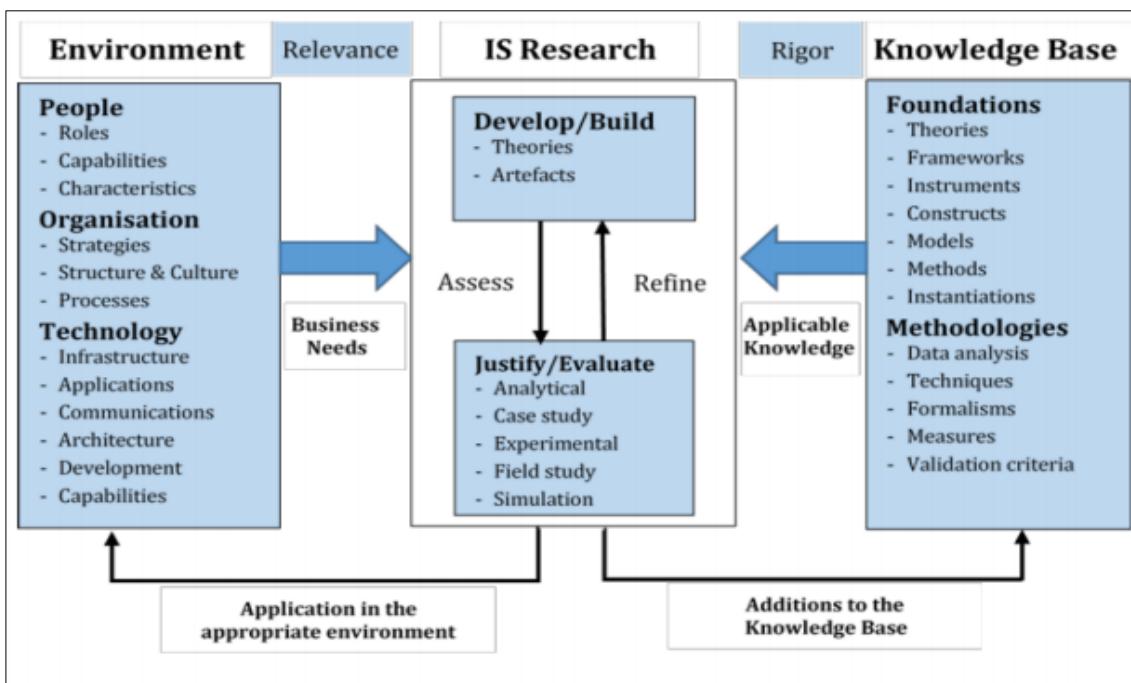
theories can be identified based on personal experiences or from prior studies. In contrast, the inductive approach starts with specific observations or real examples of events to build broader theory or observations. Thus, when researchers use the inductive approach, they establish a set of observations and then they can formulate those observations to test, and eventually develop some general conclusions. Though there are some differences between the inductive and deductive approach, they can actually be rather complementary and often address the same question.

4.5 Design Science Research Methodology

Designing science research according to Hevner and Chatterjee is “*a set of synthetic and analytical techniques and perspectives (complementing positivist, interpretive, and critical perspectives) for performing research in information system*” (Hevner and Chatterjee, 2010 p.214). Walls et al. (1992 p.37) also defined information systems design as “*a class of research that would stand as an equal with traditional social science-based theory building and testing*”. These concepts demonstrate that design science is a systematic method that seeks to design solutions for information systems. The knowledge in design science is acquired from an iterative process of a problem, which includes awareness, development, evaluation and conclusion. The first stage in order to solve the problem is to use preliminary quantitative and qualitative data collection and analysis. Then, the iterative development of an artifact is conducted. The experiment will be the final stage for evaluation, and the findings suggest opportunities for further improvement using insights or suggestions. Consequently, the findings of design science are essential artifacts as a solution to the problem in practice, and these outcomes may be refined after being delivered.

Regarding how to implement and evaluate information system research, Hevner et al. (2004) proposed a conceptual framework, as illustrated in Figure 4.1. The environment

in the proposed framework identifies the limitations of the problem, which consists of three components: people, originations and technologies. The framework aims to include two aspects of paradigms: behavioural science and design science. Design science aims to create and develop a new artifact, whilst behavioural science seeks to study behaviour in relation to IT usage. Moreover, behavioural science is seen as reactive and looking to demonstrate what already exists. Design science is seen as proactive and aims to create technological solutions for the future. Both paradigms are essential to the information system discipline in order to study the confluence of people and technology.



Source: (Hevner et al., 2004)

Figure 4.1: Information Systems Research Framework

When it comes to the knowledge base component, it provides the basic materials, which are utilised to complete IS researches. The knowledge base involves two-aspects: foundations and methodologies. Foundations provide different elements, which can be utilised in the development stage such as theories, frameworks, instruments and methods. Whilst methodologies aim to provide guidelines to justify and evaluate the stages of the research.

Von Alan et al. (2004) have proposed seven guidelines for designing science research within the discipline of information systems. The seven guidelines are provided and demonstrated in the following points:

1. Design as an artefact: Design-science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.
2. Problem relevance: The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
3. Design evaluation: The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.
4. Research contributions: Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
5. Research rigour: Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
6. Design as a search process: The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
7. Communication of research: Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

As a result, design science research requires the creation of a viable artefact for a special problem on the domain. Moreover, the artefact should provide a solution to the problem and should be a more effective solution. This artefact should be evaluated in order to make sure it is useful and beneficial for the specified problem.

Vaishnavi and Kuechler (2007) proposed other guidelines for design science research within the discipline of information systems which include five stages:

- Awareness of the problem
- Suggestions
- Development
- Evaluation
- Conclusion

Awareness of the problem stage can be generated from investigating and analysing prior studies. The findings from this stage would identify the research gap in the domain. Whilst, stage two which is about suggestions and aims to address the problems based on the theoretical foundations and methodologies (Vaishnavi & Kuechler, 2007). Accordingly, it would involve designing a viable artefact that addresses the research problem.

4.6 Method Adopted for the Current Research

Design science provides specific guidelines for evaluation and iteration within research projects which could address the problem in a coherent and logical way for information systems Vaishnavi and Kuechler (2007). When it comes to human/computer interfaces, design science approach play an essential role because it would develop HCI artifact to design and evaluate the interfaces. Therefore, many studies used design science in the HCI domain in order to design and evaluate web interfaces. For instance, Gjørseter (2015) adopted the design science research approach to propose domain-specific guidelines for designing mobile augmented reality systems. Another study used design science to develop HCI artifact to design and evaluate web interfaces signs to make them intuitive for end-users (Islam, 2017).

Accordingly, this approach provides guidance not only for what steps need to be taken to ensure the quality and contribution of the created artifact but also to understand a real-world problem, for what a solution artifact is required to be developed. Moreover, it helps HCI researcher to follow the all core phase of a HCI research methodology, design, and evaluation, whilst it keep the research rigor. Therefore, the design science research paradigm was deemed a suitable approach for this research.

When it looks at another research methodology such as action research, it appears that there is some similarity between action research and design science in term of an iterative process and solving problems. However, design science research presents specific guidelines for evaluation and iteration to the design and development of artifacts with the information system domain. Explanatory sciences is another research methodology that focuses to develop guidelines on other domains such as the natural sciences psychology and sociology, which is to develop knowledge to describe and explain phenomena in the social world. Whilst design science research aims to achieve knowledge and understanding of a problem domain by developing of a designed artefact Hevner et al. (2004). Moreover, this approach checks the validity and reliability of a process or methods from a replicability dimension.

Table 4.2 shows how the design science principles are being applied in this research. One of the essential stages in Vaishnavi and Kuechler's (2007) guidelines is awareness of the problem, which aims to identify the research gap. Whilst the development stage identifies the final goal of this research, which is about enhancing privacy technology for mobile devices.

The research objectives	Design science Stages	Processes
<ol style="list-style-type: none"> To identify and understand the potential privacy concerns that users have across the internet, social media, mobile devices and the internet of things. To review the privacy techniques and solutions to protect users' information and reduce their concerns across a range of platforms including computers and mobiles. 	Awareness of problem	Analysis of prior studies
<ol style="list-style-type: none"> To develop a new technique to manage and priorities privacy-related information. To develop usable and adaptive interfaces that maximise user satisfaction 	Suggestions	Prior studies analysis
		Designing preliminary interfaces based on HCI principles
		Participatory Study (Questionnaire)
<ol style="list-style-type: none"> To develop a novel and holistic framework for enhancing privacy technology on mobiles and meet users' privacy preferences. 	Development	Current privacy and usability preferences
<ol style="list-style-type: none"> To conduct an evaluation of the aforementioned model to determine its effectiveness. 	Evaluation	Evaluation of the framework (Focus group: experts & end-users)
	Conclusion	Develop recommendations and limitations for the proposed framework

Table 4.2: Design Science and its Applications in This Research

This research addresses the lack of current use of privacy technologies and available solutions for mobile devices in terms of how to manage a large volume of data, designing for usable privacy and transparency, and how to prioritise privacy related information. Moreover, most of the current solutions have not led to the development of a flexible solution to accommodate novice and advanced users, hence there is a gap in the literature that needs to be addressed.

Regarding the research processes, Figure 4.2 shows the stages of this study, which consists of different phases. The first phase begins with a review of the previous literature

in order to help to understand the dimensions of the research problem and identify the focus of the study. This stage has been discussed in Chapter Two and Chapter Three. Chapter Two presented a review of current users' privacy concerns in regard to different technologies. Then, Chapter Three presented an analyses of the current tools and solutions for protecting users' privacy and reducing their concerns. The outcomes of this stage have helped in identifying the research gaps.

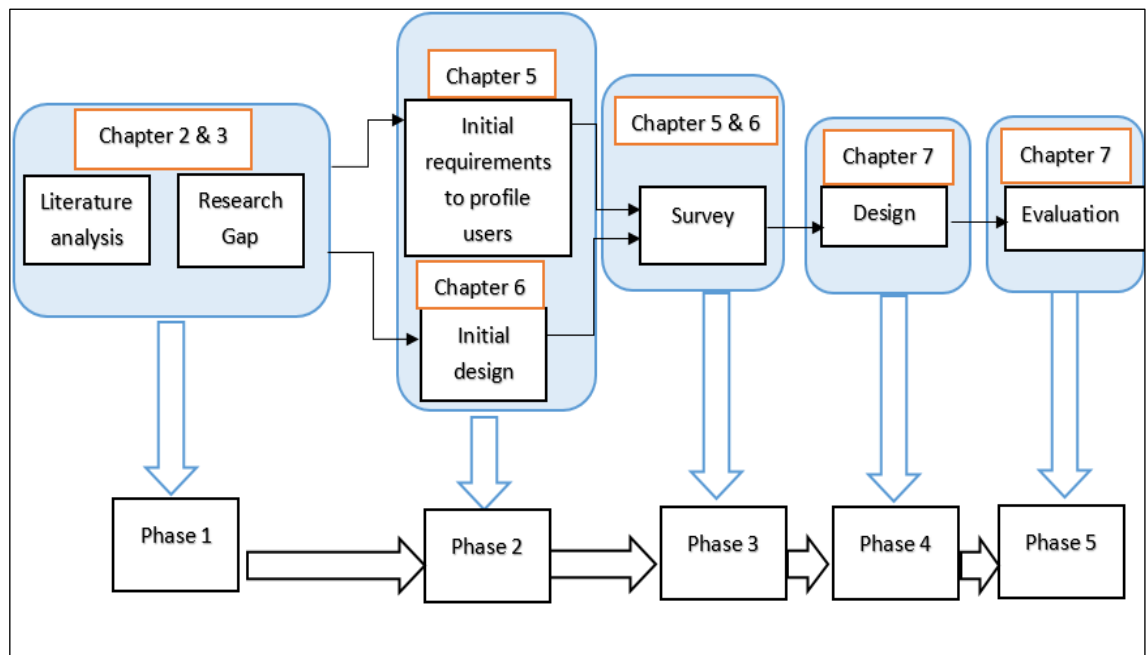


Figure 4.2: Research Processes

After understanding the problem, the thesis will discuss in detail how to address the problems (in Chapters 5 and 6). Accordingly, the initial potential requirements are described to build the system. This phase split has been into two components:

- Initial requirements to manage and prioritise the user's privacy-related information, which will be discussed in Chapter Five.
- Initial design, which will be discussed in Chapter Six.

A questionnaire has been designed in order to explore whether the initial requirements and design meet and cater to users' preferences. The questionnaire design will be

discussed in both Chapter Five and Chapter Six, and has involved employing a quantitative method. This study has used the questionnaire method because it provides researchers with quantitative data.

The outcomes of participants' responses have been utilised to refine the initial requirements and initial design, and prioritise privacy-related information. The resultant requirements and design choices finally led to building a holistic framework to enhance privacy technology. In phase 4, a Mock-Ups prototype was designed to help in visualising and better understanding how the framework would work in practice. Finally, a focus group has been conducted to evaluate designing a Mobile Device PET by end-users and experts. By using a quantitative survey and conducting focus group interviews with experts and potential users, this research has used a mixed-methods approach, albeit through different stages of the design iterations. According to Creswell (2014), using mixed methods allows the researcher to obtain essential quantifiable data on a matter, along with gaining more in-depth perspectives from key individuals. Therefore, the research has led to a thorough investigation of the proposed system for improving user privacy.

4.7 Questionnaires Design

One of the stages of this research is to design questionnaires in order to prioritise user information, identify what the current privacy preferences to manage privacy are, and also to investigate users' thoughts regarding the current design of interfaces and initial requirements. A questionnaire method was used to collect data because it has several important advantages for this research. It can provide researchers with quantitative data, which can be employed to cater for different user preferences and expectations. It also enables users to be divided into a smaller number of privacy profiles. Another advantage of the questionnaire method is that the researcher can reach a large number of mobile

users and can obtain more responses by using questionnaires, compared to the other methods such interviews. In addition, respondents may be more willing to answer sensitive questions at a convenient time on their own schedule.

One of the main goals of the questionnaire is to identify an effective method to prioritise user privacy-related information in order to overcome the burden related to managing such a large amount of information. To achieve this goal, it is important to determine the current privacy related-information. This represents a challenge due to the large volume of information in the current privacy settings in mobile operating systems such as Android and iOS, which are called permissions. Furthermore, the user's privacy information does not exist only on permissions, but there is much more personal information such as phone number, email, birthday and address, which may be shared with different apps which do not appear in the permission settings (Le, Varmarken, et al., 2015; Ren et al., 2016). Therefore, the current mobile privacy setting and the current user information in-apps have been studied and analysed to identify the users' information. Accordingly, an app privacy preferences section has been designed and organised along two dimensions: app categories and data type.

Due the questionnaire seeking to identify the current privacy preferences to manage users' privacy, the second part of the questionnaire needed be related to how to control the privacy-related information in order to meet the needs of the individual and their desire to control different aspects of their privacy. Hence, a tailored solution for users has been designed based on these needs.

Finally, a set of questions were drafted regarding usability in order to achieve the second research question, which is about how to present the information in a usable fashion. According to the literature review, there are several usability issues related to the interface displayed to users. Therefore, in order to develop usable and adaptive interfaces that

maximise prioritised privacy-related information, this research has investigated users' thoughts regarding the design of interfaces. Hence, four proposed interfaces have been designed (notifications interfaces, historical view, control and help and support). The aims of this procedure were to evaluate the following:

- If users are attracted by the use of colours in the interfaces.
- How easy user interfaces are to use.
- Whether the information provided by the software is easy to understand.
- If users are attracted by the use of icons.

Accordingly, and prior to recruitment for participation, eight subjects were asked to undertake a pilot study. A pilot study was conducted to verify that the survey instruments were understandable and reliable. The feedback from the pilot study was used to refine and enhance the survey questions.

As a result of the previous steps and processing, the survey was structured to include four parts:

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

4.8 Data Collection

The second stage of the design is discussed in this chapter, which aims to develop a new technique to prioritise privacy-related information and to develop usable and adaptive interfaces that maximise user satisfaction. In order to achieve these goals, a questionnaire was designed and participants were recruited to answer that questionnaire. The participants were recruited through a range of methods such as email, predominantly targeting students at the University of Plymouth, staff and colleagues in the Faculty of Science and Engineering, as well as friends. Additionally, it was published on Facebook, Twitter and WhatsApp. Some community centres in Plymouth were also requested to participate in the survey. Therefore, a sampling frame was not used for the current research because, as explained by Bryman (2016), representativeness was not a significant concern; rather, the views of a range of participants who use various apps was required.

Furthermore, the expected total of participants that complete responses should be within the range of other surveys in the research domain and close to the expected and targeted figure, which is about 300 to 500 participants (Watson, Lipford and Besmer, 2015; Chua and Chang, 2016; Wisniewski, Knijnenburg and Lipford, 2017). Moreover, according to Statista data, 4,978,317,680 adults own smartphones in the UK (Statista, 2017). Hence, in order to determine the sample size, the following formula was utilised for the sample size n :

$$n = N * X / (X + N - 1) \text{ where, } X = Z_{\alpha/2} * p * (1-p) / MOE^2,$$

$Z_{\alpha/2}$ is the critical value of the Normal distribution at $\alpha/2$ (e.g. for a confidence level of 95%, α is 0.05 and the critical value is 1.96), MOE is the margin of error, p is the sample proportion, and N is the population size. After applying this formula, the result was 384

people, which means this research needed this number of participants for statistically sound results.

All of the information from the questionnaires has been treated confidentially and respondents have been anonymised during the collection, storage and publication of the research material. Accordingly, it is worth noting that ethical approval (see Appendix B) was obtained, ensuring that this survey conforms to the ethical principles laid down by the University of Plymouth. Prior to displaying the questionnaire questions, its aims and structure were briefed, as well as confirming that the respondents should be 18 years of age or older, and they are free to withdraw up until the final submission of their responses (Appendix C).

4.9 Data analysis

Data analysis generates a set of scientifically valuable data, which was primarily utilised to determine the potential for improving the initial requirements for enhancing privacy technology. This also provided valuable insights on design for the third stage of the research design, which is about the development. To achieve these goals, it was important to identify which approach should be utilised to analyse the data.

Two approaches were used to analyse the data: machine learning to cluster users, and statistical analysis. In data science, clustering analysis helps in obtaining valuable insights from the data by seeing what groups the data points fall into. This technique is called unsupervised machine learning, and it aims to find similarities in the data points and collect similar data points together. However, there are two common methods used to cluster users - hierarchical clustering and k-means. Hierarchical clustering with an agglomerative approach is utilised to cluster users' mobile app privacy preferences. Hierarchical clustering provides a binary tree of the data that successively merges similar groups of points and visualise a useful summary of the data (Lin et al., 2014). Whilst the

K-means method assigns each data to the cluster whose centre, also called the centroid, is nearest. The centroid is the average of all the points in the cluster, and then the algorithm will assign each data point to its closest centroid point (Soni, 2012). However, hierarchical clustering is much more informative and more interpretable than other methods such as K-means. Moreover, determining the optimal number of clusters in K-means is a fundamental issue. Unfortunately, there is no definitive answer to determine the optimal number of clusters. The optimal number of clusters somehow relies on the technique used for measuring similarities. Therefore, different approaches for estimating the optimal number of clusters have been proposed (for example, statistical testing methods, visual exploration and precision of predicting users' preferences) (Liu, Lin and Sadeh, 2013).

Gap statistics were performed to determine the optimal number of clusters. The gap statistic compares the total within intra cluster variation for different values of k. This statistical approach avoids the increase or decrease in the monotony of other validation scores with the increasing number of clusters.

First, the intra-cluster distance is averaged over the k clusters:

$$W_k = \sum_{r=1}^k \frac{1}{2nr} \sum_{i,j} D(i,j)$$

Where nr denotes the number of elements of the cluster r.

The gap statistic is defined as:

$$\text{Gap}(k) = E(\log(W_k)) - \log(W_k)$$

Where $E(\log(W_k))$ is the expected logarithm of the average intra-cluster distance.

Another approach to determine the optimal number of clusters relies on how easy the cluster is to interpret and how meaningful the options are. The clusters that are easy to interpret would also make it easier for users to identify which cluster best matches their preferences.

The hierarchical algorithm begins with all the data points assigned to a cluster of their own. Then, two nearest clusters are combined into the same cluster. Ultimately, this type of clustering elapses when there is only one cluster left. In order to combine two clusters, this is based on the closeness of these clusters. To determine the closeness of clusters, there are multiple metrics:

- Euclidean distance: $\|a-b\|_2 = \sqrt{\sum(a_i-b_i)}$
- Squared Euclidean distance: $\|a-b\|_2^2 = \sum((a_i-b_i)^2)$
- Manhattan distance: $\|a-b\|_1 = \sum|a_i-b_i|$
- Maximum distance: $\|a-b\|_{\text{INFINITY}} = \max_i|a_i-b_i|$
- Mahalanobis distance: $\sqrt{(a-b)^T S^{-1} (a-b)}$ {where, s : covariance matrix }

In general, clustering can be a useful tool to explore how to divide users into unique groups, which in turn helps to understand how to prioritise users' information initially. However, in order to cluster the data, R code was utilised, which has an amazing variety of functions for cluster analysis. It also provides researchers with a wide variety of statistical and graphical techniques, classification, clustering, and others.

Unsupervised machine algorithm was not the only method utilised in this research, but supervised machine was also used to predict many of a user's mobile app privacy preferences, which could significantly reduce user burden with minimum questions.

Statistical analysis is another approach that was used in this research. It has been utilised to analyse users' thoughts regarding the design of interfaces, privacy controls and

management, and the correlation between participants' demographic characteristics and their preferences. SPSS software was utilised because is one of the most popular statistical tools used by researchers to attain a complex statistical analysis.

SPSS software provides the Pearson's coefficient correlation test to measure the correlation between two variables. It has a value of between +1 and -1 where 1 is a total positive correlation as the value of one variable increases, so does the value of the other variable. Whilst zero indicates there is no correlation, and -1 is total negative correlation as the value of one variable increases, the value of the other variable decreases. P-value determines if there is a statistically significant correlation between the two variables. When the p-value is less than or equal to .05, that means there is a statistically significant correlation between two variables.

In order to identify the strength of the Pearson's coefficient correlation test between two variables, Cohen, (1992) provides guidelines for the purposes of interpreting this strength, where $r = 0.10$, $r = 0.30$, and $r = 0.50$ indicate small, medium and large in magnitude, respectively, as shown in Table 4.3 .

Effect Size (Cohen)	
.10	Small
.30	Moderate
.50	Large

Table 4.3: The Strength of the Relationship

Accordingly, various approaches have been utilised in this research to analyse the data, which are summarised as follows:

- K-means and Hierarchical clustering, which was aimed at clustering users into a small number of privacy profiles

- Pearson's coefficient correlation, for the analysis of users' thoughts regarding the design of interfaces, privacy controls and management, and the correlation between participants' demographic characteristics and their preferences
- Supervised machine, which was aimed at predicting users' mobile app privacy preferences with a minimum number of questions

4.10 Evaluation

The evaluation of the framework is the third stage in the research design. Therefore, it is important to determine a suitable evaluation to ensure that the research objectives are met and they are as effective as they can be. Both qualitative and quantitative approaches can be used to evaluate a system (Howell, 2013). This research has used a qualitative approach to evaluate the system because it provides useful information to investigate users' acceptance and satisfaction in depth, which is difficult to achieve through purely quantitative approaches (Kaplan and Maxwell, 2005). This research has used a specific qualitative research method, the focus group method, which is an effective method for gaining details about the experiences of end-users and experts. Additionally, it provides content-rich, qualitative information and reveals insights that are difficult to capture with other methods.

4.11 Conclusion

This chapter has highlighted the philosophical systems, paradigms of scientific research and the strategy and the methodology adopted in this research. Moreover, the differences between each approach have been identified in order to explore their characteristics and strengths. By examining various research paradigms, the design science research paradigm was deemed a suitable approach for this research, which provides guidelines that have helped to create a discipline-oriented approach to the creation of successful artefacts.

This research has employed a survey questionnaire strategy, which is the most common method of data collection, and it helps to gain quantitative data. The quantitative approach helps to cluster users into a small number of privacy profiles, which is difficult to achieve these through a purely qualitative approach. However, a qualitative approach was also used to evaluate and investigate users' acceptance and satisfaction in depth, in order to gain content-rich, qualitative data that is difficult to capture with other approaches. The outcomes of this process have been used to determine the requirements for a mobile PET and have helped in designing and enhancing privacy technology.

Chapter Five

Requirements Analysis for Profiling Users' Privacy Information

5. Requirements Analysis for Profiling Users' Privacy

Information

Analysing and reviewing the current solutions in prior studies has revealed that current solutions have a lack of meeting users' privacy preferences in the context of how to manage and prioritise a large volume of data on mobile apps, which in turn leads to a lack of privacy protection. Therefore, this chapter seeks to identify the initial requirements based on prior studies in order to develop and enhance privacy technology and meet users' privacy preferences, which be discussed in the first section. One of the major requirements that will be presented in the first section is to prioritise privacy-related information, which would play an essential role in discovering how to manage a large volume of data.

The initial requirements have been utilised in the survey to verify and explore the current privacy preferences regarding the prioritisation of privacy-related-information and how to manage it. Moving forward, the outcomes of the survey will be discussed in this chapter, which in turn leads to an analysis of how to cluster the entire user population into a number of subgroups.

5.1 Initial requirements analysis

It is evident from the current literature review that prior research is lacking in some areas with regard to enhancing the privacy of mobile technology from the following aspects:

- Prioritisation of privacy-related information.
- Adapting privacy to the user's knowledge
- Fine-grained privacy control
- Transparency features

Accordingly, the subsequent sections will discuss how to address these problems. Previous studies have provided valuable insights and suggestions that can help to enhance the current privacy-related problems.

5.1.1 Prioritisation of privacy-related information

Users are sharing large amounts of personal information through a large volume of apps such as WhatsApp, Facebook, Twitter, Fitbit and the Amazon app. As seen in the literature review, most studies have assumed that users can manage and control such a large amount of information. Therefore, they have provided users with a mechanism to allow them to control access to sensitive data. However, users are likely to struggle to manage such a large volume of information as they are quite complex and change frequently (Liu, Lin and Sadeh, 2013).

In order to overcome the burden related to managing such a large amount of information, prior works have proposed that, despite the diversity of users' privacy preferences related information, it is possible to divide a user's mobile app privacy preferences into different profiles as the default settings for initial interfaces, which could significantly reduce the user burden (Liu, Lin and Sadeh, 2013; Lin et al, 2014a; Watson, Lipford and Besmer, 2015). For instance, some studies such as Mugan, Sharma and Sadeh (2011) and Lin et al., (2012) used this approach in location privacy to reduce the user burden, which involves the identification of privacy profiles. Another study by Watson, Lipford and Besmer (2015) also used this approach in social media and they found that the user privacy preferences of profile items and disclosure can be utilised to create initial privacy settings that better represent user preferences. Moreover, Lin et al. (2014) indicate that applying privacy profiles as default settings for initial interfaces could significantly reduce the burden and frustration of the user.

Accordingly, in order to cater to different user preferences and expectations related to privacy information initially, user profiling could be utilised to cluster users into a smaller number of privacy profiles. The strength of this approach lies in its ability to closely capture the users' preferences, which in turn should reduce individual user's burden and frustration.

5.1.2 Adapting privacy to the user's knowledge

Nielsen (2010) claims learnability is in some sense the most essential usability characteristic because most of the systems require being easy to learn, and a transition from a novice to an expert. Moreover, prior research has shown that considering the knowledge of users during the design can improve user performance, satisfaction and experience (Hwang and Yu, 2011; Chua and Chang, 2016a). In the context of privacy, Wisniewski et al. (2017) state that users differ significantly in how they learn and use different privacy mechanisms on Facebook. This draws attention to the paramount importance of considering users' needs and expertise during the design of the system, which in turn could help to attain greater usability.

Accordingly, the goal of this requirement is to make the system understandable and learnable for the novice user, while at the same time not hindering the advanced user from working productively. Researchers in the HCI domain have pursued identifying who is a novice and expert, and their role in order to be accommodated while designing the interface. Nielsen (2010), for instance, states, "*Expert users are defined as individuals who have rich interaction knowledge, task knowledge, and domain knowledge of a specific system*". Whilst novice user is defined as "*a user who is trying to complete the task in the system but has little or no past experience, have less interaction experience*". Therefore, they need additional help and support such as documentation, tutorial guides, and help in terms of how to manage and control a large volume of data. As the user takes

on board more knowledge about how to use the system, their 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.

5.1.3 Fine-grained privacy controls

According to the literature review in Chapter Three, most current privacy solutions support only a binary and static privacy control approach. This approach provides the user with two options - “*allow*” or “*deny*” - an application’s access to their private information. To overcome this limitation, Almuhimedi et al. (2015) developed a tool to notify the user about how their personal information is accessed by an app, and whether they are allowed to control their privacy preferences in an appropriate manner. TISSA (Zhou et al., 2011) also provides users with empty or bogus options for personal information, whilst AppFence (Hornyack et al., 2011) sends shadow data instead of the actual data. Bugiel et al. (2013) suggest involving the user in selecting their privacy configuration because the user’s privacy protection strongly depends on the subjective security objectives of the individual user. Consequently, the system allows users to modify their privacy settings when they realise the potential risks of using an app. Moreover, Kim et al. (2017) suggest considering multi-level privacy controls in order to achieve more flexibility in providing their private information to mobile apps and to meet users’ privacy requirements. Therefore, providing users with multilevel privacy controls allows them to limit the disclosure of their private information on multiple levels by taking factors related to the level of the user’s knowledge into account.

5.1.4 Transparency feature

According to GDPR guidelines, users have the right to be informed about the collection and use of their personal data through clear and concise information (GDPR, 2018). This

is an essential transparency requirement under the GDPR. Moreover, Christin et al. (2013) show that users desire to have a historical view to know who has accessed their data. Another study's findings emphasise that there is a strong need for more transparency to reduce users' privacy concerns and lead to more trust in services (Alrayes and Abdelmoty, 2016). It can be deduced from these findings and suggestions that a certain level of transparency would be useful to enhance privacy technology and increase user awareness. Therefore, the proposed system should allow 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. However, other prior requirements such as the user's knowledge pose different dimensions that should be considered and combined during the design of the system in the context of how to help a novice user to understand the historical interface. This would allow an advanced user to know who had access to which data, at which degree of granularity and when, without confusing novices

5.2 Methodology

This section seeks to explore how to design the privacy-related information section in the survey and how to present this information to the participants in an effective way. As previously mentioned, one of the essential requirements is to identify an effective method to prioritise users' privacy-related information in order to overcome the burden related to managing such a large amount of information. To achieve this objective, it is paramount to find out about the current privacy related-information on mobile apps.

5.2.1 Privacy related information categorisation

Due to mobile apps storing and sharing a large volume of information, this information needs to be analysed and determined before it is presented in the survey. Hence, different steps were performed to identify the current user's information.

First, Android and iOS were analysed to identify the privacy control settings. According to the Apple website, iOS provides users with settings which help them to see which apps they have permitted to access to certain information to, as well as granting or revoking any future access (Apple, 2015). This includes access to:

- Contacts
- Reminders
- Microphone
- Calendars
- Location Services
- Media library
- Camera
- Music and video
- HomeKit
- Photos
- Bluetooth sharing
- Photos
- Health
- Motion activity
- Speech recognition
- Apple Music

For Android, Google has included app permissions that allow users to selectively grant or restrict permissions for installed apps. Therefore, Android permissions were studied and it was found for this group of data (Google, 2015) that the following information is included:

- Activity_Recognition
- Storage
- Sensors
- Call_Log
- Calendar
- Sms
- Microphone
- Location
- Camera
- Contacts
- Phone

Thus, iOS and Android have some similar data sharing, such as location, calendar, motion activity and contacts. Furthermore, the user's privacy information does not exist only on permissions, but there is a lot of personal information such as phone number, email, birthday and address being shared with different apps which do not appear in the permissions settings (Le, Varmarken, et al., 2015; Ren et al., 2016). Zang et al. (2015) analysed network traffic and found that 73% of Android apps shared personal information such as email address, birthday and name with third parties. Moreover, their analysis of the results revealed that three out of the 30 health and fitness category apps in the sample

share user input with a third party. Another study found that health apps collected PII such as name and address as well as demographic data (e.g., date of birth, gender) and potentially sensitive data about activities (e.g., location, heart rate), nutrition, or medical data (Wagner et al., 2016). These studies indicate that there are different types of personal information being shared with different apps which do not appear in the permissions settings. Hence, these types of information were considered during the analysis to understand what types of data are collected by mobile apps.

Each group of data contains multiple data sources, for example motion activity contains: steps, location, calories, heart rate in beats per minute, height, speed and weight, which means there is an enormous amount of personal data that would take a long time and be difficult to answer by the participants. Therefore, to minimise the questions, data that have a similar impact were grouped into eight categories: geographical location, identity, health information, phone information, calendar, multimedia information, contact and motion activity, as shown in Table 5.1.

Data group	Data type
Health information	Heart Rate, ECG, Steps, Weight, Sleep Tracker, Place Tracker, Medical Data, Health History, Blood glucose
Personal Information	Address, Gender, Name, Date of Birth, Email, Postal Code
Location	Approximate location, Exact location
Phone Information	Device Id, call log, phone number
Calendar	Calendar
Multimedia information	Voice record, Photos, Videos
Contacts	Read contacts, modify Contacts, Social media accounts
Motion activity	Steps, calories, , height, speed and weight

Table 5.1: Data Group

5.2.2 Privacy-related information Questions

After determining the privacy-related information categorisation, it is important to identify how to present this information to the participants an effective way. According to a study by Felt et al. (2012) participants understand data types better when the data is associated with a familiar application. For example, a participant who does not understand the motion activity data in isolation might know that data is needed to record details about their activities when he or she has decided to use a fitness application. Therefore, each app category is associated with various data types. However, in order to ensure that participants fully understood the questions, these steps were performed:

- A number of people were asked if they could understand the data type associated with a familiar application in order to observe their understanding before publishing the survey.
- Each data type category includes some example that are related to the category, for instance, motion activity (steps, calories burned and sleep duration).
- These questions were presented to non-expert users to evaluate user understanding.
- The data type is short, simple, and non-technical.

The app privacy preferences section in the survey were refined and enhanced after performing the previous steps. For instance, some participants may not understand the app category; therefore, some app categories were displayed with some definitions and examples. Additionally, each app category includes photographs for some apps under these categories to help the participants to understand each category. Accordingly, the App privacy preferences section includes the following steps in order to make sure that participants understand each question:

- The definition of some categories

- Display photographs for some apps under these categories to help the participants to understand each category
- Display some examples for each category.

After processing these, the app privacy preferences section was organised along two dimensions: App categories and data type. Hence, eight app categories were associated with various data types. Table 5.2 shows 46 cells that represent the 8 app categories with their data types. Accordingly, the following question was asked participants in the survey:

“Different types of applications capture and process a variety of different types of privacy-related information, the following questions will ask you how concerned you are about such privacy-related information being shared by different categories apps”

Data Type	App Category							
	Game	Health	Fitness	SN	Shopping	Productivity	Lifestyle	Navigation
Approximate Location	✓	✓	✓	✓	✓		✓	✓
Exact Location	✓	✓	✓	✓	✓		✓	✓
Identity	✓	✓	✓	✓	✓	✓		
Contact	✓	✓	✓	✓	✓	✓	✓	✓
Multimedia	✓		✓	✓	✓	✓	✓	✓
Health Information		✓						
Phone		✓		✓	✓	✓	✓	✓
Motion			✓					
Calendar				✓		✓	✓	

Table 5.2: App categories and data types

- **Game and entertainment category question**

Mobile users can install various game apps such as Angry Birds, Candy Crush and Roblox, which could access to user's data. Therefore, this category includes the following

primary data types: approximate Location, Exact location, Identity (e.g. date of birth and name), contact, multimedia (e.g. photos and videos).

- **Health category question**

“Suppose you installed an application which is developed by a trusted medical provider eg NHS, could you please indicate your concern about letting the application send the following information”.

Chapter 2 revealed users would like to know and be able to control their health information because they are concerned about the sharing of that health information and fitness. Therefore, the survey includes the health category and fitness in order to investigate user concern regarding sharing their data with these apps.

- **Social Networks Category question**

Social media apps dominate mobile device users' time. Social networks category allow users to share many different types of information such as identity, location and multimedia. Therefore, it is important to involve the social network category in the survey.

- **Shopping category question**

Shopping applications also have direct access to sensitive information as discussed in Chapter 2. Therefore, the survey includes a shopping category to explore users' concerns regarding these apps.

Productivity apps, lifestyle apps and navigation apps can access users' private data. Therefore, the survey includes these categories with their data types. Hence, the app privacy preferences section in the survey included most app categories in a mobile device with various data types to explore users' privacy concern regarding these data, which in

turn, makes the survey comprehensive for most users' data. This section would help to divide the participants' preferences into a number of subgroups.

- **Demography questions**

Other questions related to demography were included in the survey, which included the following characteristics: gender, age, education level, occupation and the level of knowledge. The demography questions aim to explore whether there is a correlation between user preferences in the context of prioritisation of the information; users' knowledge about privacy apps on their mobiles, and managing and controlling settings and usability. Moreover, demographic characteristics have been investigated to look at whether users' demographic information, including age, gender and education level, could be utilised to assign the user to the closest profile.

- **Privacy control and management questions**

The third part of the questionnaire is about privacy control and management. It presents questions related to how to control the privacy-related information in order to meet the needs of the individual and their desire to control different aspects of privacy. Hence, a tailored solution for users could be designed based on these needs.

“Following statements about the privacy control and management. Would it be useful to have the following settings:”

- **Ability to control information across different apps**

This question is about the ability to control information across different apps. This question aimed to find out users' desire to control the information they share.

- **Display multi-level privacy control e.g. (No access, Low access, and Full Access)**

The second question is regarding the display of multi-level privacy controls (e.g. No access, Low access, and Full Access). This question was not only to find out the user's desire to have multi-level privacy controls, but explored if there was any correlation between users' demography and multi-level control.

- **Ability to change the privacy notification settings for different apps**

Another question is related to user notifications in order to notify users at the moment that data was being sent. However, the question here aims to find out users' satisfaction with being allowed to change the privacy notification settings for different apps.

- **Ability to restrict the time period of sharing your data**

As discussed in Chapter 3, none of the prior studies has considered that sharing personal information differs from time to time and from person to person. Therefore, this research seeks to explore end-users' perceptions and attitudes towards adding this feature that allows the user to restrict the time period of sharing data.

Permission settings questions.

“Read each statement carefully and indicate your level of knowledge about the privacy of apps : (all the statements are related to your privacy apps on your mobile)”

- **Understanding what permissions apps are seeking before installing.**

This question aims to find out the extent of the user understanding the app's permission. Moreover, this question aims to explore if there was any correlation between users' knowledge and understanding apps permissions.

- **How to change privacy settings for the apps.**

Due to users' concerns about the privacy protection related to mobile devices, most mobile operating systems such as Android and iOS provide some privacy safeguards for

users. Therefore, this question seeks to investigate user knowledge about these settings in the current mobile device. Moreover, this question would help to explore if there was any correlation between users' knowledge and understanding how to change privacy setting for apps.

- **Understanding privacy policy for the apps.**

This question aims to explore if there was any correlation between novice, intermediate and advanced participants and their understanding for a privacy policy.

The targeted participants were public users who are 18 years or above and have a smartphone. The participants were asked how concerned they are about such privacy-related information being shared by different categories of mobile apps on a five point Likert scale (from extremely concerned to Not at all concerned). Regarding the rating scales, this questionnaire has utilised a five-point Likert scale. Most rating scales, including Likert-type scales, contain either five or seven response categories (Peter, 1979; Bearden and Netemeyer, 1999). However, a seven-point Likert scale may be more time consuming for the participants answering the questions to make a decision. Moreover, prior studies recommend a five-point scale as it has been shown to be less confusing and to increase the response rate (Babakus and Mangold, 1992; Devlin, Dong and Brown, 1993).

5.3 Analysis of the Results

This section presents the results of the survey that was conducted to investigate current users' mobile app privacy preferences. 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 (Watson, Lipford and Besmer, 2015; Chua and Chang, 2016b; Wisniewski, Knijnenburg and Lipford, 2017b). Moreover, according to the

formula that was discussed in Chapter Four, in order to determine the expectation of sample size for the UK, the total of estimated participants were 384 people. Hence, the total number of participant responses that were collected in this survey almost corresponds to the sample size expectation and with prior studies.

5.3.1 Demographic

Demographic information was collected, including questions related to gender, age, education, and occupation in order to analyse the data, although the age ratio or any other demographic composition of the participants were not specifically controlled. Among these participants, 70% of them were male whilst the remaining respondents were female, as illustrated in Table 5.3. With regard to the age groups, more than half of the participants were between 18 and 34, and 35% of them are between 35 and 44 (see Table 5.3).

Factor	Category	Count	Percentage	Factor	Category	Count	Percentage
Gender	Male	285	70%	Occupation	Student	88	21.60%
	Female	122	30%		Employed Full time	273	67.10%
Age	18-24	34	8.40%		Employed part time	10	2.50%
	25-34	191	46.90%		Unemployed	34	8.40%
	35-44	141	34.60%		Retired	2	0.50%
	45-54	37	9%		Education	High school and lower	16
	55-64	3	0.70%	College certificate		30	7.37%
	65+	1	0.30%	Bachelor		149	36.60%
Postgraduate				212		52.10%	

Table 5.3 Summary of Respondents' Demographic Characteristics

Being within an academic institution, nearly 82 percent of the participants have a bachelor or postgraduate degree, more specifically, nearly half of the participants have postgraduate degree. Despite the analysis of the results of this survey possibly being skewed towards gender and education, the sample size appears to be a relative

representation of mobile users. Moreover, it is in-line with the United Kingdom's Office of National Statistics analysis that the age group (18-44), regardless of gender differences, were found to be the highest mobile users (Ons.gov.uk, 2018).

5.3.2 Users' Average Preferences and Their Variances

In order to analyse the users' preferences, the responses were transformed into a value number from one (extremely concerned) to five (Not at all concerned). To visualise the results, heat maps were utilised in 2D to display users' average preferences for all 407 participants in a data matrix, as shown in Figure 5.1. Red cells indicate a higher level of concern, while green cells indicate a lower level of concern. The empty cells indicate the absence of data for a particular data type. For example, according to prior studies, fitness apps sent motion activity information (steps, calories burned and sleep duration) out of the smartphone, whilst others app categories do not. Likewise, health information was shared only by the health categories.

The three use cases with the highest levels of concern were game category, which shared multimedia and contact data (multimedia: $\mu = 1.51$, contact: $\mu = 1.67$); SN which shared multimedia, contact and phone information (multimedia: $\mu = 1.73$, contact: $\mu = 1.86$), and the third highest level of concern was the shopping category, which shared multimedia (multimedia: $\mu = 1.88$). This indicates that multimedia information presented the highest level of concern for the participants, whether in the game, SN or shopping category.

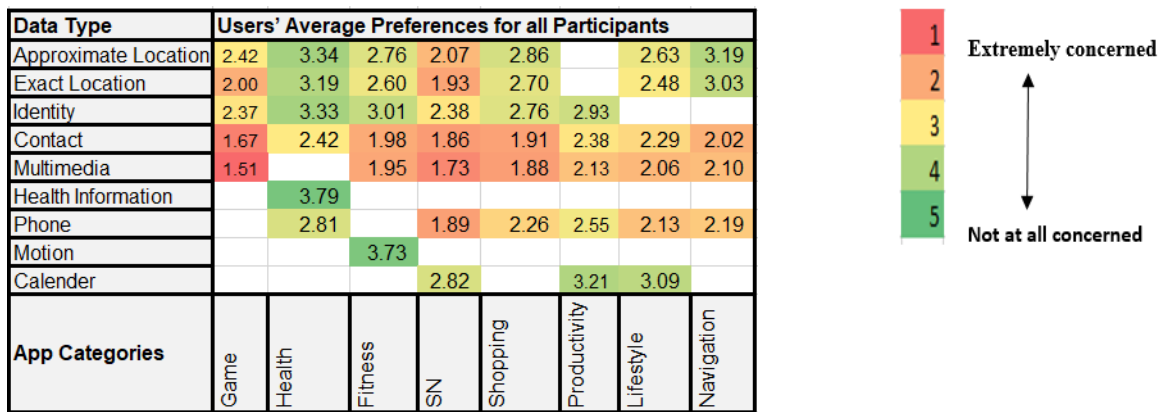


Figure 5.1: Average User Preferences

Participants are generally less concerned when an app category shares personal information related to the app’s core functionality. For example, the fitness category that shares motion data which represents a core functionality for this category ($\mu = 3.73$) and navigation which shares location (exact location $\mu = 3.03$; approximate location $\mu = 3.19$).

Regarding the exact location, participants are less concerned when app health, shopping and navigation categories share personal information related to the exact location ($\mu = 3$).

Whilst, participants are highly concerned about sharing exact location with the game and social media category $\mu = 2$. When the exact location result compares with the multimedia in the social media category, which is the lowest level of concern, the conclusion that there is no statistically significant difference between them.

In term of category, participants are highly concerned about sharing their information with the game category $\mu = 2$. On the contrary, participants feel more comfortable sharing their information with the health category $\mu = 3.14$. This result suggests that participants are unconcerned when a trusted app such as the NHS shares their information. For the remaining categories, the participants expressed different levels of concern.

The overall insight into participants’ average preferences shows a good starting point to understand the current users’ privacy preferences. However, the outcomes of the average for each category for all participants do not show much diversity in users’ privacy

preferences, yet according to the literature review, users' privacy preferences are diverse. Therefore, a serious move towards finding the variances in user preferences in each category in each app was necessary, as shown in Figure 5.2.

The darker shades of red in Figure 5.2 indicate lower variance among users' concern ratings for different categories. The variance outcome shows that users' preferences are definitely diverse. In general, variances are larger than 0.8 (of a rating in a [1 to 5] scale) in all cases and lower than three. Even though Figure 5.2 shows participants were somewhat unconcerned about their information being shared by the health category, the variance outcome implies that participants' preferences for the health category are in fact different, and represent the highest variance among the participants.

The multimedia information in-game category appears the highest diversity among the participants. Whilst, the approximate and exact location for the navigation category also show the highest diversity among the participants. The outcomes of these results show that multimedia information presented the highest level of concern for the most participants, whether in the game, SN or shopping category.

By looking at categories, the game category shows the lowest diversity among the participants. Moreover, the highest levels of concern were game category. This indicates that multimedia information presented the highest level of concern for the participants across different categories and most participants in the game category were conservative. This variance indicates that users' privacy-related information could not adequately be captured by a one-size-fits-all default approach. Therefore, it is important to move toward a depth of analysis for the data to find out the similarities and differences between the participants.

Data Type	Variances in User Preferences							
Approximate Location	1.65	2.0564	1.939	1.57	2.1176		1.924	2.47
Exact Location	1.49	2.2508	2.044	1.56	2.2548		2.038	2.65
Identity	2.04	2.3585	2.258	2.03	2.1882	2.17		
Contact	1.13	2.2237	1.738	1.48	1.5911	1.93	1.87	1.77
Multimedia	0.89		1.593	1.34	1.5082	1.75	1.73	1.96
Health Information		1.8025						
Phone		2.541		1.55	2.0502	1.93	1.774	1.94
Motion			1.928					
Calender				2.36		2.19	2.203	
App Categories	Game	Health	Fitness	SN	Shopping	Productivity	Lifestyle	Navigation

Figure 5.2 Variances in User Preferences

5.3.3 Privacy Profiling

This section aims to find out how to cluster the entire user population into a number of subgroups in order to cater to different user preferences and expectations related to privacy information initially, user profiling could be utilised to cluster users into a smaller number of privacy profiles.

Due to the dataset size is small, this research follows these processes:

- Performing simple machine learning algorithms.

As a general rule associated with machine learning, the simpler the model, the better it learns from small datasets. Therefore, when it comes to small datasets, models require low complexity to avoid overfitting the data. For this reason, low-complexity machine learning such as hierarchical clustering, k-means and SVM would be utilised in this thesis as they are more likely to work well with smaller datasets (Lin et al, 2014a; Akman et al, 2019).

- Statistical testing methods, visual exploration, and the precision of predicting users' preferences have been used to validate the clusters.
- Cross-validation have been performed in a supervised machine learning algorithm.

Unsupervised machine learning was performed to obtain valuable insights from the data by seeing what groups the data points fall into. Before clustering the entire user population into a number of subgroups, the users' preferences were encoded into a vector. After these pre-processing steps, a matrix of 46 columns which represent self-reported concern ratings of different data types, and 407 rows, were obtained, where each row of the matrix represents a participant. This step yielded a total number of 407 unique participants with 18,722 responses. Each entry on the matrix was a value between one and five.

Two algorithms were utilised to cluster users' preferences into subgroups: k-means and hierarchical cluster. As discussed in Chapter Four, determining the optimal number of clusters in a data set is a fundamental issue in K-means clustering. Therefore, different approaches for estimating the optimal number of clusters have been proposed:

- Statistical testing methods
- Visual exploration
- The precision of predicting users' preferences

Gap statistics were performed to determine the optimal number of clusters. The gap statistic compares the total within intra cluster variation for different values of k. The optimum number of clusters is the smallest value of k. It is clear from Table 5.4 that the smallest sum of errors is the fourth cluster.

No. of Clusters (K)	Sum of Errors
1	0.0131
2	0.0102
3	0.0096
4	0.0095
5	0.0105
6	0.0103
7	0.0098

Table 5.4: Clustering Error

Visualisation of each profile would also make it easier to interpret the cluster. Hence, it helps to determine the optimal number of clusters. To demonstrate the meaning of each cluster, the centroid of each cluster was computed by averaging the feature vectors of instances within the cluster.

Figure 5.3 shows that when the users' preferences were divided into more than four clusters, it will be more difficult to interpret each cluster. For example, when there are six clusters, cluster 2, 3 and 4 are similar (close) to each other. The centroid for cluster 2, 3 and 4 are 2.3, 2.63 and 2.71. In addition, both cluster 5 and 6 are almost close to each other, which represents unconcerned users. When there are seven clusters, the centroid for 2, 3, and 4 are also similar to each other. However, as the number of clusters increases, the similarity between the clusters gradually increases too. Therefore, when the number of clusters is four, it is easy to interpret and meaningful. Lin et al. (2014) also found four clusters useful, but they used hierarchical clustering with Canberra distance. They named each cluster based on their characteristics: conservatives, unconcerned, fence-sitters, and advanced users.

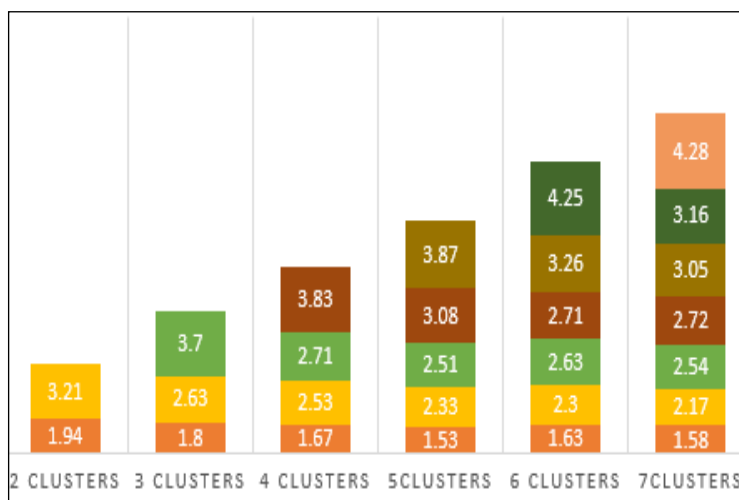


Figure 5.3: Average of Each Cluster

Multi classifications were performed to determine the optimal number of clusters. The results present the accuracy from determining each user to the cluster. In other words,

when the classifier has a high prediction of determining each user with their cluster and has high accuracy, this indicates that the number of clusters is good to utilise. Table 5.5 shows that both the number of cluster three and four have high accuracy (0.84 and 0.82) and high prediction. On the contrary, when the number of clusters is more than four, the correct prediction will decrease.

No. of Clusters (K)	Accuracy	Lowest Prediction Cluster
3	0.84	Cluster 2=77.8%
4	0.82	Cluster 3=70%
5	0.80	Cluster 1= 68%
6	0.75	Cluster 6=40%

Table 5.5: The Accuracy of Predicting Users' Preferences

Different methods were used to determine the optimal number of clusters in a data set. These methods include precision of predicting users' preferences, the interpretability and understandability, and the gap statistic method. The results from the three methods show that four clusters is the optimal number of clusters. Despite three clusters showing the highest accuracy, four clusters has the smallest sum of errors and it is easy to interpret and more meaningful. Moreover, it is similar to the number of clusters that were found by Lin et al. (2014) in their study.

Looking more deeply into the size of participant groups all four clusters, cluster 2 represents the largest participant groups (33 %) compared to the others. In order to understand the characteristics of each cluster, the average of each app category and data type was computed for each cluster. Cluster 3 represents the most conservative group because this group were extremely concerned about most of the data. Furthermore, the average of the cluster 3 is ($\mu= 1.7$) which indicates this group felt uncomfortable with mobile apps that want to share their information. In terms of people who are comfortable with disclosing their data, cluster 4 has the largest area, covered in the green colour (indicate unconcerned). In general, participants who share this privacy profile are between

slightly concerned or not concerned. Moreover, the average of the cluster 4 is ($\mu= 3.8$) and represents the lowest participant groups (14 %).

However, due to difficulties predicting the number of clusters in the k-means method and hierarchical clustering, it is easier to decide on the number of clusters by looking at the dendrogram, and so hierarchical clustering was performed in this research. Moreover, hierarchical clustering is much more informative and more interpretable than other methods such as k-means.

Agglomerative hierarchical clustering has different methods for measuring the dissimilarity between sets of observations, such as average, single, complete, and ward. Therefore, it is important to determine the best method which can be used to measure the distance between pairs of observations. However, R code provides a function to attain the agglomerative coefficient, and it measures the amount of clustering structure found (values closer to 1 suggest a strong clustering structure). Table 5.6 shows the agglomerative coefficient for different methods. Ward’s method is the strongest clustering structure out of the four methods assessed, as shown in Table 5.6.

Average	Single	Complete	Ward
0.7676869	0.5390081	0.8725427	0.9710358

Table 5.6: The Agglomerative Coefficient for Different Dissimilarity Methods

After performing Ward’s method, a dendrogram was used to represent the hierarchy of clusters. Figure 5.4 illustrates the resulting dendrogram produced by the above-mentioned clustering configurations, where different colours indicate the ten clusters when $k=10$. The dendrogram for the hierarchical method indicates that the number of clusters is more than the k-means method, which means that different groups share similar data.

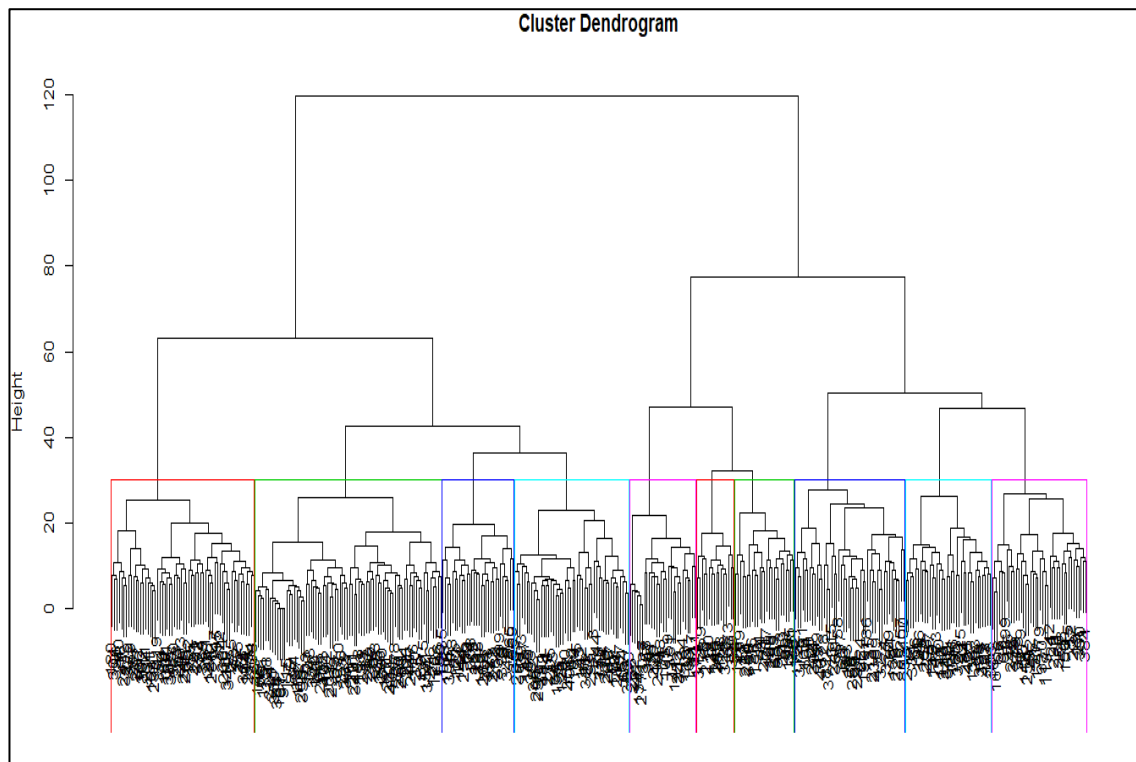


Figure 5.4: The Resulting Dendrogram Produced by Hierarchical Clustering

However, to simplify each cluster analysis and make it easy to extract the output of data analyses, the result was visualised on a scatter plot, as shown in Figure 5.5. Cluster 5 is the largest cluster compared to others, while cluster 10 is the smallest. Furthermore, looking at the distances between the clusters, it shows that cluster 4 is far from cluster 8. These outcomes trigger many questions regarding the reasons that make these clusters different from each other. Therefore, more analysis is required in order to understand the characteristics of each cluster and the disparity between them.

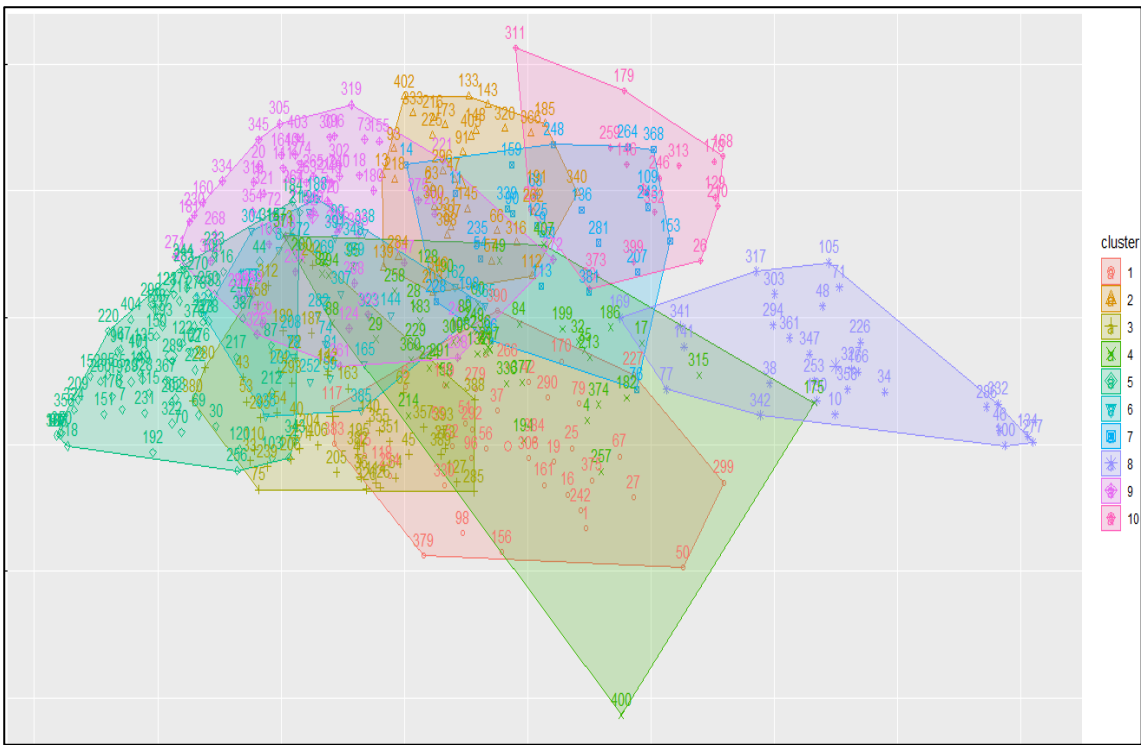


Figure 5.5: Visualisation the Clusters Result in a Scatter Plot

In order to understand the characteristics of each cluster, the average of each app category and data type was computed for each cluster, as shown in Table 5.7. Red cells indicate a higher level of concern, while green cells indicate a lower level of concern. Cluster 5 represents the most conservative group because this group were extremely concerned about most of the data. Furthermore, Table 5.8 shows that the average of cluster 5 is ($\mu=1.4$) which indicates this group felt uncomfortable with mobile apps that want to share their information, even if it is a trusted app such as NHS which shares their information. Looking more deeply into the size of participant groups, cluster 5 represents the largest participant groups compared to the others. By looking into the demographic characteristics, the largest numbers of postgraduate participants fall into cluster 5, which in turn could suggest why cluster 5 is the most conservative group. This poses another dimension to the characteristics of cluster 5.

App category-Data	Cluster									
	1	2	3	4	5	6	7	8	9	10
Game	2	2	2	2	1	2	2	3	1	3
Health	2	4	2	4	2	2	4	5	4	4
Fitness	3	3	2	4	2	2	4	4	2	4
SN	2	2	2	3	1	2	2	4	2	4
Shopping	4	3	2	2	1	3	3	4	2	3
Productivity	3	3	2	2	2	3	4	5	2	3
Lifestyle	3	2	3	2	1	2	3	4	2	4
Navigation	3	3	2	3	1	3	3	5	2	3
Approximate Location	3	3	2	3	2	3	3	4	2	4
Exact Location	3	3	2	3	1	2	3	4	2	4
Identity	3	4	2	3	2	2	4	4	3	4
Contact	3	2	2	3	1	2	2	4	2	2
Multimedia	3	1	2	3	1	2	2	4	1	2
Phone	3	2	2	3	1	2	3	4	2	3
Calendar	4	4	2	3	2	3	4	5	3	5

Table 5.7: Average of Each App Category and Data in Each Cluster

Clusters 3, 9, and 6 represent participants who are moderately concerned about sharing privacy-related information with the apps. When the centroid of each cluster was computed by averaging the feature vectors of instances within the cluster, clusters 3, 9, and 6 indicate moderately concerned at $\mu=2.07$, $\mu=2.13$ and $\mu=2.33$ respectively, as shown in Table 5.8. Nevertheless, despite the centroid of clusters 3, 9, and 6 being quite similar, the participants have different levels of concern regarding the app category and data type. For instance, cluster 9 is extremely concerned about the game category, whilst cluster 3 and 6 are not. This observation raises an essential question regarding the variance between quite similar clusters because the significant variance similar cluster could possibly help to identify each profile. When each cluster in Table 5.7 was analysed, the outcome revealed that each cluster has a unique profile, even though there are some similarities between some clusters.

Cluster Ranking	Average of each cluster
Cluster 5	1.4
Cluster 3	2.07
Cluster 9	2.13
Cluster 6	2.33
Cluster 2	2.73
Cluster 4	2.87
Cluster 1	2.93
Cluster 7	3.07
Cluster10	3.47
Cluster8	4.2

Table 5.8: Cluster Ranking With the Average

In terms of people who are comfortable with disclosing their data, cluster 8 has the largest area, covered in the green colour (indicate unconcerned). In general, participants who share this privacy profile are between slightly concerned or not concerned. On the contrary, the game category shows most concerned for cluster 8 and 10, which implies that groups are not unconcerned regarding all information. However, these groups (cluster 8 and 10) represent 10% of all the participants, which indicates the unconcerned groups are a small number of participants compared to the other groups who are most concerned. A closer analysis suggests a possible interpretation that it might be the age groups of participants that plays a role in the falling into these groups because 63% of participants are age between 18 and 34 in cluster 8.

In terms of the social psychology of privacy, an interesting finding from the analysis is that the preferences of the conservative group were the largest group, whilst Westin found that small numbers of users would fall at both extremes of the spectrum (i.e. privacy fundamentalist, and unconcerned) (Kumaraguru and Cranor, 2005). A possible interpretation might be that nearly half of the participants have a postgraduate degree in the whole dataset, as discussed in the demographic section, which may play a role in the appearance of a large number being conservative, as shown in the analysis of the dataset.

Overall, the result of analysing of the ten clusters has revealed a significant variance between each cluster, which in turn could possibly help to predict many of the users' preferences. Otherwise, users have to manually configure, which could significantly increase the burden on, and frustration of, the users.

In terms of privacy knowledge, the results show that almost half of the participants were intermediate. Whilst 20% of them were a novice and 31% were advanced users, as shown in Figure 5.6. Regarding the question about understanding privacy settings for the apps, 26% of participants rated themselves as extremely knowledgeable. The vast majority of them were advanced users.

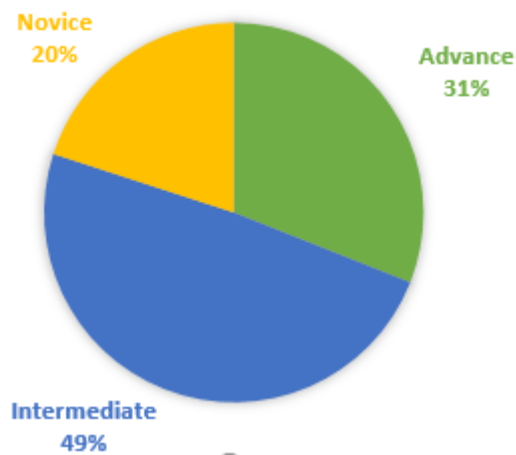


Figure 5.6: The Percentage of Novice, Intermediate and Advance

On the other hand, 71% of participants who chose “Not knowledgeable at all” were novice users, as shown in Figure 5.7. In addition, there was a positive correlation between the levels of knowledge about the privacy of apps and understanding the privacy settings of 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, there was a positive correlation ($r = 0.524$, $p < 0.00$) as well.

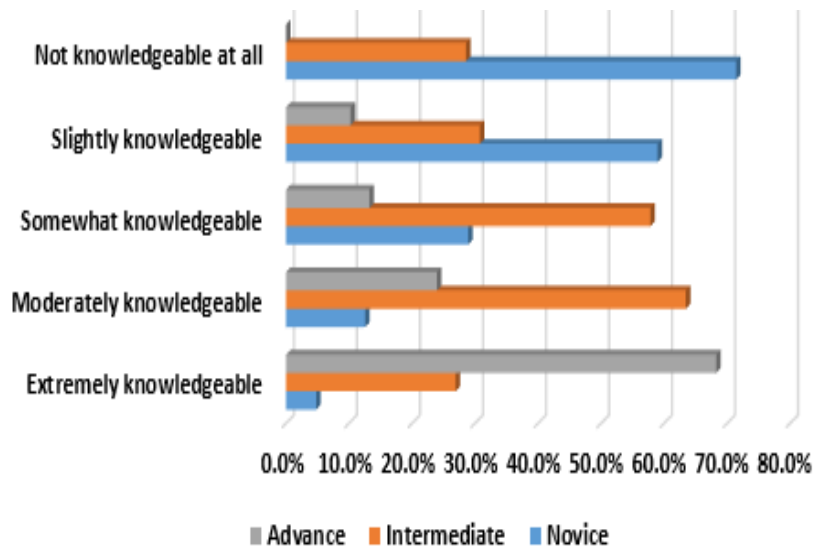


Figure 5.7: Answers Distribution between Novice, Intermediate and Advance to the Question (Understanding Privacy Settings)

Additionally, the following questions that are related to understanding privacy policy and privacy permissions yielded statistically significant correlations, as shown in Table 5.9. 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.

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

Table 5.9: The Correlation between Understanding the Privacy of Apps and the Three Categories

Further investigation looking at whether users’ demographic information, including age, gender, and education level, were conducted to check for 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 results indicate significant differences between males and females in the context of knowledge ($r = -0.98$, $p = 0.04$).

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 results show that the effect of education level is 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's (1992) guidelines, as discussed in the methodology chapter. Table 5.10 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	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 5.10: The Correlation between Demographic Information and the Level of Knowledge

Regarding providing user multi-level privacy controls (No access, Low access, and Full Access), 87% of participants strongly agree or somewhat agree to have this feature. The results indicate the need to provide users with more fine-grained privacy controls on mobile platforms. Furthermore, there is a statistically significant correlation between knowledge and display for multi-level privacy controls. When the level of knowledge increases, the need to display multi-level privacy controls increases as well ($R=-0.115$, $p=0.021$).

5.3.4 Possible Ways to Assign Privacy Profiles

This section examines how to predict many of a user's mobile app privacy preferences, which could significantly reduce user burden with minimum questions. Accordingly, different techniques were utilised to assign users to the privacy profiles that most closely capture their privacy preferences. First of all, users' demographic information was

examined to look at whether users' demographic characteristics, including questions related to gender, age, education and level of knowledge, are sufficient to determine which privacy profile a user should be assigned.

The results of the demographic information shown in Table 5.11 indicate that apps should not directly use gender, age, education or level of knowledge to assign users to privacy profiles that closely capture their preferences, because each demographic information attribute is distributed between each cluster, and there are no significant differences in these distributions.

Demographic		Cluster									
		1	2	3	4	5	6	7	8	9	10
Age	18-24	9%	6%	6%	18%	9%	3%	12%	18%	18%	3%
	24-34	10%	12%	8%	13%	16%	8%	6%	6%	13%	7%
	35-44	12%	9%	13%	9%	23%	6%	5%	6%	17%	1%
	44+	2%	0%	27%	7%	29%	12%	5%	2%	12%	2%
Education	Less bachelor	13%	9%	11%	20%	13%	7%	7%	7%	7%	9%
	Bachelor	9%	8%	9%	15%	15%	7%	6%	9%	15%	6%
	Postgraduate	9%	9%	14%	7%	23%	8%	6%	5%	17%	1%
Knowledge	Novice	13%	10%	8%	10%	20%	6%	7%	12%	10%	4%
	Intermediate	9%	10%	16%	13%	14%	8%	5%	6%	17%	4%
	Advance	10%	6%	8%	10%	26%	8%	7%	6%	15%	5%
Gender	Male	11%	7%	13%	14%	20%	6%	6%	5%	13%	4%
	Female	7%	13%	8%	5%	18%	10%	7%	11%	18%	3%

Table 5.11: Distribution of Demographic in each User Group

Even when the combination of demographic information has computed the distributions between clusters, there are no significant differences as well. Therefore, another technique was performed to predict the users' mobile app privacy preferences.

The machine learning approach was applied in order to predict the users' mobile app privacy preferences. R program supports different machine algorithms, such as Support Vector Machines (SVM), Random Forest (RF) and K-Nearest Neighbors (kNN). Before using the classifier, it was important to determine which questions are the most important to ask users in order to minimise the questions. Therefore, the following techniques were

used to minimise the 46 questions and help the models perform better and more efficiently, as shown in Figure 5.8.



Figure 5.8: Feature Selection Methods

- Machine learning assigns a weight to general questions about privacy-related information. Hence, it should be easy to minimise the number of questions, which in turn could actually help reduce user burden. Table 5.12 shows the features ranked according to the ranking algorithm with their weight.

N	Category	Weight
1	Exact Location	0.12
2	Health	0.10
3	Multimedia	0.10
4	Contact	0.10
5	Approximate Location	0.09
6	Shopping	0.08
7	Identity	0.08
8	Productivity	0.07
9	Fitness	0.07
10	Lifestyle	0.06
11	Navigation	0.05
12	Social media	0.04
13	Game	0.03

Table 5.12: The 13 Most Important Questions

Ten fold cross-validations were performed to estimate accuracy. This divides the data into 10 groups, train in nine and test in one, and is repeated for all combinations of train-test splits. The process was repeated three times for each algorithm with different splits of the data into 10 groups, in an effort to attain a more accurate estimate to predict the users' mobile app privacy preferences. SVM machine-learning algorithm was evaluated in order to select an appropriate number of questions to ask the user.

In order to study the effect of change from the number of questions on the accuracy, the accuracy of the SVM algorithm was evaluated based on several question sets (13 to 1 question respectively). Figure 5.9 shows that from 13 to 5 questions had accuracy equal or greater than 80%. Whilst the result between 4 to 1 questions shows a low precision ($\leq 70\%$) which indicates indicate a large number of False Positives. Despite 91% being the highest accuracy with 13 questions, 13 questions could increase the user's burden. Therefore, looking at a lower number of questions, the SVM classifiers show the five questions would be a reasonable result, which could be used in the initial interface to assign the user to the profile. This result reflects the exploration of trade-offs between accuracy and the number of questions; in other words, trade-offs between accuracy and user burden. The result also decreased by 90% (46 to 5 questions) of the user's effort.

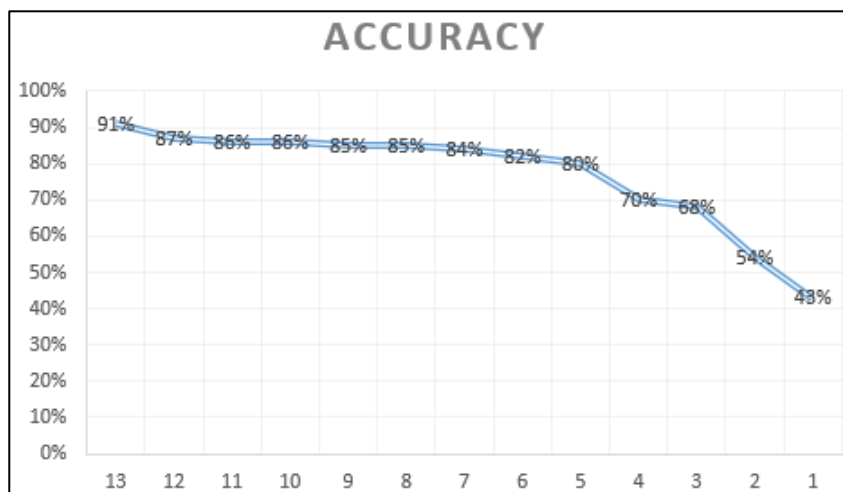


Figure 5.9: The Results of Accuracy from SVM Algorithm

To compare the outcomes of SVM model with other algorithms, three different machine-learning algorithms were evaluated in order to determine the best algorithm for this problem. The following list shows these algorithms:

- Linear Discriminant Analysis (LDA).
- Classification and Regression Trees (CART).
- K-Nearest Neighbors (kNN).

Figure 5.10 indicates that the CART algorithm shows the lowest accuracy compared to other algorithms. Whilst, the SVM algorithm had the highest accuracy with different question sets. These outcomes indicated that the SVM algorithm could be used in this model because it offers the highest accuracy with different question sets. This algorithm also has the advantage of being quite efficient computationally compare to other algorithms.

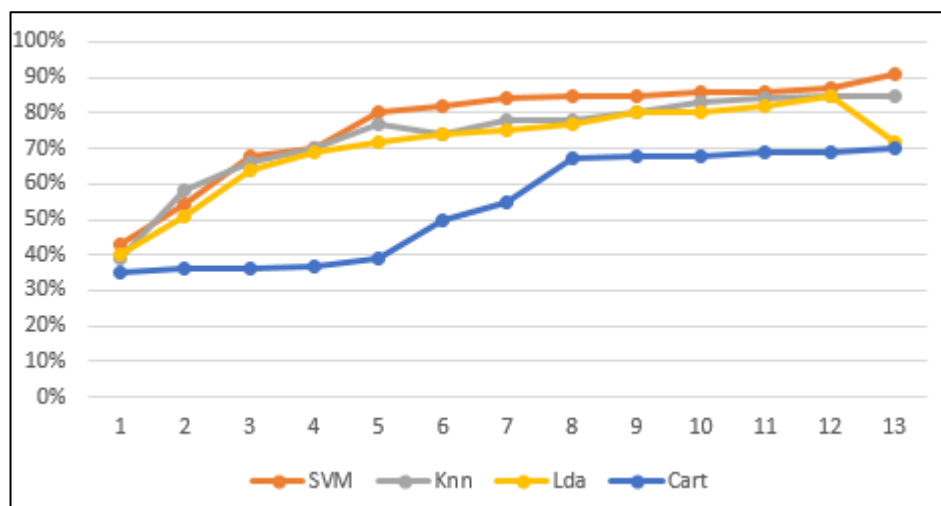


Figure 5.10: The Results of Accuracy from Different Algorithms

5.4 Conclusions

The initial requirements were set out in this chapter according to prior studies in order to enhance privacy technology on mobile apps, which in turn would help users to increase their awareness of privacy issues, and help them to manage a large volume of data, taking into account the level of users' knowledge. The survey was designed to include these initial requirements in order to explore whether these requirements would meet the current users' privacy preferences and achieve their desires. The results of the survey have been derived from a range of participants with a variety of backgrounds in terms of gender, age, education, and level of knowledge, and these factors had some impact on the users' privacy preferences.

The survey findings reveal interesting results related to the prioritisation of information. The outcomes from this study indicate that it is possible to divide the users into 10 unique subgroups that have similar preferences in terms 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 it is possible to prioritise information because each cluster has a different prioritisation of information.

Chapter Six

Requirements Analysis for Privacy usability

6. Requirements Analysis for Privacy usability

6.1 Introduction

It has been found from the analysis of the literature review in Chapter Three that there is an issue regarding how to design usable interfaces that maximise user satisfaction. Therefore, this chapter seeks to design usable initial interfaces based on HCI principles. The initial interfaces have been used to investigate end users' perceptions and attitudes towards usability in order to develop usable and adaptive interfaces that maximise user satisfaction. This analysis and investigation is in the form of a survey, and the third section presents the methodology of the survey questions. The fourth section provides an insight into vision-related ways of how to improve the initial interface, which in turn could overcome the usability issues without compromising the users' convenience.

However, it is important to consider the interfaces that are presented to end-users due to users playing an essential role in controlling their personal information, which in turn will increase users' awareness and help them to discriminate potentially harmful actions. Therefore, usability is arguably one of the essential requirements in the field of privacy today, which is described as *“the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”* (ISO 9241, 1998).

6.2 Usable Interface Design Literature

Numerous studies have been published in the usability literature that have focused on identifying usability problems and proposing guidelines and recommendations to address them (Nielsen, 1994; Johnston, et al., 2003). Nielsen (1994) has developed the 10 most general principles for interaction design by comparing several published sets of usability heuristics with a database of existing usability problems. Nielsen (1994) has also found

that these principles seem to be excellent for explaining the usability problems previously found. The 10 general principles are presented in Table 6.1.

Criteria of HCI	Description
1. Visibility of system status	The system should always keep users informed about what is going on through appropriate feedback within reasonable time.
2. Match between system and the real world	The system should speak the users' language with words, phrases and concepts familiar to the user, rather than system-oriented terms. Moreover, it should follow real-world conventions, making information appear in a natural and logical order.
3. User control and freedom	Users often choose system functions by mistake and will need a clearly marked " <i>emergency exit</i> " to leave the unwanted state without having to go through an extended dialogue. Support undo and redo functions.
4. Consistency and standards	Users should not have to wonder whether different words, situations, or actions mean the same thing. It should follow platform conventions.
5. Error prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. The system should either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
6. Recognition rather than recall	Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
7. Flexibility and efficiency of use	Accelerators — unseen by the novice user — may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. It allows users to tailor frequent actions.
8. Aesthetic and minimalist design	Dialogues should not contain information, which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
9. Help users recognize, diagnose, and recover from errors	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
10. Help and documentation	Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, such as a list of concrete steps to be carried out, and not be too large.

Source: (Nielsen, 1994)

Table 6.1: Nielsen 10 Usability Heuristics

Plaisant and Shneiderman (2005) have proposed eight usability guidelines, based on the researchers' experience of over more than two decades. Nielsen's 10 guidelines and

Plaisant and Shneiderman's Eight Golden Rules of interface design are the most widely used set of usability. Looking at the similarities and differences between Nielsen's rules and Plaisant and Shneiderman's rules, it is found that five of the presented rules are the same for both sets of principles:

- Flexibility and efficiency of use
- Consistency and standards
- Visibility of system status
- Error prevention and/or recovery
- Memory load reduction

However, Nielsen focuses more on help, aesthetic and minimalist design, whilst Plaisant and Shneiderman provide users with more control to meet the user's desire and make them the initiators of actions rather than the responders. However, the limitation of both these studies is that they are general usability guidelines and the researchers have not considered the security impact or created a balance between security and usability.

In term of security, Johnston et. al. (2003) introduced a new term in the usable security field called HCI-S. The term is defined as "the part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human-computer interaction applied in the area of computer security." Johnston et. al. (2003) developed a set of six HCI guidelines in order to form a balance between security and usability, as shown in Table 6.2

However, the HCI-S concept introduced by Johnston et. al. (2003) did not address how to enhance users' security awareness, in particular, privacy, yet enhancing users' privacy awareness would help users to make informed decisions and reduce their degree of exposure.

Criteria of HCI	Description
1. Convey features	The interface needs to convey the available security features to the user.
2. Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
3. Learnability	The interface needs to be as non-threatening and easy to learn as possible.
4. Aesthetic and minimalist design	Only relevant security information should be displayed.
5. Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6. Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?

Source: Johnston et al. (2003)

Table 6.2: HCI-S Criteria

Ibrahim et al. (2010) also developed a set of HCI-S guidelines based on a literature review in order to enhance security tool interfaces. These guidelines focus on how to provide users with a usable alert to help them to make informed decisions and give a timely response with a consistent presentation of information. The guidelines are listed below:

- **Interface Design Matches User’s Mental Model:** The interfaces should be designed according to user’s thinking to match the user’s mental model.
- **Aesthetic and Minimalist Design:** The interfaces should only show the important and relevant information.
- **Visibility of the Alert Detector Name:** It is useful to display the security tool name when the alert appears.
- **Establish Standard Colours to Attract Users’ Attention:** It would be useful to design attractive colours to draw the user’s attention and help them to interpret the content quickly.

- Use Icons as Visual Indicators: It is important to utilise the icons and pictures during the design to make the interfaces easily interpretable and understood by the user.
- Explicit Words to Classify the Security Risk Level: The level of the risk should be displayed clearly in the system
- Consistent Meaningful Vocabulary: The sentences on the interfaces should be look consistent and function in a similar way.
- Consistent Controls and Placement: The controls should appear in an appropriate location in the interface in order to be found by users easily.
- Learnability and Flexibility: The security alert should provide users with more flexibility and enhance the user's ability to learn the required security basics.
- Take Advantage of Previous Security Decision: Displaying information about the triggered alert and simple statistics, which summarises this information, would be useful for the user to make an informed decision.
- Online Security Policy Configuration: The designers should develop default settings for the security policy.
- Confirm / Recover the Impact of User Decision: The security tool should give users the opportunity to recover the error and modify the response.
- Awareness of System Status all the Time: It would be useful to provide users with a simple report regarding the state of the system.
- Help Provision and Remote Technical Support: The user should be able to obtain more help with extra information at the time of the alert with an appropriate response.
- Offer Responses that Match User Expectation: The security tool should meet users' expectations and requirements.

- Trust and Satisfaction : The security tool should be easy to understand and prevent performance failure to increase users' acceptance and satisfaction.

Additionally, several researchers (Whitten and Tygar, 1999; Yee, 2002; Zhou, Blustein and Zincir-Heywood, 2004), have proposed a set of design guidelines that consider security. These studies aim to address the security features of the GUI in order to design a more user-friendly interface that is easier to understand. These guidelines could be utilised in this research to overcome the usability issues and improve the interface. For instance, Whitten and Tygar (1999) focus on the issue of novice and non-technical users who have little initial understanding of security. They emphasise that security interfaces may confuse novice users due to a lack of consistency in their design and not clarifying the message, thus hindering rather than helping users. Therefore, they suggest that to make the interface usable, the designer needs to consider the novice user during the design. This draws attention to one of the research requirements, which is about adapting the interface to the user's knowledge, which in turn should be considered during the design of the interface.

To enhance privacy technology in the user interfaces, LaTouche (2013) proposed eight guidelines which focus on user interfaces for Web-based privacy-enhancing technologies in order to help designers to address the lack of user control features. The guidelines are listed as follows:

- Visibility of user-controlled e-privacy features.
- Conformance of privacy policy statements and user preferences.
- Navigation and graphical design.
- User control and freedom over personal data.
- Help users recognize and track the use of personal information.
- Follow the appropriate use of standard privacy practices.

- Allow easy monitoring and notification of accesses to personal data.
- Help and feedback.

However, the design would be more difficult when it comes to mobile interfaces and their apps due to the screen size and resolution restricting mobile phones in displaying content. Moreover, the usability guidelines for mobile interfaces are limited, which creates more challenges during the design of the proposed system. To overcome this limitation, Baharuddin et. al. (2013) proposed usability guidelines that could help researchers to design usable mobile applications, which include four dimensions: mobile user, mobile task, mobile technology and mobile environment. These factors would guide designers to decide which usability dimensions should be considered during the design. The user profile is an essential factor that helps to identify the characteristics of potential users and design the information required by them, which in turn determines which information is more suitable to be presented for users.

6.3 Initial Interfaces

As seen in Chapter Three, most of the solutions introduced to protect the users' privacy focus on technical issues, whilst only a few studies have focused on the usability perspective. Usability problems in these systems can lead to privacy vulnerabilities because users may miss an attack altogether or misdiagnose it. Moreover, when interfaces are presented with too little or misleading information, or are too cumbersome, or overwhelm the users with too much information, then security could be failing.

To overcome the usability limitations in the prior studies, this research seeks to design the initial system according to HCI principles. However, privacy notification is one of the primary requirement of privacy and data protection in order to educate and enhance the user's awareness of data protection issues (Schaub, Balebako and Cranor, 2017).

Therefore, notification interfaces have been designed which include a clear indication of the current privacy status and warnings for events of interest or concern. Informing the user about what is going on through appropriate feedback is suggested by Nielsen (1994) and Johnston, et al., (2003) which has guided the visibility of system status.

The first consideration for the notification design is the type of information being communicated (Kim, 2015). In general, the notification contains contextual information related to on-going data transfers such as location or contact. The second consideration is how to design user interfaces for the notification. One of the options would be to show a small icon in the device's status bar, similar to those used by Android to indicate GPS usage, as shown in Figure 6.1.



Figure 6.1: The Small Icon in the Status Bar

The problem with this method is it may easily go unnoticed (Wagner et al., 2016). Therefore, Wagner et al. (2016) suggest a small notification and a large pop-up window. Therefore, these two types of notification have been presented to the participants in order to investigate their expectations and preferences.

Another important aspect is the integration of user controls and consent into notifications to make them actionable (Schaub, Balebako and Cranor, 2017). Agarwal and Hall (2012) proposed two options - “*Protect*” or “*Allow*” - on the notification in order to control the data which can be utilised.

Accordingly, Figure 6.2 was designed in order to inform the user about on-going privacy risks and provides the user with mitigation options to minimise the risk incurred. 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 attempting to understand the notification. This is particularly useful for novice users to understand what a privacy notification means (Nurse et al., 2011).

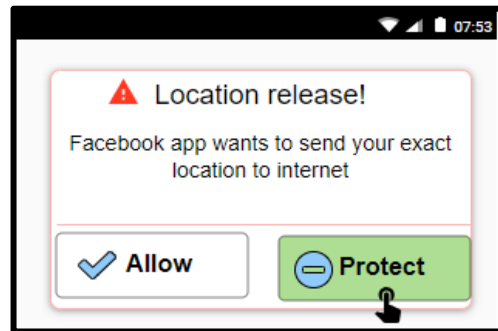


Figure 6.2: Short Interface Notification

A large pop-up window is another option to inform the user about on-going privacy risks, as shown in Figure 6.3.

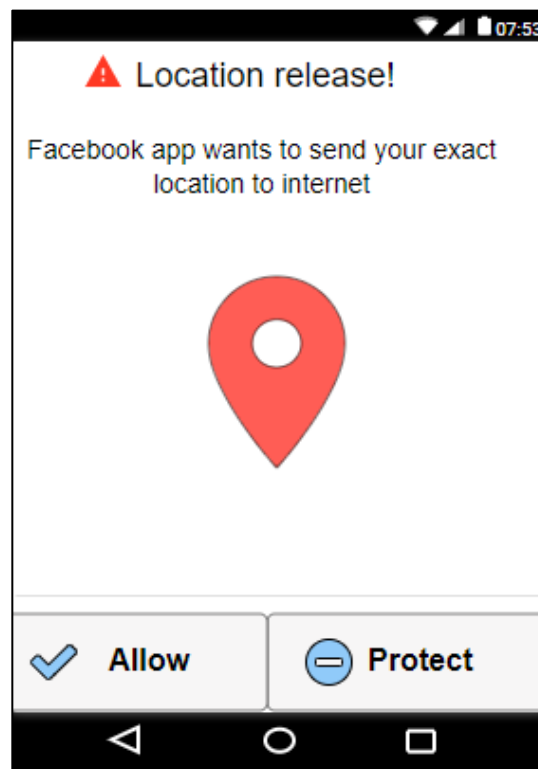


Figure 6.3: Full Interface Notification

As previously mentioned, it is important to provide the user with mitigation options to minimise the incurred risk. Hence, privacy protection settings have been designed, as

shown in Figure 6.4, which shows how the protection settings look for the proposed system. The interface will be displayed when the user clicks the protect button from the notification interface. To support different multi-level privacy controls for users in the proposed system, Figure 6.4 shows three levels: full access, low access and no access.

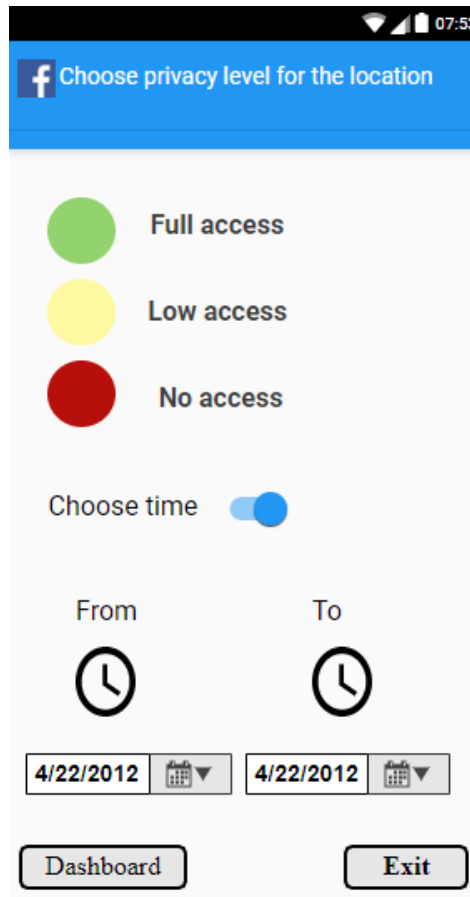


Figure 6.4: Three Levels Privacy Protections Settings

Moreover, Sheikh et al. (2008), Christin et al. (2011), and Kim et al. (2017) suggested more than three levels of privacy control in order to achieve more flexible privacy controls. Accordingly, another interface has been designed with four levels for the protection settings as shown in Figure 6.5.

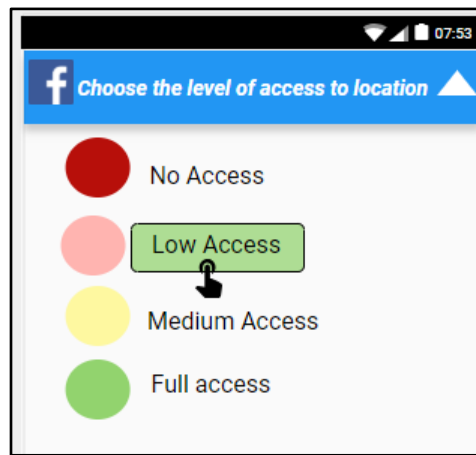


Figure 6.5: Four Levels Privacy Protections Settings

In general, the criteria of several researchers (Chiasson et al. (2006), Chiasson et al. (2007), Herzog and Shahmehri (2007) Johnston et al. (2003), Nielsen (2005) Whitten and Tygar (1999) and Yee (2002)) has guided the interfaces design and how it should match users' mental model. Mental models are connected to the way that users look at the world around them based on belief, not facts, and simulating these models into the system. For instance, when users see a bin on the desktop, they expect it to be for delete files. Therefore, this design seeks to match the user's mental model because mental models play a significant role in HCI and interaction design. Paul et al. (2012) proposed the C4PS privacy interface which utilises a colour coding scheme for making privacy settings more usable. Moreover, Muñoz-Arteaga et al. (2008) utilised the colours of traffic lights to determine security level. For instance, the system displays a traffic light image with the green colour to indicate the system is protected. Hence, a traffic-light pattern approach has been adopted for designing the privacy protection setting interfaces to make privacy protections more usable and assist the user to understand the function of these options quickly.

To design different options for the protection levels interfaces, a review of the design and API documentation of Android and iOS was conducted, and it was found that there is another option to display multi-level controls, which is about sliders. Sliders simulate

well from the real world to touchscreens. The mobile operating system provides two types of sliders: continuous slider and a discrete slider. The discrete slider allows users to make slider adjustments until meeting their preference, as shown in Figure 6.6.

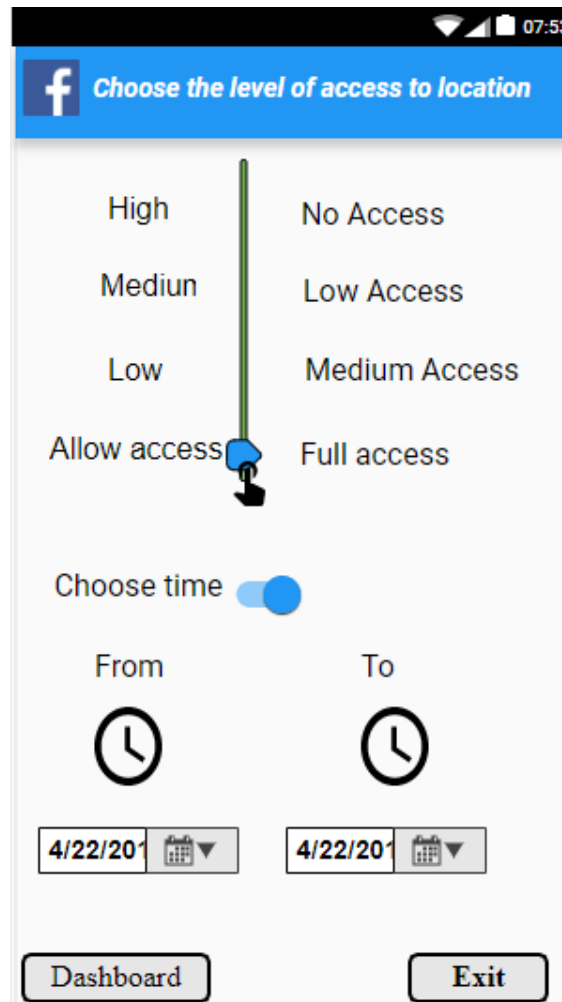


Figure 6.6: Four Levels of Privacy Protections Settings Sliders

The protection settings interface contains a risk impact interface in order to help the novice user to make an informed decision about protecting his or her privacy. Bal et al. (2015) proposed the Styx privacy tool, which displays the risk impact interface and seeks to enhance the comprehensibility of privacy risks while at the same time increasing trust and reducing concern. Johnston et al. (2003) and Nielsen (2005) emphasise providing built-in help to enable the user to respond correctly. Accordingly, a graphical risk impact

interface has been designed, as shown in Figure 6.7. One of the essential criteria for Johnston et al. (2003) is learnability, which can be achieved by a risk impact interface.

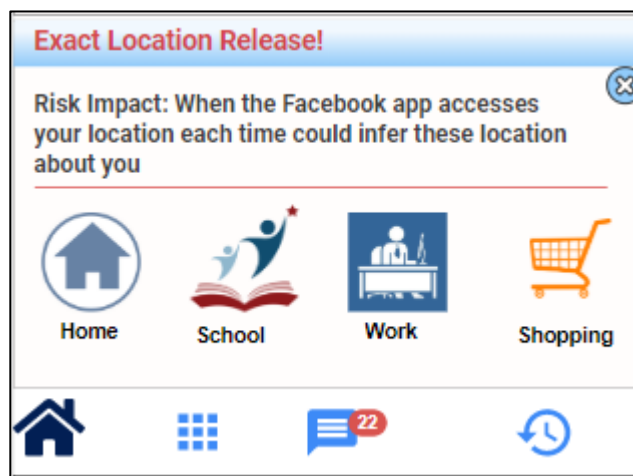


Figure 6.7: Graphic User Interface

Katsabas et al (2005) found that novices will find it hard to comprehend the security threats if technical vocabulary and advanced terms are used profusely. Therefore, the use of technical terms in the risk impact interface was avoided because it could confuse the user attempting to understand the information.

From a psychology perspective, it is possible to distinguish between two types of memory retrieval: recognition versus recall (Budiu, 2014). Therefore, Nielsen (2005) proposed one of the primary usability guidelines, which is recognition rather than recall. Recognition refers to the human ability to “*recognise*” information as being familiar, whereas recall indicates the retrieval of related details from memory (Budiu, 2014). Hence, visual icons have been used in the risk impact interface in order to attract users’ attention to make the content of the interface easily interpreted and understood and to promote recognition.

However, some users may prefer the Text-based User Interface (TUI), and a Graphic User Interface (GUI) does not always mean ease of use. Chen and Zhang (2007) compared between TUI and GUI interfaces in term of performance, and they found that a TUI

interface was better for advanced users than a GUI interface; although it is difficult to use the TUI interface for novice users. This indicates the importance of considering both interfaces, GUI and TUI, in the design and investigating the users' preferences. Accordingly, a TUI risk impact interface has been designed, as shown in Figure 6.8.

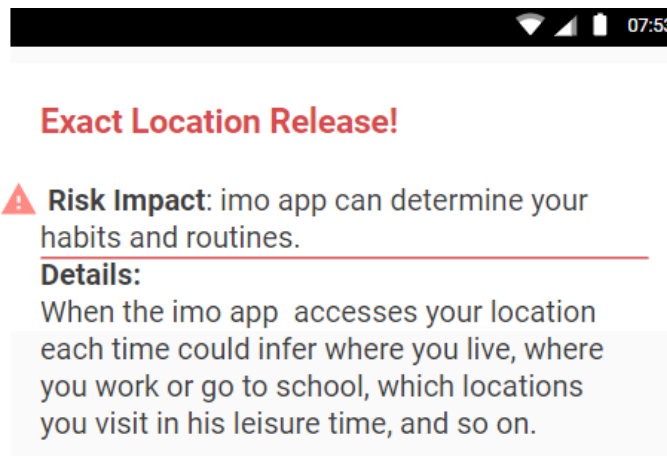


Figure 6.8: Text-based interface

Regarding the transparency requirement that was discussed in Chapter Five, historical view interfaces have been designed, as shown in Figure 6.9. Ibrahim et al. (2014) suggest taking advantage of previous security decisions because it will be useful for the users in the decision-making process and provide them with the opportunity to evaluate the effect of their decision. However, historical view interfaces utilised the colours of the traffic light to determine the protection level, similar to the colours on the protection level interface mentioned above. This design has led to achieving one of the important guidelines proposed by Plaisant and Shneiderman (2005) which is about striving for consistency.

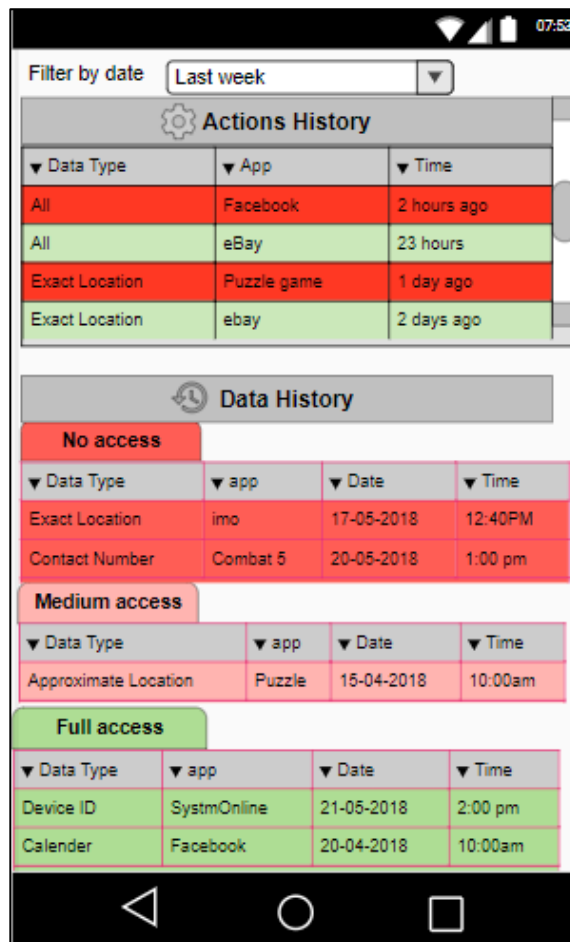


Figure 6.9: Historical View Interfaces with Colours

Hall and Hanna (2004) highlight that black text on a white background was found to be more readable than other combinations of colours. Lynch (2008) also suggests a white background with black text for optimal contrast results. Deubel (2003) recommends other colours such as grey and pastels for backgrounds. In these studies, providing a sufficient contrast is an essential factor to improve readability and would make the interface easy to interpret for colour-blind users. Accordingly, another historical view interface was designed to consider another colour such as black text and white background, as shown in Figure 6.10, which could improve the readability. One of the advantages of this interface is that it uses a few colours because the fewer colours used in the design, the fewer instances there will be for the confusion.

Filter by date				
Last week				
Actions History				
Data Type	App	Actions	Time	
All	Facebook	No access	2 hours ago	
All	eBay	Full access	23 hours	
Exact Location	Puzzle game	No access	1 day ago	
Email	Ebay	Full access	2 days ago	
Data History				
Data Type	app	Date	Time	Actions
Exact Location	imo	17-05-2018	12:40PM	No access
Approximate Location	Puzzle	17-05-2018	10:00am	Medium access
Contact Number	Combat 5	20-05-2018	1:00 pm	No access
Device ID	SystemOnline	21-05-2018	2:00 pm	Full access
Calendar	Facebook	22-05-2018	10:00am	Full access
Approximate Location	Budget app	23-05-2018	5:00 pm	No access

Figure 6.10: Historical View Interface White and Black Colours

Accordingly, the initial interfaces were designed based on the following guidelines from different sources:

- Interface design matches user's mental model (Chiasson et al. (2006), Chiasson et al. (2007), Herzog and Shahmehri (2007) Johnston et al. (2003), Nielsen (2005), Whitten and Tygar (1999) and Yee (2002)).
- Visibility of the System Status (Nielsen, 2005).
- Recognition Rather than Recall guidelines (Nielsen, 2005).
- Use Icons as Visual Indicators (Ibrahim et al. 2014).
- Strive for consistency within (Plaisant and Shneiderman 2005).
- Learnability (Johnston et al., 2003).
- Take advantage of previous security decisions (Ibrahim et al., 2014).
- Help and documentation (Nielsen, 2005).

6.4 Survey Methodology

To explore end-users' perceptions and attitudes towards the initial design, the survey was designed to include these interfaces. The survey includes four primary questions related to usability which were derived from the initial requirements and organised as follows:

1. Notification interfaces questions

Regarding the notification questions, two interfaces were displayed to the participants because the prior study suggested a small notification and a large pop-up window, as discussed in the section on initial interface design. This would help to investigate users' expectations and preferences towards these two interfaces. Accordingly, this question has been presented to the participants:

"Two interfaces will be displayed to you. The first interface is full-screen notification whilst the second interface is short screen notification. Please, read each statement carefully and rate each point based on the above interface"

- The icons used in the notification.

This question would help to find out how the icon on the notification interface can visually please users and enhance the aesthetic appeal of the design.

- The understanding of the interface.

Prior studies demonstrated that users struggle to understand privacy notification. Therefore, this question aims to measure how easy to understand the information provided in notification.

- The ease of use

Another important aspect is the integration of user controls and consents into notifications to make them actionable. The notification contains two options - “Protect” or “Allow” - in order to control the data. Accordingly, this question aims to assess how options - “Protect” or “Allow” - on the notification interfaces are easy to use.

2. Help and support interfaces questions

The survey also includes help and support interfaces in order to help the user to make an informed decision about protecting his or her privacy. The help and support interfaces questions aim to investigate users’ understanding of interfaces. Additionally, the participants were asked to choose between the Graphic User Interface (GUI) and Text-based for the risk impact interface to find out to what extent participants prefer any interface. Moreover, the following scenario was presented to the participants:

“From this interface, you can understand the risk impact when the app sends your personal information each time. For example, when the Facebook app wants to send your location each time, it could infer the location of your work, home, and school.”

After presenting the scenario to the participants, the following statements have been shown to them:

- The icons used in the risk impact interfaces.

As demonstrated in the initial interfaces section, visual icons have been utilised in the risk impact interface in order to attract users’ attention to make the content of the interface easily interpreted and understood. To make sure this aim is achieved, therefore, this question was presented to the participants.

- The understanding of risk impact.

The question aims to make sure the participants could easily to understand the risk impact. Hence, the responses for this question would help to make sure the interface convey the available privacy features to the user effectively.

- The text font used in the risk impact interface.

This question aims to identify any problems with the font in terms of readability and size.

3. Privacy control interfaces questions.

Two Privacy control interfaces have been included in the survey aim to explore how easy the interface to use and to understand. The interfaces were presented to the participants as animated pictures to help them to understand how to perform the tasks. Then, the following statements were presented to the participants:

“From the interface, you can select a certain level of privacy to help you control your personal information easily. Please, read each statement carefully and rate each point based on the above interface”

- The understanding of privacy control interfaces.

The privacy control should be easy to understand in order to increase users' acceptance and satisfaction. Therefore, this question would assess how easy it is to understand the information provided in these interfaces.

- The icons used in the interface.

The traffic-light icons have been utilised for designing the privacy protection setting interfaces to make privacy protections more usable and assist the user to understand the function of these options quickly. Therefore, there is a question regarding how well the

icons are designed. This question would help to find out how the icons can visually please users and enhance the aesthetic appeal of the design.

- The ease of selecting a certain level of privacy.

The questionnaire displays some interfaces such as privacy control interfaces and has an animated image to guide the user on how to use the interfaces. Therefore, after displaying the interfaces, the question was presented to participants concerning how easy the interfaces are to use. This question aimed to assess how efficient the interfaces make completing tasks. The user interface needs to be intuitive, which means even if the user has never used the interface before, they should be able to predict how it works and navigate it with ease.

4. Historical view interfaces questions.

The survey also includes historical view interfaces to investigate user' understanding regarding these interfaces and how well the colours are designed. As discussed in the section on initial interface design, prior studies suggested two types of interfaces historical colour interface and another historical view interface that consider another colour such as black text and white background. Therefore, the survey includes these two interfaces to investigate to what extent participants prefer any interface. Moreover, the interfaces included the following statement:

“The interface presents data history to help you to know who has accessed data, when and at which degree of granularity. Please, read each statement carefully and rate each point based on the above interface.”

- The colour used in the history interface.

Due to using colour on the history interfaces, therefore there were questions regarding colour. The right choice of colour will make it easier for users to immediately determine what they can do on each interface and will satisfy aesthetic needs and provide visual solutions. Ultimately, this question would help to create a clear and harmonious style that meets users' needs.

- The understanding of the history interface

This question aims to measure how easy it is to understand the information provided in the interfaces. Moreover, this question would help to identify what aspect of the interfaces are difficult to understand, especially by novice users, which would help to improve the interface design in the context of how easy they are to understand.

- **The text font and size**

This question aims to identify any problems with the font in terms of readability and size. The right choice of text could measurably improve user productivity and increase user satisfaction.

In general, these questions are aimed at helping to measure users' satisfaction with the interfaces and to find out the possible weaknesses in these interfaces. Moreover, there is a comment field in order to receive useful feedback, which in turn would improve the design interfaces to meet users' satisfaction.

The next step is regarding the types of scale that can be suitably used in the survey. Nielsen (2012) describes usability as a quality attribute that assesses how easy user interfaces are to use. Therefore, the rating scales used five points of the level of quality, which include poor, fair, good, very good and excellent, which in turn measure users' satisfaction with the interfaces.

Accordingly, the initial interfaces were designed based on HCI principles to overcome usability issues without compromising the users' satisfaction. Therefore, the initial interfaces were included in the survey in order to explore the users' thoughts regarding the design of those interfaces. Moreover, the current approach in the survey involved creating two types of interfaces for various notifications and screens in order to cater for the full range of users' needs and expectations, which in turn provide participants with a level of flexibility by providing users with different options of the interface (Christin et al., 2012). This approach might be perceived as a sensible trade-off between the flexibility and to reduce participants burden to be less confusing to increase the response rate.

6.5 Analysis of the Results

This section aims to explore 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 notifications, whilst 43.7% of participants prefer the short screen. In terms of the icons that are used in the notification interfaces, 72% of participants stated that the icons are excellent or very good in the full-screen notification, and an almost similar result of 70% was found for the short screen.

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

Another requirement to help the user to make an informed decision for protecting his or her privacy is the risk impact interface. In general, 90% of participants indicated they

understood the risk impact from the interface by combining the scale from excellent to good. In the context of the novice participants, the vast majority of them (86.7%) indicated they understood the risk impact from the interface. When the participants were asked to choose between Graphic User Interface (GUI) and Text-based, 80% chose the GUI for the risk impact interface. The comparative study of user preferences with regards help and notification interfaces revealed differing results. While the vast majority of participants prefer one particular help interface called “GUP”, two notification interfaces appeared to be equally preferred by the participants.

Specific questions were asked to investigate users’ usability perspectives regarding the history interface, and 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. 92% of participants stated that the interface is excellent or very good or good for understanding the history view. Regarding the colour of the interface, 86% of the participants indicated the colour is excellent or very good or good.

In relation to participants’ attitudes towards icons and colours on all interfaces, as shown in Figure 6.11, the responses were above 85%, which represents good and over. 86% is the lowest percentage, which is about the history interface. This would indicate that the history interface requires further improvement in term of colour design. One of the advanced users stated in the comments that the red colour affected his understanding of the interface. Most of the comments regarding the history interface are about the red colour being too flashy and so it requires more improvement. In addition, there is a statistically significant correlation between knowledge and understanding the history

interface. When the level of knowledge increased, the understanding of the interface increased as well ($R=-0.144$, $p=0.004$).

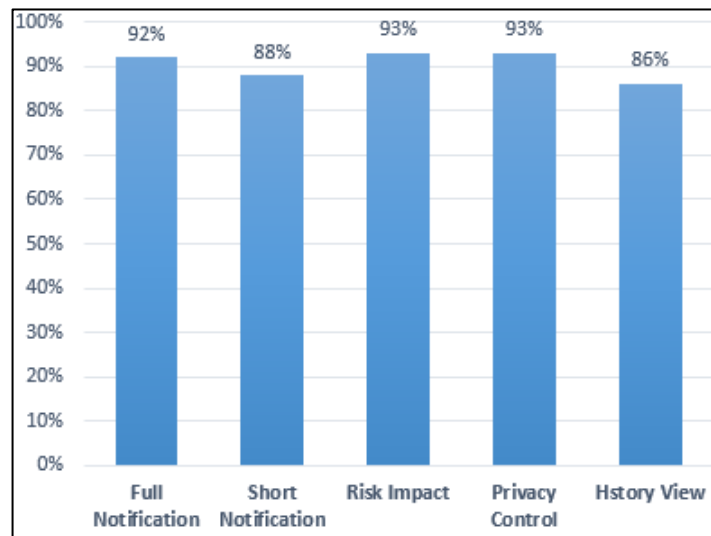


Figure 6.11: The Participants' View on Icons and Colours

As a result, it is difficult for novice users to understand the history interface when there is a large volume of data. Therefore, it is important to consider both expert and novice users when interfaces are being designed. For instance, one of the comments regarding history interface is: *“users or moderators looking for simplicity when using applications”*.

In general, the results presented in Figure 6.12 indicate that over 90% of the participants stated that the interfaces are easy to understand. This is perhaps due to the icons and colours, which could make the interface simple and easy to understand with less technical terminology. When it comes to the text font used for the interfaces, 92% of the survey respondents rated it excellent or very good or good. This result shows that the font is good in terms of readability, which in turn should increase user satisfaction.

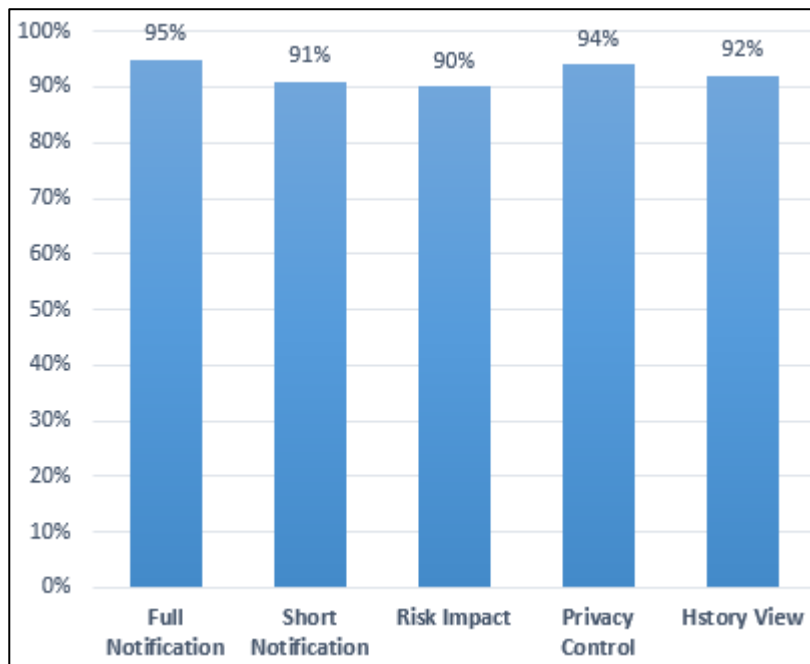


Figure 6.12: The Participants' View on Understanding the Interfaces

When examining the participants' preferences according to their knowledge, and finding out the differences between novice, intermediate and advanced users in terms of which screen they prefer, the results indicate that there is no significant difference between novice, intermediate and advanced users. This result shows that there is no correlation between users' preferences regarding the interfaces and knowledge factors.

Advanced participants

It is important to consider advanced participants' opinions towards the attributes of the interfaces to investigate whether they have any ideas regarding the design, which in turn could help to improve the interfaces.

Regarding how easy the interfaces are to understand, a few participants chose poorly for this attribute. However, for some interfaces such as the history interface, protection settings and full-screen notification, no expert participants chose the poor level to understand the interfaces. Rather, the vast majority of their choices are between excellent or good, as shown in Figure 6.13.

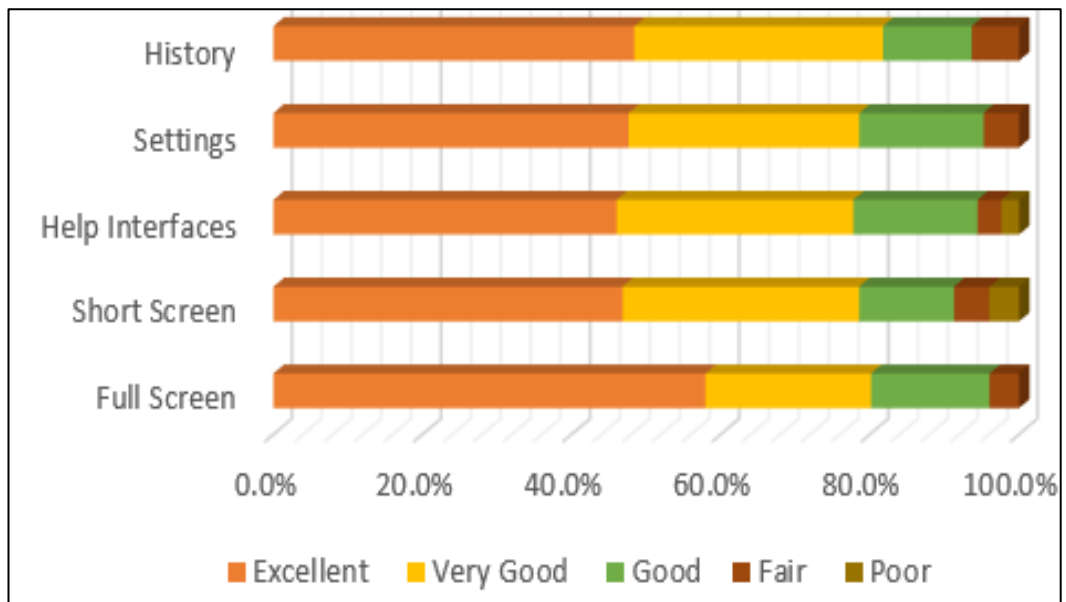


Figure 6.13: Experts' Opinions about Understanding the Interfaces

Similarly, regarding how easy the interface to use, the vast majority of expert participants chose excellent or good. However, the protection settings interface revealed the lowest percentage for those who chose excellent or good compared to the other interfaces, as shown in Figure 6.14. When looking at the differences between novice users and experts regarding how easy it is to use the protections settings, it is found there is no difference, as 74% of novice users stated they are excellent or good, while 73% from the experts did so. The experts' choices for the lowest level of the scale (poor or fair) were very little, which indicates that interfaces in general are easy to use.

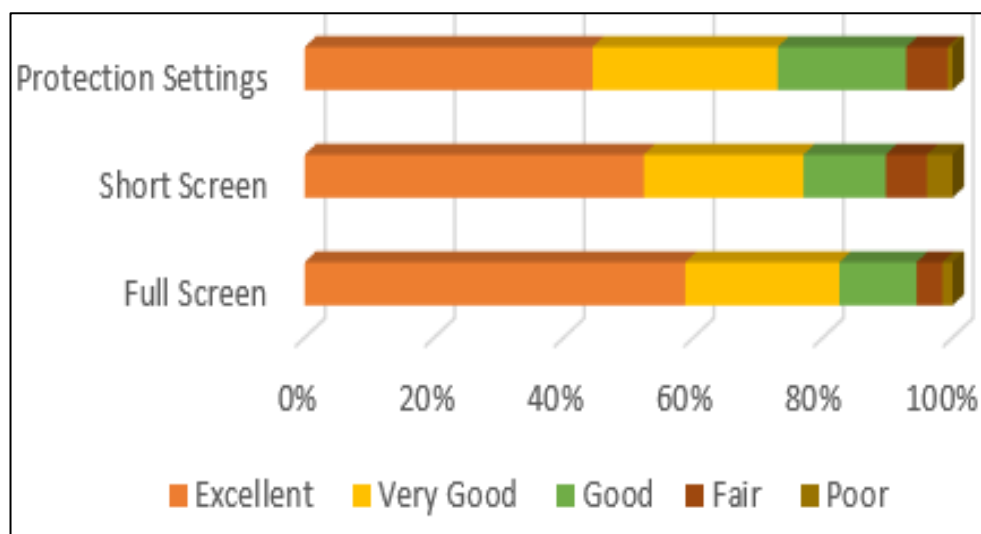


Figure 6.14: Experts' Opinions about How Easy to Use Interfaces

In general, the experts' opinions were positive regarding each attribute of the interfaces, where the overall percentage is over 90% when combining between excellent or very good or good, as shown in Figure 6.15. The most interesting point is that there is an agreement across most of the results for these attributes: easy to use, easy to understand, font and the quality of icons. It can be deduced from these outcomes that there are no remarkable differences between experts' opinions and all participants' opinions. This is perhaps due to considering the knowledge level during the design phase of these interfaces, which has been discussed in Chapter Five.

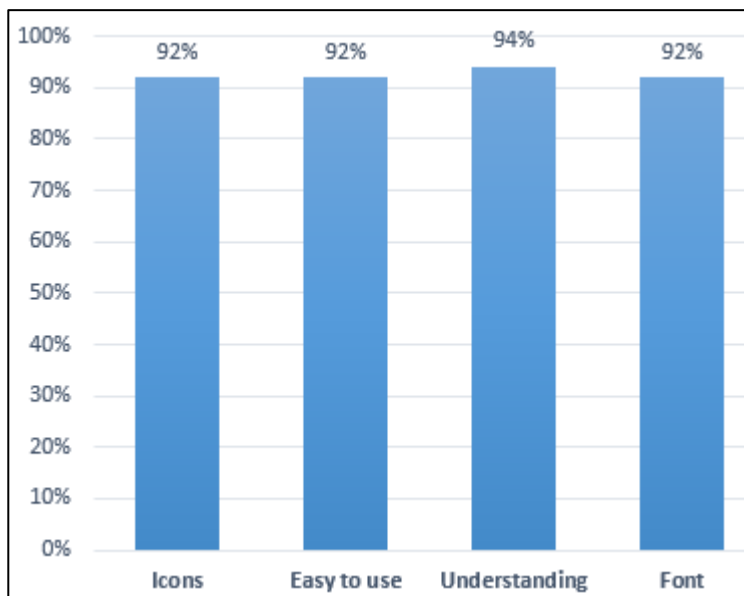


Figure 6.15: Experts' Opinions about All Interfaces

6.6 Conclusion

The initial interfaces were designed based on HCI principles to overcome usability issues. The initial interfaces were included in the survey in order to explore the users' thoughts regarding the design and the functionality of those interfaces, which in turn could help to overcome the usability limitations without compromising the users' convenience. In general, the majority of the participants' perceptions and attitudes towards the initial interfaces were positive, which reveals that the initial design contains usable interfaces

which should maximise user satisfaction. Furthermore, the survey revealed an interesting result whereby users are different not only in the context of prioritisation of their information, as seen in Chapter Five, but also in the context of design, multilevel privacy controls, and level of knowledge. This, in turn, emphasises the need for a holistic tailored solution for users, considering all these dimensions.

When it comes to comparing participants' preferences between two interfaces, the vast majority of participants tend towards a single interface, except for the notification interface, where it appears to be equally preferred by the participants. This highlights the importance of considering which interfaces will be the default in the proposed system.

However, some interfaces require some improvements regarding the colour, in particular, the history interface, because colours play a significant role in readability and user satisfaction. Moreover, the history interface requires further consideration of the knowledge of users during the design of that interface because the results have revealed that when the level of the user's knowledge increases, the understanding of the interface increases as well. On the other hand, the evaluation of the interfaces shows that novice users prefer visual aids on the interface to understand the system, in particular, the risk impact interface. Therefore, visual aids would also help novice users to understand the system.

Chapter Seven

Design and Development of a Privacy-Enhancing Framework for Mobile Devices

7. Design and Development of a Privacy-Enhancing Framework for Mobile Devices

7.1 Introduction

Chapter Five revealed considerable results regarding how to prioritise privacy-related issues, which represents an essential role in building an initial user profile. Chapter six also shows significant outcomes regarding initial interfaces and how to improve them. Accordingly, this chapter builds upon the knowledge in Chapter Five and Six to develop a novel privacy framework that considers the current privacy preferences, followed by detailed architectural specifications designed in a modular and robust manner. The chapter continues to present the interfaces in order to practically prove that the concept of the proposed architecture would work in practice.

Additionally, this chapter seeks to achieve a comprehensive understanding of the effectiveness of the proposed approach. Despite the users' feedback and results, presented in Chapter Five and Six of this thesis, for preliminary system requirements and interfaces, there is a need for an additional qualitative evaluation involving the core stakeholders of the system and experts to investigate users' acceptance and satisfaction in-depth, which is difficult to achieve through purely quantitative approaches.

7.2 Essential Requirements

Based on the analysis contained in the literature review (Chapter 3), the outcomes from the survey (Chapter 5 and Chapter 6), and in order to offer an effective novel mobile privacy mechanism, the proposed system requirements have to be specified prior to the architecture design. Therefore, the following essential system requirements have been established:

- **Prioritisation of privacy-related information based on users' privacy preferences**

As seen in the survey results, privacy preferences are diverse and cannot adequately be captured by one-size-fits-all default settings because the level of privacy required differs from user to user. Therefore, in order to cater to different user preferences and expectations, initially, the ten point privacy profiling that was generated in Chapter Five could be utilised to determine which of these profiles provides the best match for a given user. Each profile effectively represents a cluster of like-minded users and captures their privacy-related information preferences. According to the machine learning results, it is possible to match individual users with profiles by asking those users five questions. In turn, the ten profiles could help predict, with a high level of accuracy, many of the users' privacy-related information preferences.

- **Personalised response system to inform and control the flow of privacy-related information**

The outcomes of the data collection strongly indicate that users desire to be notified about information being shared by apps. A push notification feature is effective for enhancing users' awareness, especially for users with little experience. Therefore, a personalised response system to inform and control the flow of privacy-related information has been implemented. The notifications would be personalised according to the user's prioritisation. For instance, some users are extremely concerned about their personal information on social media platforms, therefore, the notification that requires action from the user will display the information related to social media.

- **Historical auditing - to provide an overview of privacy-related information usage across apps and prior user decisions**

In order to meet the user's requirements and their preferences, this system offers a historical auditing feature. Transparency mechanisms can increase trust in the system and

reduce privacy concerns. The proposed system allows users to access the date of the data that was sent out of the mobile and which app has shared this data and at what degree of granularity. In order to help a novice user to understand the historical interface, they can view the history of data in a high-level format without going deeper into the details. This also allows an advanced user to know who has had access to which data, at which degree of granularity and when, without confusing the novice.

- **Multi-level privacy control – to provide users with a non-binary choice over privacy and thus more flexibility**

The result of the survey indicates current 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 on multiple levels, taking factors such as the level of user's knowledge into account. 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 to the information but medium access or low access requires modification. Numerous studies have defined methods for modifying 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 the year, month and day, while low level access is to just the year and month. Another example is that location information can also be classified into four options: full access, no access, medium access and low access: the system shares the city location 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, therefore the proposed system allows novice users to access a minimum set of features in order to protect their privacy. For example, when the app wants to send the user's location out of the mobile, the system notifies the user and provides the user with two options: allow or protected.

In contrast, the system provides intermediate and advanced users with more options to protect their privacy, and these options have different colours in order to assist the user to understand the function of these options and he or she can respond quickly.

- **Adaptable privacy-related guidance depending upon prior knowledge and experience**

The results of the survey draw attention to the fact that the users are different in term of level of knowledge. This, in turn, emphasises the need to divide the privacy options into different levels. The goal of this requirement is to make the system understandable and learnable for the novice user, while at the same time not hindering the advanced user from working productively. A novice is a user who is trying to complete the task in the system but has little or no experience of privacy systems in terms of how to manage and control a large volume of data. Therefore, they need additional help and support such as documentation and tutorial guides. A novice might also need a clearer description of the alert. As the user gains 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.

- **Privacy impacts**

Another requirement to help the novice user to make an informed decision for protecting his or her privacy is the risk impact feature, which motivates users to respond and helps

them understand potential impacts on their privacy. Prior studies, as discussed in Chapter Two and Chapter Three, have highlighted that users may have difficulties in understanding the risk signals. Therefore, the permission screens that have been provided by mobile operating systems are not effective privacy indicators. Additionally, the outcomes of the data collection indicate that a risk impact feature can help the novice user to understand potential impacts on their privacy.

- **Continuously monitor**

Due to users being assigned to the closest profile, as shown in Chapter Five, the application and data type in each profile needs to be monitored in order to notify the user about information being shared by apps. Therefore, the system should have the ability to monitor the privacy-related information flow between the device and applications in real-time. The advantage of prioritising the user's information is to make the monitor focus on the most important information for the user, which will reduce the overheads in the system, as the system, in this case, will not monitor every single piece of data. Moreover, the proposed system should continuously review the privacy settings on each app in order to be compared.

- **Usable interfaces**

Users play an essential role in the proposed system in term of how to manage privacy settings; therefore, it important to design interfaces based on HCI and usability principles. The analysis of the users' thought towards the interfaces has revealed that some users stated that some interfaces' colour needs more improvement. Hence, interfaces should be clear, easy to use and easy to understand in order to meet the users' requirements and satisfaction. Moreover, the interfaces should have a minimalist design in terms of the information displayed on the screen and system interactions. Irrelevant or rarely needed information should not be displayed on the interfaces.

- **A Flexible design**

The outcomes of the survey in Chapter Six showed an interesting result, as the users differed not only in the context of prioritisation of their information, as seen in Chapter Five, but also in the context of design. For instance, notification preferences are diverse because some of the participants prefer full-screen notifications whilst others prefer the short screen. Thus, the system should have a level of flexibility by providing users with different options to change interface themes, colours and size. These options could help different people, such as colourblind people and older people. Moreover, the design of the interface does not rely on colour alone to convey a message because some people such as colourblind people might make it difficult to understand the history interfaces. Therefore, visual icons and colours have been used in the interface in order to make the content of the interface easily understood and to promote recognition. As discussed in Chapter 6, the interfaces should contain a few colours because the fewer colours used in the interfaces, the fewer instances there will be for the confusion. Additionally, the proposed system used textures and colours to show contrast because it might be difficult for colour blind users to interpret contents and charts.

- **Use Icons as Visual Indicators**

As seen in the results of the survey, users are most often affected by the use of pictures and icons on the interfaces. In particular, when visual icons were used on the risk impact interface in order to attract users' attention to make the contents of the interface easily interpreted and promote recognition. Therefore, it is very important to utilise this feature and ensure it can be easily interpreted and understood by the user.

The aforementioned requirements can be fulfilled by utilising the enhanced privacy technology architecture, which is described in the following section.

7.3 Enhancing Privacy Technology Architecture

Stemming from the above-mentioned essential requirements, enhancing privacy technology architecture is proposed. A novel architecture for user privacy encompasses the core functionality to allow for the personalisation of privacy awareness and adaptive interfaces. Adaptive interfaces can assist in providing personalisation and supporting flexibility. Figure 7.1 illustrates an architectural enhancing privacy technology, beginning with an initial interface that displays a series of questions related to users' information, aiming to assign users to the privacy profiles that most closely capture their privacy preferences. These questions were identified in chapter 5 where the SVM classifiers showed the highest accuracy of 80% with five questions, which could be used in the initial interface to assign the user to the profile. Then, the system will update the personal privacy preferences of the user based on their interactions. Updating personal privacy preferences would enable the system to create individual privacy profiles in order to adapt an individual's specific preferences without overly burdening them. The system will use user's profile to monitor the privacy-related information flow between the device and applications in real-time. The outcomes of the survey also indicate that the users are different in term of level of knowledge. This, in turn, emphasises the need to divide the privacy options into different levels. Therefore, the system also provides a user-adaptive interface. In this case, the system could meet personal privacy preferences and personal visualisation.

Accordingly, the framework has been designed based on different phases, which begin with initial requirements in chapter 5 and 6. Then the initial requirements were improved according to the outcomes of the survey, which demonstrated in section 7.2. Hence, the framework consists of a number of key components aimed at enhancing privacy technology on mobile apps. An outline of the components is provided below:

User-related information: When the user logs on to the proposed system for the first time, five primary questions related to the user’s information would be displayed. These questions have been examined by the machine-learning algorithm in Chapter Five to determine the minimum questions related to users’ information. SVM classifiers showed the highest accuracy of 80% from five questions, but it is possible to achieve 91% with 13 questions, as shown in discussed in Chapter Five. The 13 questions are listed below:

- Exact Location
- Health
- Multimedia
- Contact
- Approximate Location
- Shopping
- Identity
- Productivity
- Fitness
- Lifestyle
- Navigation
- Social media
- Game

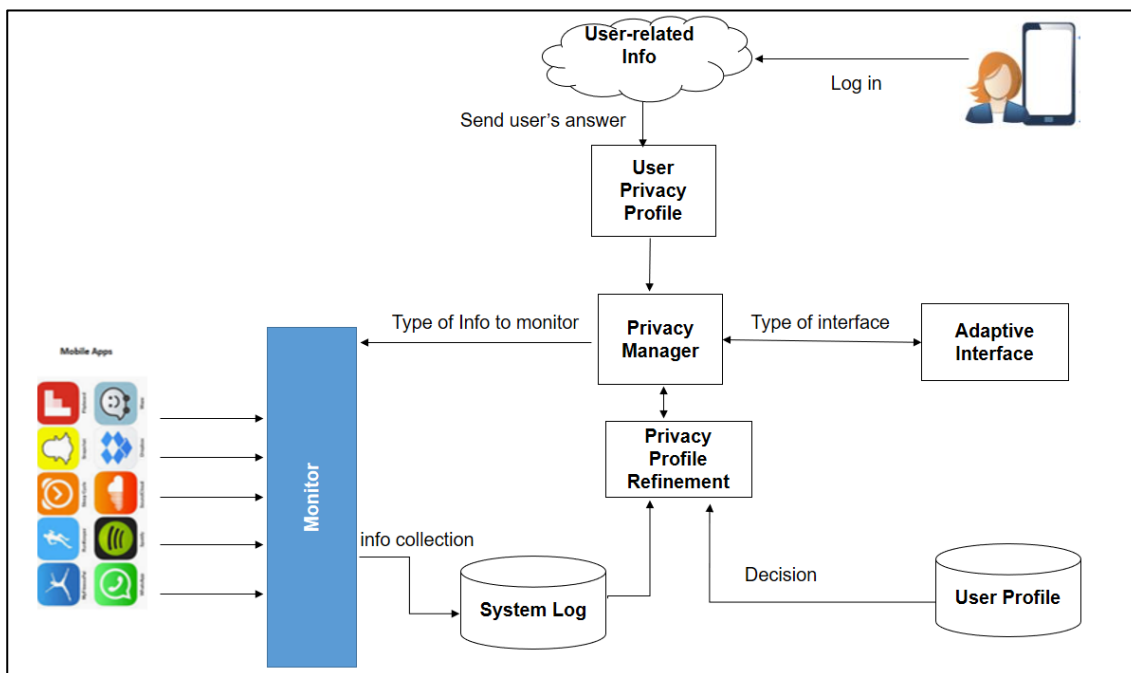


Figure 7.1: Mobile Privacy Awareness framework

When the user answers these questions, the Privacy Manager passes the information to the user profile storage in order to select the user’s preferences. Other information on

knowledge level will be pass to an Adaptive Interface component in order to display the appropriate control level and interfaces.

Adaptive Interface: The basic premise behind the Adaptive Interface is that users are different and therefore have different needs from the system in the context of adapting what information to present, how to present the information, and how to interact with this information. Due to users being different in term of their knowledge and skills, the Adaptive Interface will provide novice users with a simple interface in order to make the system understandable for them, whilst at the same time not hindering the advanced user from working productively. This simplicity also includes the adaptation of users to appropriate controls over their privacy-related information. Additionally, this component aims to notify the user about potential privacy risks based on that user's preferences. In this case, the presenting of information and notifications will dynamically change when the system updates the user's preferences. Hence, the Adaptive Interface is further broken down into three smaller components, as illustrated in Figure 7.2, which include how to present information, controls and responses. Ultimately, this is the user-facing component of the system and therefore its design is of key importance.

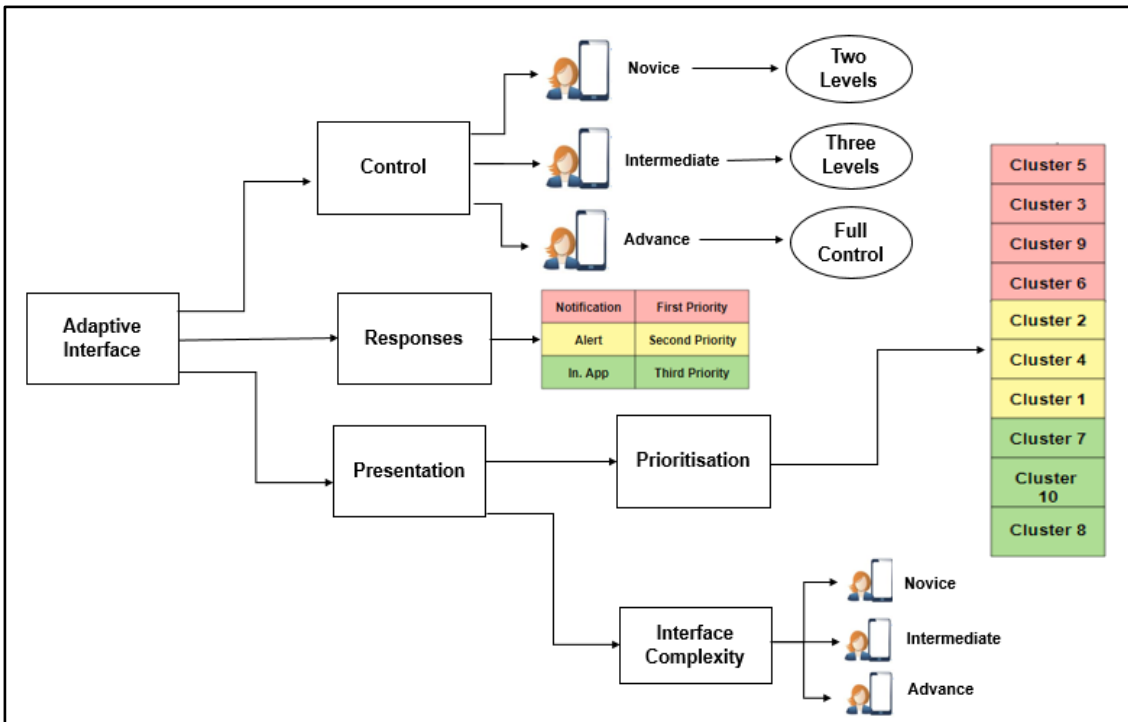


Figure 7.2: Adaptive Interface Components

Control Level

The proposed system provides users with multi-levels of control, as discussed in the requirements. The full access and no access options are easy to apply because there are no modifications of the information, but medium access or low access requires modification. Users can select a certain level from among the four levels. Table 7.1 shows different examples of the four levels. When a user desires to select a certain type of data unmodified to a mobile application, the user can select the full access. Otherwise, if the user does not want to provide any data, the user can select the no access level.

Data Type	Full access	Medium Access	Low Access	Ref
Exact Location	GPS coordinates	City Block	City	Sheikh et al. (2008)
Approximate Location	Cell Tower or Wi-Fi	City Block	City	Sheikh et al. (2008)
Calendar	Year, month, day, hour, minute	Year, month, day,	Year, month	Knijnenburg et al. (2013)
Audio	Original voice	Modified background audio	Modified background audio and foreground	Moncrieff et al. (2008)
Image	Original image	Number of people	Face blued	Christin et al. (2011)

Table 7.1: Private Information Modified at Various Levels

For instance, Robert wants to use Twitter, and this app wants to share location information. Robert desires to share his location information at medium level, rather than sharing his exact location with Twitter. In this case, the original location will be modified to the city block location. For instance, when GPS coordinates are 50.487 and 150.354, the original GPS coordinates will be then changed to be 50.490, 150.360. In this case, the medium access is approximately 539.87 meters away from the exact location, as shown in Figure 7.3.

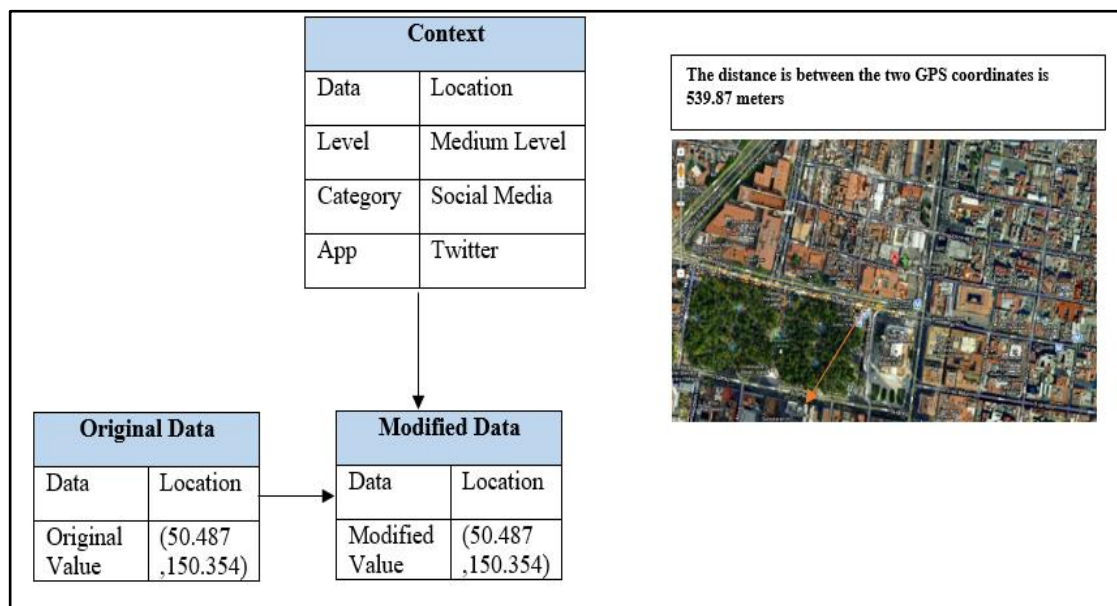


Figure 7.3: Location Information Representation at Medium level

Monitor: The primary goal of the monitoring component is to collect privacy-related information from a user such as location, contact, Email and multimedia. Given the range of monitoring modalities that can be captured by a device, and utilised by a user, their related agents are put into effect to capture their information characteristics simultaneously and transparently. However, some tools could be utilised to monitor data, such as PrivacyGuard and ReCon, as mentioned in Chapter Three. ReCon requires root permissions and knowledge about VPN technology, whilst PrivacyGuard does not require root permissions and runs in its entirety on the local device. It also does not require a

remote VPN server or any knowledge about VPN technology from its users. Therefore, PrivacyGuard could be utilised as the implementation of this component.

All data that is collected would be stored in the storage which consists of (but is not limited to) the requested application name, types of data, date, time and category. The architecture runs the data on the local device in order to increase the level of privacy and security. However, during the latter process, the data is used by the Privacy Manager to verify the user's profile.

User Privacy Profile: in order to assign the user to the privacy profile that most closely captures their privacy preferences, the initial interface will display a series of questions related to users' information when the user logs on to the system for the first time. The questions have been examined by the machine learning algorithm in Chapter Five to determine the minimum questions needed to predict the user's mobile app privacy preferences. These questions include questions about, Exact Location, Health, Multimedia, Contact, and Approximate Location. Based on the user's answers, the User Privacy Profile will determine the closest privacy profile for the user from the profile storage.

User Profile storage: this component stores the ten unique profiles that were derived from hierarchical clustering, as explained in Chapter Five. Ten unique privacy profiles provide a reasonable default prioritisation of information for an initial interface. Figure 7.4 shows how each cluster prioritises the information according to the users' privacy preferences for each profile. The red colour represents a higher level of concern, while green indicates a lower level of concern.

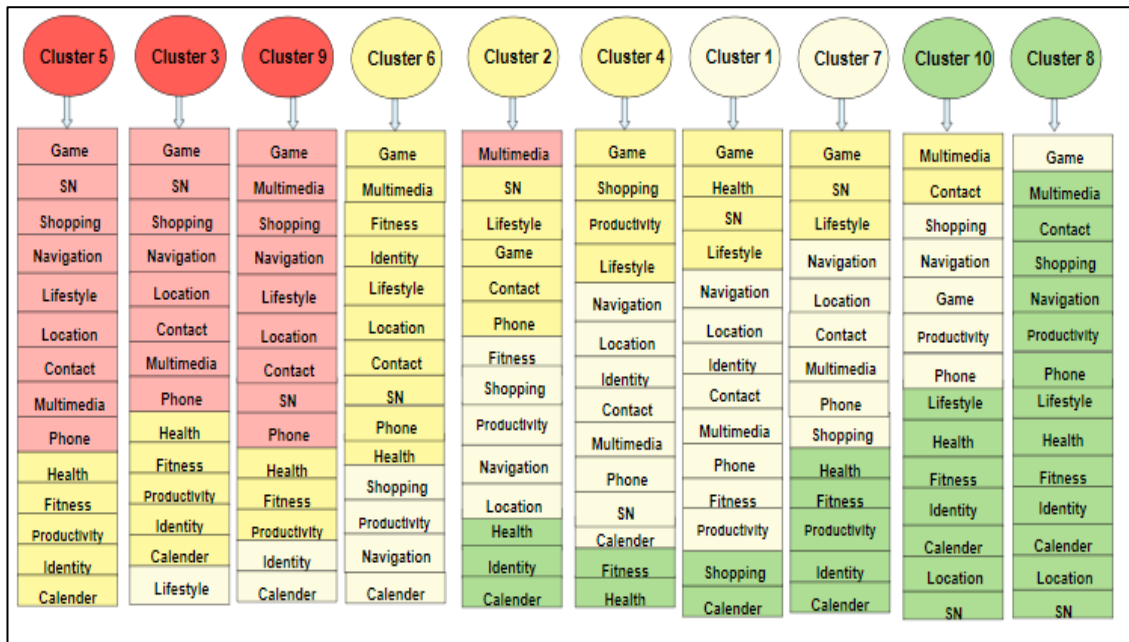


Figure 7.4: Ten-Privacy Profiles

The priority of notifications would be changed according to the user’s profile. For instance, when the user’s profile is Cluster 2, the user would be notified about multimedia because this category is the first priority for cluster 2, which is represented by the red colour; whilst, multimedia in Cluster 8 is not a high priority to them. Therefore, when the system assigns the user to the right profile, the Privacy Manager passes the user’s preferences to the Monitor in order to monitor this information, and passes this information to the Adaptive Interface component to notify the user about potential privacy risks based on the user’s Profile.

Privacy Profile Refinement: the vital function of this component, which should receive more care, is to refine the user profiles that were derived from the system logs. It is responsible for updating personal privacy preferences for individual users based on users’ interactions that stored on the System Log. The Privacy Profile Refinement then takes the System Log as the input and tries to match the information related to the user with a current user profile to observe if there is any change in order to update the user’s profile.

System Log: the main task of System Log is to perform the collection of a wider dataset of all information which is related to capturing the interaction with the users' personal information.

Privacy Manager: this is the core component of the proposed system. The main function of privacy manager is to control the processing between these elements: User Privacy Profile, Adaptive Interface and Monitor. When the system chooses a privacy profile that is the closest to the user's preferences from Profile storage, which includes the ten clusters, the Privacy Manager passes the user's preferences to the Monitor in order to monitor this information.

In order to update the personal privacy preferences for individual users, the Privacy Manager will keep passing the privacy preferences from the Privacy Profile Refinement, which were extracted from the System Log component, to the monitor.

When the user selects the level of his or her knowledge from the first interface, the Privacy Manager will pass the level of the user's knowledge to Adaptive Interface component in order to provide the user with appropriate information and settings.

7.4 Privacy Enhancing Technologies Interfaces

The privacy enhancing technologies interfaces have been designed to help in visualising and better understanding how the architecture would work in practice. The Moqups web app was utilised to design the mobile interfaces and provides a streamlined web app that helps to design, test and validate the system with quick wireframes and detailed mock-ups. The advantage of the Moqups is also to prove the concept by showing interactive interfaces. Building the interfaces would help to show the end-user and the experts what the software will look like and allow them to evaluate the system.

The users' interface is composed of five primary interfaces, which are historical view, dashboard, app privacy settings, response control and notifications. These interfaces were designed according to the users' perceptions and suggestions from the questionnaire and based on HCI principles in order to develop usable and adaptive interfaces that maximise user satisfaction. The system also provides users with different features, such as historical auditing, to provide an overview of privacy-related information usage across apps and prior user decisions, multi-level privacy controls, consequences of the disclosure of sensitive information and personalised responses. The information from the registration interface will help to prioritise the user's information. This prioritisation will play an essential role in many interfaces, such as the order of apps in the app setting interfaces, history interface and notification.

Regarding the user's knowledge, novice, intermediate and advanced users have some different interfaces in the context of interface complexity, app privacy controls and historical view. Table 7.2 demonstrates the characteristics of each interface for different users.

Characteristics	Type of user		
	Novice	Intermediate	Advanced
Privacy Controls	Two levels	Three levels	Full control
Interface complexity	Simple	Medium level descriptions	More details and information
Historical view	Visual aids on the interface (Word and icons cloud)	Statistical charts	Statistical charts

Table 7.2: Characteristics of Interface

Therefore, the main challenge is how to design a system that can accommodate novice, intermediate and advance users. In order to overcome the usability issues without compromising the users' convenience, some guidelines have been utilised to design the interfaces. When a user installs the proposed system for the first time, the registration screen displays six questions related to the user's information, as shown in Figure 7.5. The first five questions centre on how concerned users are about their privacy-related information being shared by categories of apps. These questions will assign users to the privacy profiles that most closely capture their privacy preferences; whilst the last question will determine the level of user's knowledge. The system will allow users to change their level of knowledge from novice to intermediate or advanced if they desire from the settings of the system, which in turn gives the system more flexibility and helps users to change their preferences regarding their level of knowledge. Additionally, users can change their preferences related to the priority of information. Hence, the system will update the personal privacy preferences of the user based on their interactions. The advantage of updating personal privacy preferences is that it would enable the system to create individual privacy profiles.

Registration

Please answer the following questions in order to assign you to the right profile

How concerned you are about such privacy-related information being shared by different categories of apps

	Extremely	Moderately	Somewhat	Slightly	not at all
Exact Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multimedia	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contact	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

How would you rate your knowledge about the privacy of individual apps?

Novice Intermediate Advanced

Figure 7.5: User Registration Interface

When the user selects novice user, the system will display a novice dashboard which is simple and easy to understand, as stated in the characteristics of novice user interfaces. Figure 7.6 shows the dashboard for the novice user, which consists of two sections: active controls section and word cloud. The first section allows the novice user to select from two options - allow or deny - to share the information with apps. Each data type of information is represented by icons to help the novice user to scan the page more easily.

The second section in the novice dashboard displays the amount of user data that is shared by the apps in the word clouds technique. The word clouds are a visualisation technique which uses word size to indicate numerical values. The larger the word shown in the

cloud, the more user data shared by the app. Gruen et al. (2007) and Bateman et al. (2008) found that font size is the most effective aesthetic to convey information when they investigated various measures of impression-forming. It is clear from Figure 7.6 that Facebook is the app that uses the most user's data. However, when the novice user clicks the Facebook app in the word cloud section, the system will display another interface, which includes more details about the user's data on Facebook. In this case, the interface does not overwhelm the users with too much details information.

Figure 7.6 also displays the menu in the bottom bar. Icons are used on the menu elements to make navigation simple and easy-to-use. Each icon in the bottom bar guides the user directly to a specific destination in order to minimise the number of clicks.



Figure 7.6: Novice Dashboard

When it comes to the intermediate and advanced user, the dashboard would present more details and information. Moreover, the system provides them with multi-level controls to

regulate access to privacy-related information. This allows them to limit the disclosure of their private information on multiple levels taking factors around the level of the user's knowledge into account, as stated in the requirements.

Figure 7.7 shows the advanced user interface, which displays three sections. The first section represents the alert that is required to interact by the user. The interface does not only display the alert to the user, but it is also associated with multiple active controls to reduce the amount of user effort to accomplish a task and achieve the system's efficiency. The second section, which is about a recent activity to allow the user to change the recent setting controls in case he changes his mind about the settings. This is because Chapter Three highlights that users may change their privacy preferences from time to time. This could help reduce the user burden and the frustration of the user.

Charts are an important feature for the user to visualise a useful summary of the data and enable users to advance their understanding. Therefore, advanced and intermediate users can see some charts on the dashboard, as seen in Figure 7.7. A few charts will be presented here to reduce the number of contents in order to not overburden the user with too much data. Users can click on any chart to go beyond simple charts to express more advanced insights about quantitative information which in turn reduce the amount of data in this dashboard.

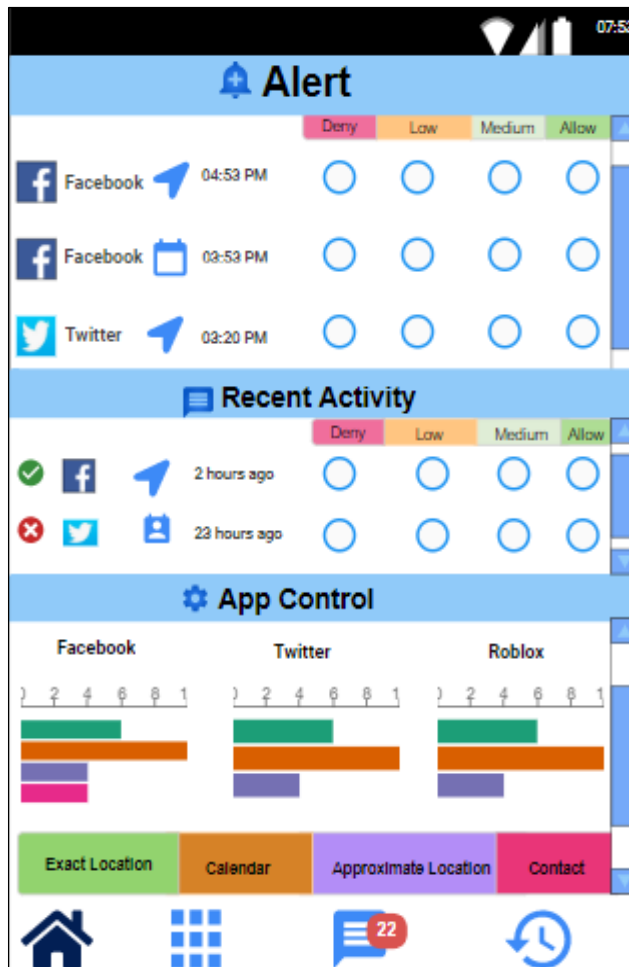


Figure 7.7: Advanced Dashboard

According to the outcomes of the survey, users desire to be notified at the moment data is being sent. Therefore, the dashboard displays notification icons in the menu bar. The notification icon badge shows the number of unread alerts and it is omnipresent on the app icon. It is a simple way of informing the user, at a glance, if they have an unread notification.

Regarding the responses feature, which represents one of the essential requirements, the system provides three levels of responses based on the user's priority related to privacy information, as shown in Figure 7.8. As a result, all data does not require action to be taken by the user, so they do not feel overwhelmed by the warning messages. However, the high-priority notification is a foreground notification and offers two options - to deny or protect - which in turn easily focuses the user's attention on the most important pieces

of data to them. The system also displays an alert for the second priority categories for the user; whilst the third priority would also be displayed on the system. To elaborate more about how the system distinguishes between the three levels, Figure 7.8 shows one example from Cluster 9. From multimedia to the health category, it represents the first level or the highest importance for users in Cluster 9, whilst fitness and productivity represent the second level. Accordingly, the system prioritises these responses according to the user's profile, which would reduce overwhelming the user with superfluous warnings and achieve a connection between the user's profile and the notifications.

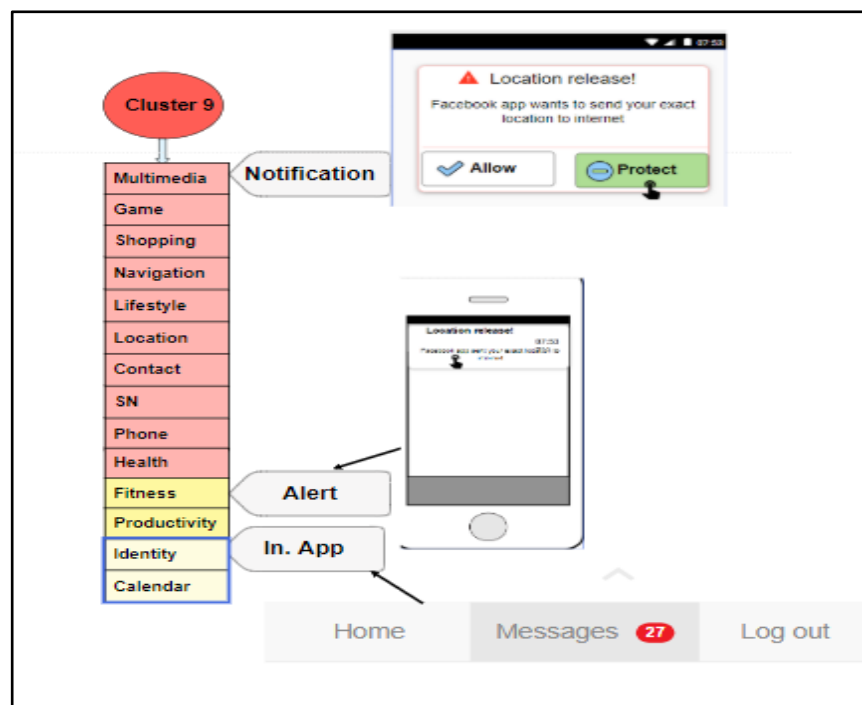


Figure 7.8: Sending Notification According to the Importance of Data in Cluster 9

Due to the survey findings revealing that participants strongly desire to have the ability to change privacy notification settings for different apps, the user can change the response settings in the proposed system. When the user clicks the notification icon on the dashboard, the system displays the alert settings interface. When the user clicks on the setting icons for the calendar in the Facebook app, he would be provided with more control to change the order of priority for the notification and alert, as shown in Figure 7.9.

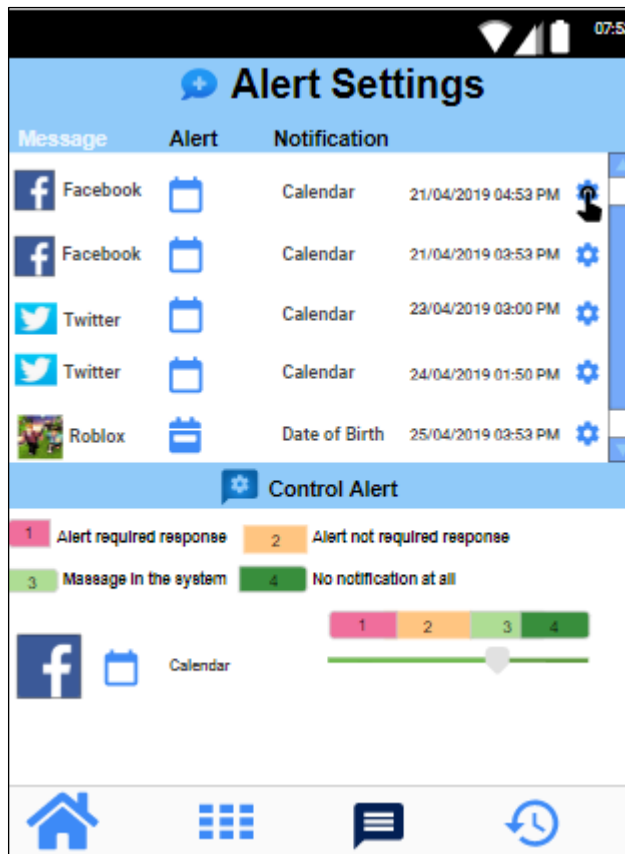


Figure 7.9: Control the Priority of the Alert

One of the requirements to help users to make an informed decision for protecting their privacy is the risk impact. Therefore, when the app is going to share the data, the system displays the notification screen to deny or protect the user's information. As seen in the results of the survey, users are most often affected by the use of pictures and icons on the risk impact interface. Therefore, it is very important to utilise this feature and ensure it can be easily interpreted and understood by the user. When the user clicks on the protect button, they will be able to select the level of protection. The vast majority of participants prefer the colours of the traffic light on protections settings in the initial interface to determine the protection level. Therefore, this interface was utilised in the final design. To help the user to make an informed decision and to learn about the actual privacy risks, the system provides a risk impact button. Figure 7.10 shows the risk impact of the location at the bottom of the interface by clicking on the risk impact button. This could help to

educate users about the importance of protecting their privacy and about the risks of disclosing their information. Hence, they could make an informed decision about controlling their data.



Figure 7.10: Risk Impact Interface

The dashboard contains app icons to change the order of importance of the data in each app. When the user clicks on the icon, the app settings would be displayed, as shown in Figure 7.11. The order of each app on the app settings interface is based on the cluster profile order. For instance, Figure 7.11 shows the game apps as the first category, whilst social media is the second category, because this interface displays the profile for Cluster 5. However, each user has their own privacy preferences. Therefore, the system learns the user preferences based on his or her past click history data and personalises based on the user's preferences. Hence, the order of each app on the app settings interface would be updated according to individual privacy preferences. This approach would make users

concentrate on the important apps for them, in contrast to current mobile privacy where the apps do not organise according to the users' preferences.

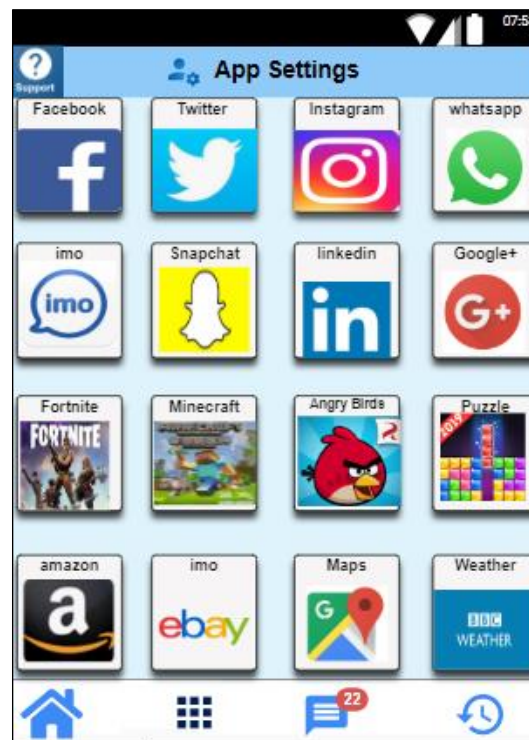


Figure 7.11: App Settings Interface

When the novice user clicks on any app, the privacy settings are displayed for this app. For instance, when the novice user clicks on the Facebook app, he is enabled to control the privacy settings for the Facebook app in binary form, as seen in Figure 7.12. Whilst the system allows advanced users to manage their privacy controls by selectively providing their private information to applications.

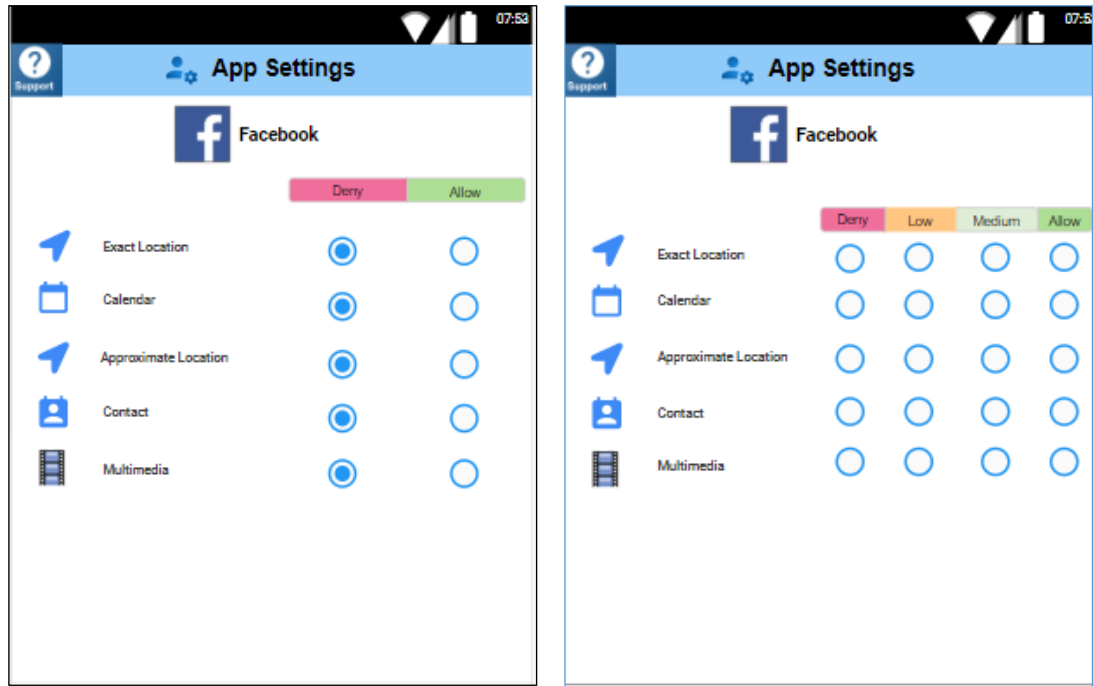


Figure 7.12: Novice and Advance App Settings

In order to meet the user's requirements and their preferences, this system offers a historical auditing feature, which aims to show the user how his or her personal information is being used, thus enhancing user awareness even further. Moreover, it would increase trust in the system and reduce privacy concerns. The outcomes of the survey in Chapter 6 also indicate that the history interface requires further improvement in term of colour design. Therefore, the chart for the privacy-related information usage was utilised on the history interface instead of flashy colour that confused participants in the initial interfaces.

The system allows users to access the date of the data that was sent out of the mobile and which app shared this data and at which degree of granularity. The dashboard displays a historical icon which users can use to acquire statistics about the accessed data for each app. However, the system also distinguishes between novice and advanced users in terms of presenting more information related to the level of access. Figure 7.13 shows the historical interface for the novice user, which contains icons to represent each data type.

The size of the icon indicates the usage of each data type to make the interface easy to understand; whilst the advanced and intermediate users can see a chart for the privacy-related information usage, as shown in Figure 7.14.

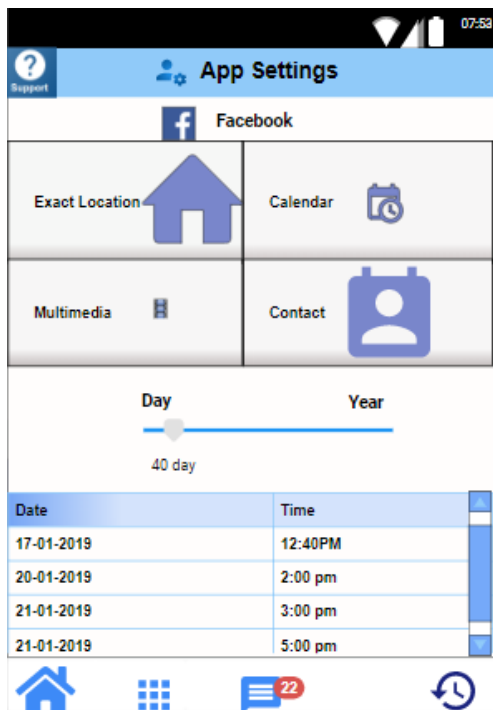


Figure 7.13: Historical Interface for Novice User

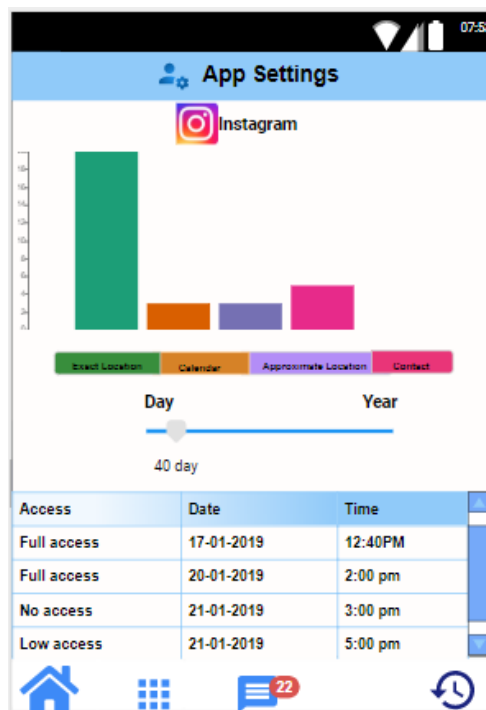


Figure 7.14: Historical Interface for Advanced User

7.5 Evaluation of the Proposed Approach

As discussed in the literature review that numerous studies evaluated their systems in term of a technical issue for capturing and monitoring the data. Therefore, the main goal of this section is to achieve a comprehensive understanding of the effectiveness of the proposed approach regarding ease of use, comprehension, user satisfaction and enhance their awareness about privacy on mobile apps. Hence, this study focuses more specifically on the end-user interaction with at the interface level. Despite the user feedback results obtained in Chapter Five and Chapter Six, there is a need for additional qualitative evaluation by the core stakeholders of the system and experts to investigate users'

acceptance and satisfaction in-depth, which is difficult to achieve through purely quantitative approaches.

Two separate stakeholders (end users - experts) were involved in the focus group. The investigative questions for the end-users were about their perceptions and acceptance of the proposed system. When it comes to the experts, the questions were more advanced and were about the feasibility, achievability, and practicality of the system.

Five experts were invited to the focus group at The Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), July 2019, in Nicosia to evaluate the proposed system and whether it could meet users' privacy preferences and enhance privacy technology. When the experts accepted to participate in the focus group, each was asked to sign a consent form. A summary of how the system works, including screenshots of the interfaces and a question list, was presented to the experts. The session was recorded after gaining the permission of the focus groups interviewees, and was transcribed afterwards. The focus groups lasted approximately an hour. Table 7.3 shows a summary of the participants' background and their assigned IDs.

ID	Participants
A1	Researcher in user security and privacy
A2	Researcher in Cyber-Social Engineering
A3	Researcher in Information Security and Risk Management
A4	Researcher in Information Security Policy
A5	Researcher in IT

Table 7.3: Expert Participants' Background

As has previously been identified (in Chapter 4), end-users are the main stakeholders of the system, therefore, their opinions on the system are essential. Moreover, experts have been involved in order to provide a more accurate scientific judgment of the proposed system, and to better understand the acceptability and usability of the system. The

questions were drafted and reviewed in terms of being understandable and objective in order to achieve the aims of the focus group method. The purpose of the evaluation questions can be summarised as follows:

- To evaluate the identified research problem.
- To evaluate the feasibility, achievability, and practicality of the method.
- To identify the strengths and weaknesses of the developed system.
- To identify the key barriers moving forward.
- The attractiveness of the format and layout of the system interfaces.
- To evaluate the three-level approach, which includes novice, intermediate and advanced.
- To evaluate the main dashboard.
- To assess users' satisfaction with colour.
- To evaluate the utilisation of the following functions in the proposed approach and if it could enhance the user's awareness about privacy-related information?
 - Historical privacy
 - Controlling privacy
 - Notification
- To obtain suggestions in order to integrate anything that might have been missed from the system.
- To gain the experts' and end users' opinions about the system and whether it is easy to use.
- To evaluate the utilisation of the prioritisation privacy-related information based on users' privacy preferences.
- To obtain the users' feelings about understanding the components and the features of each interface of the system.

7.5.1 Experts

The interviews with the experts revealed valuable outcomes regarding the open-ended questions. The following number of themes or key points are identified to gain useful insight from the participants' perceptions and experiences concerning the proposed solution in this research.

A. The importance of the identified research problem

Regarding the first question, which is about the relevance of the research problem identified, they indicated that it is considered a vital issue in terms of how to manage a large volume of data, designing for usable privacy, and transparency, therefore the solution should be valuable.

A3 states: *"This research addressed a vital issue related to privacy and it is a comprehensive solution which addressed different dimensions: usability, transparency and prioritisation. However, the prioritisation looks important question because if I have a hundred apps it is hard to control a large volume of apps"*. This, in turn, emphasises the importance of data ranking for the user, especially with the growth of apps, which makes it difficult for the user to control the huge amount of information.

A1 states: *"The research problem is so important because the proposed solution considers that privacy preferences are diverse and cannot adequately be captured by one-size-fits-all default settings"*. This feedback highlighted that it is unrealistic to assume homogeneous privacy requirements across the whole population as most prior studies proposed. Most of the prior studies assume the homogeneity of privacy preferences across users, yet users' privacy preferences differ from one user to another in the context of how to control and manage their data, prioritisation of information, personalised notifications, and levels of knowledge.

A4 states, " The research problem enhances user awareness and user empowerment which aims to inform users about the privacy consequences of the disclosure of sensitive information". This underlines the important role for risk impact feature, which could help the user to make an informed decision about protecting his or her privacy where the protection settings interface contains a risk impact interface. A1 and A5 also believed that notification feature is effective for enhancing users' awareness; especially the solution does not overwhelm the users with too much notification. This emphasised the feature of a personalised response system to inform and control the flow of privacy-related information according to the user's prioritisation.

In general, most of the expert opinions regarding evaluating the identified research problem were positive and they believed that the prioritisation of privacy-related information based on users' privacy preferences would be useful especially with the growth of apps, which makes it difficult for the user to control the huge amount of information. They also indicated that users need this solution because it would make privacy management significantly easier to perform and enhance the user's awareness.

B. The feasibility of the proposed design at the operational level

Regarding the feasibility, achievability, or practicality of the method: It is quite feasible, as long as the monitoring tool required detecting the privacy-related information is available. A1 and A4 have a concern about this approach could requires root permissions for the mobile device. Regarding this issue, the ReCon requires root permissions and knowledge about VPN technology, whilst PrivacyGuard does not require root permissions and runs in its entirety on the local device. Therefore, PrivacyGuard could be utilised as the implementation of this component.

In the context of the performance overheads of the system runtime, A3 and A2 indicate that it is possible to monitor sensitive information for users in real-time but they have a concern regarding the performance when the system handles a large volume of data.

A3 explained: *“The performance of the system should be considered for analysing very large and real-time data available from data repositories, social media, sensor networks and the Web”*. A2 also stated, *“Technically, it is possible to implement it”*. These comments reveal a positive impression concerning the possibility of its application in a real environment, taking into account the speed of system performance. Therefore, to be practical, the performance overheads of the system runtime must be minimal due to the system being comprehensive and handling a large volume of data. However, when looking at the proposed solution, it shows that prioritising the user’s information make the monitor focus on the most important information for the user, which will reduce the overheads in the system, as the system, in this case, will not monitor every single piece of data.

C. The convenience and usability of the proposed design

To investigate expert perceptions towards usability in terms of the colour, the layout, ease of use, and being easy to understand, they indicated these factors are convenient and usable to increase the user’s awareness. When it comes to the format and layout, A2 states, *“The format and the layout of the interfaces are well designed and the notification was easy to understand”*. A3 also stated *“The format and layout of the setting controls interface is considered as easy to use, and can help the user to recognise the level of privacy easily”*. This, in turn, emphasised the importance of utilised the colours of the traffic light feature to determine the protection level.

Experts' participants also indicate that when the historical interface contains icons to represent the usage of each data type, it makes the interface easy to understand for the novice user. This feedback highlighted that important to consider the level of knowledge during the interface design where the proposed solution considers the adaptive interface requirement. The goal of this requirement is to make the system understandable and learnable for the novice user, while at the same time not hindering the advanced user from working productively.

The reason for these positive results is due to the initial interfaces were designed based on HCI principles to overcome usability issues. Moreover, the initial interfaces were included in the survey in order to explore the users' thoughts regarding the design and the functionality of those interfaces, which in turn could help to overcome the usability limitations without compromising the users' convenience. However, some of them suggested changing the colour of the word clouds for the novice user interface to match with the app colour. For instance, the Facebook app uses a blue colour for the Facebook icon, therefore the word cloud should use the blue colour; hence the user can quickly scan the interface.

D. Evaluation of the three-level approach, which includes novice, intermediate and advanced.

Concerning experts' opinions on the three-level approach that is provided by the system, which includes novice, intermediate and advanced, they claimed that the approach made the system flexible and accommodating to novice and advanced users. Although novice users may need more assistance and systematic guidance to understand the indications of some symbols that are used to represent the information and how to use the settings of the system. A3 explained, "*In terms of usability, novice user needs more guidance and tutorial to understand the system at glance*". However, although the system was designed

to provide some assistance to understand the nature of privacy work and help in decision-making, there seems to be a need to include more support for novice users, as the experts suggested.

E. The key barriers in the proposed system

When it comes to identifying the key barriers moving forward, they indicated that the motivation aspect is one of the key challenges to using the system. Therefore, they stated that information privacy concerns have an essential impact on enhancing users' privacy awareness. Increasing users' concerns regarding the importance of privacy could significantly motivate users to preserve their privacy and enhance their awareness. They suggested increasing the risk impact features that are provided by the system to justifiably heighten their concerns and hence increase the use of the system.

Regarding utilising the historical view, and controlling the information and notifications in the proposed system, they believe using these features would provide users with effective transparency into the system and reduce privacy concerns. However, while the prioritisation of the categories of apps in the historical interface and app settings is a great idea to implement, it would require more description to explain to the user how the system uses prioritisation for the apps on these interfaces. In general, prioritisation of information would significantly reduce the burden while allowing users to better control information.

F. The convenience of the main dashboard

To ensure that the main dashboard of the developed system allows the user to quickly control and track the use of information or not, generally, most experts agree that the main dashboard has achieved the purpose of its function and design.

G. Identifying the strengths and weaknesses of the developed system.

Moving forward to exploring the experts' opinions about the system's strengths and weaknesses, two lists have been driven by their opinions:

Strengths:

- The system utilises many efficient methods for enhancing users' awareness about privacy-related information on mobile apps, which includes the historical view, prioritisation of user's information, multi-level privacy controls and considering the user's knowledge.
- The historical view increases the transparency of the sharing process.
- The risk impact interface helps users to understand the privacy risks and motivates users to respond.
- The system gathers different functions regarding privacy together in one place, which reduces the user's burden and frustration.
- It is very useful to use the system because it allows users to know who has accessed their data, when and at what degree of granularity.

However, the experts identified some weaknesses or concerns, some of which have already been implemented or taken into account, and others that can be considered in future work:

- Another method for presenting the information is to display the apps that most commonly share a user's information.
- In term of usability, the novice user needs more guidance and a tutorial to understand the system quickly.
- It is better to show whether the user's information is related to the app's functionality or not.

- The multi-level of privacy controls requires more description to help the user to understand each level of each data.

Finally, despite some experts stating some concerns and weaknesses, in general, the majority of the experts' opinions on the system are positive.

7.5.2 End-Users

The aim of the focus group was to evaluate the system regarding ease of use, comprehension and user satisfaction. In order to make the questions understandable for the end-users, advanced questions were avoided and the questions simplified for them. Accordingly, a number of open-ended questions were asked in such a way to trigger discussion among the participants, which in turn revealed some interesting results.

All the participants agreed that they really need this system to enhance their awareness about privacy on mobile apps. It has educated them about how the different apps collect and share their information without their knowledge because the current privacy settings on mobile operating systems such as Android do not help users to know the frequency and destination of data being shared by apps. Therefore, they stated explicitly that they would be more aware of what information apps collect about them when they used this system. One of the participants said, *“The system would help them to check the usage of data in particular when my child uses his mobile because children are more exposed and vulnerable than adults.”* However, another participant stated regarding the usage of data *“A very important idea, it is designed very well, but it needs to explain how to use the word cloud for novice users”*. This, in turn, emphasises the point raised by the experts that novice users may need more support regarding understanding the system.

A number of participants indicated their desire to have multi-level privacy controls. One of the participants stated that providing multi-level of privacy controls would allow him

to limit the disclosure of their private information. Another participant liked the privacy controls on the dashboard because he struggled to find how to control his permissions from the current privacy settings on his mobile. However, these features need more description to explain the meaning of multi-level settings and how to use them. One of the participant said, "*It is a good project because this system supports his rights to control his personal information as the EU General Data Protection Regulation (or GDPR) stated.*"

Regarding the notifications, they like to be notified when an app wants to share their information based on their preferences. Despite the system allowing the user to know the implications of sharing their data, they need more features like this to enhance their awareness, and they suggested this to be through notifications, as the experts suggested.

In terms of adaptable privacy depending upon the prior knowledge feature, the participants indicated the need for this feature to make the system flexible and accommodating for novice and advanced users. One of the participants stated, "*It is a flexible system that provides different options for a different type of users*". Despite end-users wanting this feature in the system, they suggested including some steps and guidelines to help users to understand the differences between novices, intermediate and advanced users.

Some questions were asked to investigate users' usability perspectives regarding the ease of using some functions, and the colour and ease of understanding. They stated that the layout of the interfaces is simple and easy to use and navigate through, which is one of the advantages of this system. They do not see any difficulties in using the system by a simple user. However, one of the comments was, "*I enjoyed the good interfaces of the system. I suggest enhancing the colours*". Despite changing the colour of the initial design, it seems that this comment raises a vital point, which is about how to satisfy all

different users regarding the colours, which means more difficulty during the design. Another participant highlighted that the interfaces are well designed but he added one point regarding the description of the icons. He said, "*The system has been designed professionally but needs to add some descriptions for some icons*".

7.6 Conclusion

The requirements for the design and development of a privacy-enhancing technology framework for mobile devices have been established, followed by detailed architectural specifications designed in a modular and robust manner that would support such a system in practice, considering a personalised response; prioritisation of privacy-related information; multilevel privacy controls; usability, and the level of knowledge.

The architecture offers a mobile privacy awareness mechanism to enhance users' awareness and meet their needs to protect their privacy. The architecture also provides prioritisation of privacy-related information, based on an individual user basis to reduce user burden and the frustration of the user.

A comprehensive description of the system architecture, and its components and functionalities, has been provided. The architecture has the potential to meet the requirements of offering a holistic framework for increasing users' privacy awareness across the different mobile operating systems. Moreover, the mock-up interfaces have been designed, developed and presented in order to practically prove that the concept of the proposed architecture would work in practice.

This chapter has also presented a focus group evaluation by two separate groups: experts and end-users. The evaluation outcomes provide support for the view that the system has large potential to be implemented to help users to enhance their awareness and meet their needs to protect their privacy. The research problem identified represents a vital issue;

therefore, the solution should be valuable. With the rapid growth in mobile devices, the key barriers have become far less than a few years ago, and as such, this privacy system is able to monitor and detect privacy related information and could be applied across different operating systems on mobile apps. In general, the majority of the feedback from respondents was positive about the system. The outcomes confirm that the system provides more transparency and more control than current provision, to limit the disclosure of users' private information, and in turn, the system is capable not just of detecting but also protecting the user's privacy. Designing a good user interface, efficient management and the attractiveness of the system interfaces are the significant achievements of the system, which have been supported by the evaluation results. This system should gain a higher level of acceptability from the end-user and hence increase its opportunities to be deployed widely.

Chapter Eight

Conclusions and

Future Work

8. Conclusions and Future Work

This chapter presents and concludes the main achievements of this research. It begins with outlining the key contributions and achievements, and then proceeds to discuss the limitations of the research and identifies future research directions.

8.1 Achievements of the Research

Overall, the thesis has accomplished all the objectives and aims initially identified in Chapter One, with quantitative studies undertaken to meet users' requirements and needs in order to develop a mobile privacy awareness system and enhance privacy technology.

The key achievements of this research are:

- Reviewing the current privacy techniques across a range of platforms and applications in order to understand current state-of-the-art of privacy methods, including both the problems and available solutions.
- Developing a novel approach to manage and prioritise privacy-related information and assign users to the privacy profiles that most closely capture their privacy preferences by using machine learning.
- One of the significant achievements of the system is designing a usable user interface according to the user's perceptions and based on HCI principles to overcome the usability issues without compromising the user's convenience.
- To design and develop a framework for enhancing privacy technology on mobile devices to meet users' privacy preferences considering all these dimensions: multilevel privacy controls, personalisation responses, prioritisation privacy-related information and adaptable privacy-related guidance depending upon prior knowledge and experience.

- Evaluation of the proposed approach has also been accomplished to ensure that the objectives are met and they are as effective as they can be. The evaluation results of the experts and end-users can be considered as positive, constructive and valuable.

8.2 Limitations of the Research Project

Despite the concrete contributions and the achievements of the research having been accomplished, there are some limitations that have been identified, which are:

- Although the effectiveness of the privacy enhancing technology approach has been assessed by different groups - experts and end-users - through mock-up interfaces and the results were positive and valuable, it should be noted that the system was not a full implementation and captures real data in order to provide feedback and recommendations based on actual data. Fully operational software would be very useful to evaluate this approach in a real environment, and would have provided a better insight into the effectiveness of it.
- The data that is used to cluster users into different profiles is limited to two dimensions - app categories and data type – although it would be useful to add another dimension about the purpose of the app to share this information. This is required to analyse the static code and look up the third-party libraries to understand the purpose or functionality associated with each piece of data.
- The system categorises users into three types: novice, intermediate and advance according to the user's self-report in the initial interfaces. However, it would also be helpful to capture the user's level by monitoring the user's behaviour over time.
- This study has shown that is possible, theoretically, to predict the user's mobile app privacy preferences by asking the user a small number of questions. However,

this approach has neither been operationalised nor evaluated with actual users before.

8.3 Suggestions and Scope for Future Work

Despite the limitations mentioned above, this research has enhanced the privacy technology for mobiles in general, as illustrated by the experts and end-users' evaluation feedback. In addition, as with any research, this research offers many other opportunities that need further research and improvement. These suggestions are highlighted below:

- The system needs full implementation based on the proposed model in a real environment and monitoring real data. This is required to develop a technology to capture and measure privacy-related information across different mobile operating systems and different mobile resources, which might be difficult due to their operating system features and some technical aspects.
- Developing an interactive profile assignment that utilises permission settings on a user's mobile to elicit the user's privacy preferences would allow the system to generate a number of tailored questions about their privacy preferences in order to assign the user to the privacy profile that best aligns with their preferences.
- In addition, this research can also be further developed as a crowdsourcing system to provide each user with personalised recommendations when the user wants to make a decision to protect his data. The ten unique profiles could be utilised to generate recommended data settings for users in each cluster. It would help users to make informed decisions, in particular, the novice user, and reduce their degree of exposure.
- Further research could investigate the reasons behind the user's preference to grant certain information to a given app for a particular purpose (functionality/advertising) for further development.

8.4 The future of mobile phone privacy

The total number of mobile apps continues to increase and these apps can access and share storing financial, medical and business information that is considered is sensitive and valuable. Therefore, the enormous amount of private and personal information that is stored on the mobile phone has increased. Moreover, new technology allows mobile phones to connect to many smart devices at home and could control these devices from their mobile phones, e.g TVs, smart appliances, thermostats and smartwatch. Therefore, it would be difficult for the average user to assert control over such large amounts of data and it is undesirable to present a user with large privacy information or a large number of requests. The future of privacy protection on the mobile phone will have to consider seamless adaptation to include the evolution of wearables (e.g. smart glasses and watches) Internet of Things technologies in general. Therefore, it would be useful to prioritise user's privacy-related information according to user's preferences. This, in turn, would help user to manage a large volume of data and reduce privacy concerns.

References

1. 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.
2. 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.
3. Akman, O. *et al.* (2019) ‘Data Clustering and Self-Organizing Maps in Biology’, in *Algebraic and Combinatorial Computational Biology*. Elsevier, pp. 351–374.
4. Alaggan, M., Gambs, S. and Kermarrec, A.-M. (2015) ‘Heterogeneous Differential Privacy ’’, *Arxiv*, pp. 1–14.
5. Von Alan, R. H. *et al.* (2004) ‘Design science in information systems research’, *MIS quarterly*. Springer, 28(1), pp. 75–105.
6. Ali, S. *et al.* (2018) ‘Privacy and security issues in online social networks’, *Future Internet*. Multidisciplinary Digital Publishing Institute, 10(12), p. 114.
7. Allen & Overy (2016) *The EU General Data Protection Regulation*, *AllenOvery.com*. Available at: <http://www.allenoverly.com/publications/en-gb/data-protection/Pages/default.aspx> (Accessed: 1 September 2019).
8. 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.
9. Alrayes, F. and Abdelmoty, A. (2016) ‘Towards location privacy awareness on geo-social networks’, *International Conference on Next Generation Mobile Applications, Services, and Technologies*. IEEE, pp. 105–114. doi:

10.1109/NGMAST.2016.26.

10. 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.
11. Appari, A. and Johnson, M. E. (2010) 'Information security and privacy in healthcare: current state of research', *International Journal of Internet and Enterprise Management*, 6(4), p. 279. doi: 10.1504/IJIEM.2010.035624.
12. apple (2016) *Find My Friends: Share your location*. Available at: https://support.apple.com/kb/PH19426?locale=en_US (Accessed: 28 February 2017).
13. Apple (2015) 'Privacy Controls'. Available at: https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf (Accessed: 1 October 2017).
14. Babakus, E. and Mangold, W. G. (1992) 'Adapting the SERVQUAL scale to hospital services: an empirical investigation.', *Health services research*. Health Research & Educational Trust, 26(6), p. 767.
15. Baharuddin, R., Singh, D. and Razali, R. (2013) 'Usability dimensions for mobile applications-a review', *Res. J. Appl. Sci. Eng. Technol*, 5(6), pp. 2225–2231.
16. Bal, G., Rannenber, K. and Hong, J. I. (2015) 'Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns', *Computers and Security*, 53(69), pp. 187–202. doi: 10.1016/j.cose.2015.04.004.
17. 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*, pp. 12:1--12:11. doi: 10.1145/2501604.2501616.
18. Bateman, S., Gutwin, C. and Nacenta, M. (2008) *Seeing Things in the Clouds: The Effect of Visual Features on Tag Cloud Selections*. Available at:

www.amazon.com/tags (Accessed: 28 July 2019).

19. Bearden, W. O. and Netemeyer, R. G. (1999) *Handbook of marketing scales: Multi-item measures for marketing and consumer behavior research*. Sage.
20. Ben-Asher, N. *et al.* (2013) 'On the need for different security methods on mobile phones', *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services - MobileHCI '11*, 15(September 2015), p. 465. doi: 10.1145/1940941.1940971.
21. Benisch, M. *et al.* (2011) 'Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs', *Personal and Ubiquitous Computing*, 15(7), pp. 679–694. doi: 10.1007/s00779-010-0346-0.
22. Boutsis, I. and Kalogeraki, V. (2013) 'Privacy preservation for participatory sensing data', *2013 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, (March), pp. 103–113. doi: 10.1109/PerCom.2013.6526720.
23. Brandimarte, L., Acquisti, A. and Loewenstein, G. (2012) 'Misplaced Confidences: Privacy and the Control Paradox', *Social Psychological and Personality Science*, 4(3), pp. 340–347. doi: 10.1177/1948550612455931.
24. Bryman, A. (2016) *Social research methods*. Oxford university press.
25. Bryman, A. and Bell, E. (2011) 'Ethics in business research', *Business Research Methods*, 7(5), pp. 23–56.
26. Budiu, R. (2014) *Memory Recognition and Recall in User Interfaces*, *Human Computer Interaction*. Available at: <https://www.nngroup.com/articles/recognition-and-recall/> (Accessed: 21 October 2019).
27. Bugiel, S., Sadeghi, A.-R. and Heuser, S. (2013) 'Flexible and Fine-grained Mandatory Access Control on Android for Diverse Security and Privacy Policies', in *22nd USENIX Security Symposium*. Washington, pp. 131–146.

28. Caine, K. *et al.* (2015) 'Designing a Patient-Centered User Interface for Access Decisions about EHR Data: Implications from Patient Interviews', *Journal of General Internal Medicine*, 30(1), pp. 7–16. doi: 10.1007/s11606-014-3049-9.
29. Cao, Q. *et al.* (2012) 'Aiding the detection of fake accounts in large scale social online services', *NSDI'12 Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, p. 15.
30. Carson, D. (2001) *Qualitative marketing research*. SAGE.
31. Chen, J.-W. and Zhang, J. (2007) 'Comparing text-based and graphic user interfaces for novice and expert users', in *AMIA annual symposium proceedings*. American Medical Informatics Association, p. 125.
32. Chiasson, S., Van Oorschot, P. C. and Biddle, R. (2006) *A Usability Study and Critique of Two Password Managers*.
33. Chin, E. *et al.* (2012a) 'Measuring user confidence in smartphone security and privacy', *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, (1), p. 1. doi: 10.1145/2335356.2335358.
34. Chin, E. *et al.* (2012b) 'Measuring user confidence in smartphone security and privacy', *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, (1), p. 1. doi: 10.1145/2335356.2335358.
35. Christin, D., Reinhardt, A., Kanhere, Salil S., *et al.* (2011) 'A survey on privacy in mobile participatory sensing applications', *Journal of Systems and Software*. Elsevier Inc., 84(11), pp. 1928–1946. doi: 10.1016/j.jss.2011.06.073.
36. Christin, D., Reinhardt, A., Kanhere, Salil S, *et al.* (2011) 'A survey on privacy in mobile participatory sensing applications', *Journal of systems and software*. Elsevier, 84(11), pp. 1928–1946.
37. Christin, D. *et al.* (2012) 'Exploring user preferences for privacy interfaces in mobile sensing applications', *Proceedings of the 11th International Conference on*

- Mobile and Ubiquitous Multimedia, MUM 2012*. doi: 10.1145/2406367.2406385.
38. Christin, D., Michalak, M. and Hollick, M. (2013) 'Raising User Awareness about Privacy Threats in Participatory Sensing Applications through Graphical Warnings', *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*, p. 445. doi: 10.1145/2536853.2536861.
39. Chua, W. Y. and Chang, K. T. T. (2016a) '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.
40. Chua, W. Y. and Chang, K. T. T. (2016b) '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.
41. Chung, W. and Paynter, J. (2002) 'Privacy issues on the Internet', *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2002-Janua(c), pp. 1–9. doi: 10.1109/HICSS.2002.994191.
42. CIO (2013) *Privacy in mobile apps Guidance for app developers*. Available at: <https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf> (Accessed: 30 September 2019).
43. Cohen, J. (1992) *A Power Primer*, *Psychological Bulletin* [*PsycARTICLES*]. Available at: <http://www2.psych.ubc.ca/~schaller/528Readings/Cohen1992.pdf> (Accessed: 15 February 2019).
44. Consortium, W. W. W. (2002) 'The platform for privacy preferences 1.0 (P3P1. 0) specification'. World Wide Web Consortium.
45. Cornelius, C. *et al.* (2008) 'AnonySense : Privacy-Aware People-Centric Sensing Categories and Subject Descriptors'.

46. 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.
47. Creswell, J. W. (2014) *A concise introduction to mixed methods research*. SAGE publications.
48. Cristofaro, E. De and Soriente, C. (2013) 'Participatory privacy: Enabling privacy in participatory sensing', *IEEE Network*, 27(1), pp. 32–36. doi: 10.1109/MNET.2013.6423189.
49. Deubel, P. (2003) 'An investigation of behaviorist and cognitive approaches to instructional multimedia design', *Journal of educational multimedia and hypermedia*. Association for the Advancement of Computing in Education (AACE), 12(1), pp. 63–90.
50. Devlin, S. J., Dong, H. K. and Brown, M. (1993) 'Selecting a scale for measuring quality.', *Marketing research*, 5(3).
51. Dhawan, M. and Ganapathy, V. (2009) 'Analyzing Information Flow in JavaScript - based Browser Extensions JavaScript - based Extensions (JSEs)', *Computer Security Applications Conference, 2009. ACSAC 09. Annual*, (December), pp. 382–391. doi: <http://doi.ieeecomputersociety.org/10.1109/ACSAC.2009.43>.
52. Dimitriou, T., Krontiris, I. and Sabouri, A. (2012) 'PEPPER : A Querier ' s Privacy Enhancing', pp. 93–106.
53. 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.
54. 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.

55. European Commission (2016a) *JUST Newsroom - Article 29 Working Party - European Commission*. Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (Accessed: 14 March 2017).
56. European Commission (2016b) *Reform of EU data protection rules - European Commission*. Available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm (Accessed: 14 March 2017).
57. Faresi, A. Al, Alazzawe, Ahmed and Alazzawe, Anis (2014) 'Privacy leakage in health social networks', *Computational Intelligence*, 30(3), pp. 514–534. doi: 10.1111/coin.12005.
58. Federal Trade Commission (2013) 'Mobile privacy disclosures - Building trust through transparency', (February), p. 29.
59. Felt *et al.* (2012) 'Android Permissions: User Attention, Comprehension, and Behavior'. doi: 10.1145/2335356.2335360.
60. Felt, A. P., Egelman, S. and Wagner, D. (2012) 'I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns', *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 33–44. doi: 10.1145/2381934.2381943.
61. Fire, M., Gilad, K. and Elovici, Y. (2012) 'Strangers Intrusion Detection - Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies', pp. 26–39.
62. Fire, M., Goldschmidt, R. and Elovici, Y. (2013) 'Online Social Networks: Threats and Solutions Survey', *IEEE COMMUNICATION SURVEYS & TUTORIALS Online*, 16(4), pp. 1–20. doi: 10.1109/COMST.2014.2321628.
63. Fuchs, C. (2011) 'Towards an alternative concept of privacy', *Journal of Information, Communication and Ethics in Society*, 9(4), pp. 220–237. doi: 10.1108/14779961111191039.

64. Gall, M. D., Borg, W. R. and Gall, J. P. (1996) *Educational research: An introduction*. Longman Publishing.
65. GDPR (2018) *Transparency and the GDPR: Practical guidance and interpretive assistance from the Article 29 Working Party*. Available at:
<https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/> (Accessed: 5 October 2019).
66. Gerber, P. *et al.* (2016) 'Usability versus Privacy instead of Usable Privacy [Google ' s balancing act between usability and privacy]', 45(February), pp. 16–21.
67. Gjørseter, T. (2015) 'Interaction with mobile augmented reality: An exploratory study using design research to investigate mobile and handheld augmented reality'. The University of Bergen.
68. Google (2015) *Manifest.permission_group | Android Developers*. Available at:
https://developer.android.com/reference/android/Manifest.permission_group
(Accessed: 1 October 2017).
69. Gruen, D. M. *et al.* (2007) 'Getting our head in the clouds: Toward evaluation studies of tagclouds'. doi: 10.1145/1240624.1240775.
70. Guba, E. G., & Lincoln, Y. S. (1994) *Competing paradigms in qualitative research*. Sage.
71. Guha, S. *et al.* (2012) 'Autowitness: locating and tracking stolen property while tolerating gps and radio outages', *ACM Transactions on Sensor Networks (TOSN)*, pp. 29–42. doi: 10.1145/1869983.1869988.
72. 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.
73. Hall, R. H. and Hanna, P. (2004) 'The impact of web page text-background colour

- combinations on readability, retention, aesthetics and behavioural intention’, *Behaviour & information technology*. Taylor & Francis, 23(3), pp. 183–195.
74. Hamed, A. and Ayed, H. K. Ben (2015) ‘Privacy scoring and users’ awareness for Web tracking’, *2015 6th International Conference on Information and Communication Systems, ICICS 2015*, pp. 100–105. doi: 10.1109/IACS.2015.7103210.
75. Hedin, D. *et al.* (2014) ‘JSFlow: Tracking information flow in JavaScript and its APIs’, *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, pp. 1663–1671. doi: 10.1145/2554850.2554909.
76. Hevner, A. and Chatterjee, S. (2010) ‘Design Science Research in Information Systems’, in, pp. 9–22. doi: 10.1007/978-1-4419-5653-8_2.
77. Himma, K. E. and Tavani, H. T. (2009) *The Handbook of Information and Computer Ethics, The Handbook of Information and Computer Ethics*. doi: 10.1002/9780470281819.
78. 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.
79. Humphreys, L., Gill, P. and Krishnamurthy, B. (2010) ‘How much is too much? Privacy issues on Twitter’, *Ica 2010*, 1, pp. 1–29. doi: 10.1145/2181176.2181178.
80. Hwang, T. K. P. and Yu, H.-Y. (2011) ‘Accommodating Both Expert Users and Novice Users in One Interface by Utilizing Multi-layer Interface in Complex Function Products’, in. Springer, Berlin, Heidelberg, pp. 159–165. doi: 10.1007/978-3-642-21660-2_18.
81. Iachello *et al.* (2006) ‘Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world’, *Proceedings of the SIGCHI conference on*

- Human Factors in computing systems - CHI '06*, p. 1009. doi:
10.1145/1124772.1124923.
82. Ibrahim, T., Furnell, S. M., Papadaki, M., & Clarke, N. L. (2014) 'Assessing the Usability of Personal Internet Security Tools', *Igarss 2014*, (1), pp. 1–5. doi: 10.1007/s13398-014-0173-7.2.
83. Ibrahim, T. *et al.* (2010) 'Assessing the usability of end-user security software', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6264 LNCS, pp. 177–189. doi: 10.1007/978-3-642-15152-1_16.
84. Ilija, P. *et al.* (2015) 'Face/off: Preventing privacy leakage from photos in social networks', *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 781–792. doi: 10.1145/2810103.2813603.
85. Insight, C. (2019) *Wearables Market to Be Worth \$25 Billion by 2019 - CCS Insight*. Available at: <https://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight/> (Accessed: 18 November 2019).
86. *Internet Growth Statistics* (2019). Available at: <https://internetworldstats.com/emarketing.htm> (Accessed: 13 August 2019).
87. Islam, M. N. (2017) 'Using a Design Science Research Approach in Human-Computer Interaction (HCI) Project: Experiences, Lessons and Future Directions', *International Journal of Virtual and Augmented Reality (IJVAR)*. IGI Global, 1(2), pp. 42–59.
88. ISO 9241, I. 159/SC 4 E. of human-system interaction (1998) *Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs).: Guidance on Usability*. International Organization for Standardization.
89. Jamie Carter (2014) *Wearable cameras are all the rage but should we all become*

- lifeloggers?* / *TechRadar*. Available at: <http://www.techradar.com/news/world-of-tech/life-through-a-lens-trials-and-tribulations-of-a-life-logger-1251717> (Accessed: 24 February 2017).
90. Jamie McGinnes (2010) *Facebook users fleeced by hackers* / *The Sunday Times*. Available at: http://www.thesundaytimes.co.uk/sto/news/uk_news/Society/article387158.ece (Accessed: 14 March 2017).
91. Johnston, J., Eloff, J. H. P. and Labuschagne, L. (2003) 'Security and human computer interfaces', *Computers and Security*. doi: 10.1016/S0167-4048(03)00006-3.
92. Katsabas, Dimitris, S. M. Furnell, and P. S. (2005) 'Proceedings of The Fifth International Network Conference 2005 (INC 2005) - Steven Furnell, Paul Dowland, Georgios Kormentzas - Google Books', in *Proceedings of the Fifth International Network Conference*. Greece.
93. Kazemi, L. and Shahabi, C. (2013) 'TAPAS: Trustworthy privacy-aware participatory sensing', *Knowledge and Information Systems*, 37(1), pp. 105–128. doi: 10.1007/s10115-012-0573-y.
94. 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.
95. Kezer, M. *et al.* (2016) 'Age differences in privacy attitudes, literacy and privacy management on Facebook', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1). doi: 10.5817/CP2016-1-2.
96. Kim, F. (2015) *Indicators, Validations, and Notifications: Pick the Correct Communication Option*. Available at: <https://www.nngroup.com/articles/indicators->

validations-notifications/ (Accessed: 19 October 2019).

97. Kim, Seung Hyun, Ko, I. Y. and Kim, Soo Hyung (2017) 'Quality of Private Information (QoPI) model for effective representation and prediction of privacy controls in mobile computing', *Computers and Security*. Elsevier Ltd, 66, pp. 1–19. doi: 10.1016/j.cose.2017.01.002.
98. Klasnja, P. *et al.* (2009) 'Exploring privacy concerns about personal sensing', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5538 LNCS, pp. 176–183. doi: 10.1007/978-3-642-01516-8_13.
99. Krasnova, H. and Veltri, N. F. (2010) 'Privacy calculus on social networking sites: Explorative evidence from Germany and USA', *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 1–10. doi: 10.1109/HICSS.2010.307.
100. Krombholz, K., Merkl, D. and Weippl, E. (2012) 'Fake identities in social media: A case study on the sustainability of the Facebook business model', *Journal of Service Science Research*, 4(2), pp. 175–212. doi: <http://dx.doi.org/10.1007/s12927-012-0008-z>.
101. Kuhn, T. S. (1962) 'The Structure of Scientific Revolutions (3rd, 1996 ed.)'. Chicago: University of Chicago Press.
102. Kulyk, O. *et al.* (2016) 'Encouraging privacy-aware smartphone app installation: Finding out what the technically-adept do', *Proceedings of the Usable Security Workshop*, (February). doi: 10.14722/usec.2016.23016.
103. Kumaraguru, P. and Cranor, L. (2005) 'Privacy indexes: A survey of westin's studies', *School of Computer Science, Carnegie Mellon University*, Tech. rep.(December), pp. 1–22. Available at: <http://repository.cmu.edu/isr%5Cnhttp://www.casos.cs.cmu.edu/publications/papers>

/CMU-ISRI-05-138.pdf%5Cnhttp://repository.cmu.edu/isr/856/.

104. LaTouche, L. W. (2013) 'Usability Issues in the User Interfaces of Privacy-Enhancing Technologies.', *ProQuest LLC*. ERIC.
105. Le, A., Irvine, U. C., *et al.* (2015) 'AntMonitor : A System for Monitoring from Mobile Devices', (1), pp. 15–20.
106. Le, A., Varmarken, J., *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.
107. Levin, A. and Abril, P. S. (2009) 'Two Notions of Privacy Online.', *Vanderbilt Journal of Entertainment & Technology Law*, 11(4), pp. 1001–1051.
108. Li, J. (2013) "'Privacy policies for health social networking sites'", *Journal of the American Medical Informatics Association : JAMIA*, 20(4), pp. 704–7. doi: 10.1136/amiajnl-2012-001500.
109. Lin, J. *et al.* (2012) 'Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing', *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, p. 501. doi: 10.1145/2370216.2370290.
110. Lin, J. *et al.* (2014a) 'Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings', *12th USENIX security symposium.*, pp. 199–212.
111. Lin, J. *et al.* (2014b) 'Modeling Users ' Mobile App Privacy Preferences : Restoring Usability in a Sea of Permission Settings', *Proceedings of the tenth Symposium on Usable Privacy and Security*, 1, pp. 1–14.
112. 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).
113. Liu, Y. *et al.* (2015) ‘Identifying Personal Information in Internet Traffic’.
114. Liu, Y. *et al.* (2016) ‘An improved design of wearable strain sensor based on knitted RFID technology’, in *2016 IEEE Conference on Antenna Measurements & Applications (CAMA)*. IEEE, pp. 1–4. doi: 10.1109/CAMA.2016.7815769.
115. Lynch, P. J. (2008) *Web style guide*. Yale University Press.
116. Madden, M. *et al.* (2013) ‘Teens , Social Media , and Privacy’.
117. Mao, H., Shuai, X. and Kapadia, A. (2011) ‘Loose Tweets: An Analysis of Privacy Leaks on Twitter: An Analysis of Privacy Leaks on Twitter’, *10th annual ACM workshop on Privacy in the electronic society - WPES '11*, p. 1. doi: 10.1145/2046556.2046558.
118. Michelfelder (2001) ‘The moral value of informational privacy in cyberspace’, *CEUR Workshop Proceedings*, 1225(March), pp. 41–42. doi: 10.1023/A.
119. Motti, V. G. and Caine, K. (2015) ‘Users’ privacy concerns about wearables: Impact of form factor, sensors and type of data collected’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8976, pp. 231–244. doi: 10.1007/978-3-662-48051-9_17.
120. Mugan, J., Sharma, T. and Sadeh, N. (2011) ‘Understandable Learning of Privacy Preferences Through Default Personas and Suggestions’, pp. 1–31. Available at: <http://reports-archive.adm.cs.cmu.edu/anon/anon/usr0/ftp/home/ftp/isr2011/CMU-ISR-11-112.pdf>.
121. Muñoz-Arteaga, J., González, R. M. and Vanderdonckt, J. (2008) ‘A classification of security feedback design patterns for interactive web applications’, *Proceedings - The 3rd International Conference on Internet Monitoring and Protection, ICIMP*

- 2008, pp. 166–171. doi: 10.1109/ICIMP.2008.21.
122. Muslukhov, I. *et al.* (2012) ‘Understanding users’ requirements for data protection in smartphones’, *Proceedings - 2012 IEEE 28th International Conference on Data Engineering Workshops, ICDEW 2012*, pp. 228–235. doi: 10.1109/ICDEW.2012.83.
123. 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.
124. Nguyen (2016) *The Most Successful Wearables for Consumers | Wearable Technologies*. Available at: <https://www.wearable-technologies.com/2016/01/the-most-successful-wearables-for-consumers/> (Accessed: 28 March 2017).
125. Nielsen, J. (1994) ‘10 Heuristic Principles’, *Uxness*. Available at: <http://www.uxness.in/2015/02/10-heuristic-principles-jakob-nielsens.html>.
126. Nielsen, J. (2010) *PART 1 PART 1 Defining Usability*. Available at: https://booksite.elsevier.com/samplechapters/9780123751140/02~Chapter_1.pdf (Accessed: 4 October 2019).
127. Nielsen, J. (2012) *Usability 101: Introduction to Usability*. Available at: <https://www.nngroup.com/articles/usability-101-introduction-to-usability/> (Accessed: 5 November 2019).
128. 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.
129. Ons.gov.uk (2018) *Internet users, UK - Office for National Statistics*. Available at: <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/int>

ernetusers/2019 (Accessed: 1 January 2020).

130. Page, T. (2015) 'A Forecast of the Adoption of Wearable Technology', *International Journal of Technology Diffusion*, 6(2), pp. 12–29. doi: 10.4018/IJTD.2015040102.
131. Paul, T. *et al.* (2012) 'C4PS - helping facebookers manage their privacy settings', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7710, pp. 188–201. doi: 10.1007/978-3-642-35386-4_15.
132. Pearce, P., Felt, A. P. and Wagner, D. (2012) 'AdDroid: Privilege Separation for Applications and Advertisers in Android', *ACM Symposium on Information, Computer and Communication Security (ASIACCS)*. doi: 10.1145/2414456.2414498.
133. Peter, J. P. (1979) 'Reliability: A review of psychometric basics and recent marketing practices', *Journal of marketing research*. SAGE Publications Sage CA: Los Angeles, CA, 16(1), pp. 6–17.
134. Pistoia, M. *et al.* (2015) 'Labyrinth: Visually Configurable Data-Leakage Detection in Mobile Applications', *Proceedings - IEEE International Conference on Mobile Data Management*, 1, pp. 279–286. doi: 10.1109/MDM.2015.69.
135. Plaisant, C. and Shneiderman, B. (2005) 'Show me! Guidelines for producing recorded demonstrations', in *2005 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC'05)*. IEEE, pp. 171–178.
136. Politou, E., Alepis, E. and Patsakis, C. (2018) 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions', *Journal of Cybersecurity*. Oxford University Press, 4(1), p. tyy001.
137. Raij, A. *et al.* (2011) 'Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment', *Proceedings of the 2011 annual*

- conference on Human factors in computing systems - CHI '11*, p. 11. doi:
10.1145/1978942.1978945.
138. Rasthofer, S. *et al.* (2014) 'DROID FORCE: Enforcing Complex, Data-Centric, System-Wide Policies in Android', *International Conference on Availability, Reliability and Security*, Ninth, pp. 40–49.
139. Regulation of Investigatory Powers Act (2012) 'Regulation of Investigatory Powers Act 2000'. Statute Law Database. Available at:
<http://www.legislation.gov.uk/ukpga/2000/23/contents> (Accessed: 14 March 2017).
140. Ren, J. *et al.* (2016) 'ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic', *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '16)*, pp. 361–374. doi:
10.1145/2906388.2906392.
141. Richards, K. (2003) *Qualitative inquiry in TESOL*. Springer.
142. Richmond (2010) *For Sale: Fake and Stolen Facebook Accounts - The New York Times*. Available at:
<http://www.nytimes.com/2010/05/03/technology/internet/03facebook.html>
(Accessed: 14 March 2017).
143. Romero-Tris, C. *et al.* (2015) 'Design of a P2P network that protects users' privacy in front of Web Search Engines', *Computer Communications*, 57, pp. 37–49. doi: 10.1016/j.comcom.2014.09.003.
144. Rose, K., Eldridge, S. and Lyman, C. (2015) 'The internet of things: an overview', *Internet Society*, (October), p. 53. doi: 10.1017/CBO9781107415324.004.
145. Ross, K. W. and Maltz, D. A. (2011) 'Inflight Modifications of Content: Who are the Culprits?', *Leet II*.
146. Schaub, F., Balebako, R. and Cranor, L. F. (2017) 'Designing Effective Privacy Notices and Controls', *IEEE Internet Computing*, 21(3), pp. 70–77. doi:

10.1109/MIC.2017.75.

147. Sheikh, K., Wegdam, M. and van Sinderen, M. (2008) 'Quality-of-context and its use for protecting privacy in context aware systems.', *JSW*, 3(3), pp. 83–93.
148. Sipior, J. C., Ward, B. T. and Mendoza, R. A. (2011) 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons', *Journal of Internet Commerce*, 10(1), pp. 1–16. doi: 10.1080/15332861.2011.558454.
149. Song, Y. (2015) 'PrivacyGuard : A VPN-Based Approach to Detect Privacy Leakages on Android Devices', pp. 15–26. doi: 10.1145/2808117.2808120.
150. Soni, M. (2012) 'AN OVERVIEW ON CLUSTERING METHODS', *IOSR Journal of Engineering*, 2, pp. 719–725.
151. Squicciarini, A. C., Shehab, M. and Paci, F. (2009) 'Collective privacy management in social networks', *Proceedings of the 18th international conference on World wide web - WWW '09*, p. 521. doi: 10.1145/1526709.1526780.
152. Stahl, B. C. (2007) 'Positivism or Non-Positivism-Tertium Non Datur Sexual Exploitation of Children in the Digital Society View project Responsible Innovation View project'. doi: 10.1007/978-0-387-37022-4_5.
153. Starov, O. and Nikiforakis, N. (2018) 'PrivacyMeter: Designing and developing a privacy-preserving browser extension', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10953 LNCS, pp. 77–95. doi: 10.1007/978-3-319-94496-8_6.
154. Statista (2017) • *UK: mobile phone ownership 1996-2018* / Statista. Available at: <https://www.statista.com/statistics/289167/mobile-phone-penetration-in-the-uk/> (Accessed: 28 December 2019).
155. Statista (2016) *Number of worldwide social network users 2010-2020* / Statistic. Available at: <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/> (Accessed: 14 March 2017).

156. Statista (2018) • *Adblock usage* | *Statista*. Available at:
<https://www.statista.com/statistics/351862/adblocking-usage/> (Accessed: 24 December 2019).
157. Stuart J. Johnston (2010) *Microsoft Survey: Online 'Reputation' Counts - InternetNews*. Available at:
<http://www.internetnews.com/webcontent/article.php/3861241/Microsoft+Survey+Online+Reputation+Counts.htm> (Accessed: 30 March 2017).
158. Takano, Y. *et al.* (2014) 'MindYourPrivacy: Design and implementation of a visualization system for third-party Web tracking', *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014*. IEEE, pp. 48–56. doi: 10.1109/PST.2014.6890923.
159. Talebi, N., Hallam, C. and Zanella, G. (2016) 'The new wave of privacy concerns in the wearable devices era', in *2016 Portland International Conference on Management of Engineering and Technology (PICMET)*, pp. 3208–3214. doi: 10.1109/PICMET.2016.7806826.
160. Thierer, A. D. (2014) 'the Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation', *J.L. & Tech*, 2(1). doi: 10.2139/ssrn.2494382.
161. Tong, A. *et al.* (2012) 'Enhancing transparency in reporting the synthesis of qualitative research: ENTREQ', *BMC Medical Research Methodology*. BioMed Central, 12(1), p. 181. doi: 10.1186/1471-2288-12-181.
162. Toubiana, V. *et al.* (2012) 'Photo-TaPE: User Privacy Preferences in Photo Tagging', *Proceedings of the 21st International Conference on World Wide Web*, pp. 617–618. doi: 10.1145/2187980.2188155.
163. Trend Micro (2015) *Facebook Privacy Scanner*. Available at:
<http://docs.trendmicro.com/en-us/consumer/titanium2013/tools/facebook-privacy->

- scanner.aspx (Accessed: 15 March 2017).
164. 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).
165. van der Velden, M. and El Emam, K. (2013) “‘Not all my friends need to know’”: A qualitative study of teenage patients, privacy, and social media.’, *Journal of the American Medical Informatics Association : JAMIA*, 20, pp. 16–24. doi: 10.1136/amiajnl-2012-000949.
166. Ventola, C. L. (2014a) ‘Mobile devices and apps for health care professionals: uses and benefits’, *Pharmacy and Therapeutics*. MediMedia, USA, 39(5), p. 356.
167. Ventola, C. L. (2014b) ‘Social media and health care professionals: benefits, risks, and best practices.’, *P & T: a peer-reviewed journal for formulary management*. MediMedia, USA, 39(7), pp. 491–520. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/25083128> (Accessed: 29 March 2017).
168. Wagner, I. *et al.* (2016) ‘User interface design for privacy awareness in eHealth technologies’, *2016 13th IEEE Annual Consumer Communications and Networking Conference, CCNC 2016*, (September), pp. 38–43. doi: 10.1109/CCNC.2016.7444728.
169. Walls, J., Widmeyer, G., and El Sawy, O. (1992) ‘Building an Information System Design Theory for Vigilant EIS’, *Information Systems Research*, 36–59.
170. Walters, N. (2014) ‘Improving Mobile Device Privacy Disclosures’.
171. Wang *et al.* (2011) ‘Who Is Concerned about What? A Study of American, Chinese and Indian Users’ Privacy Concerns on Social Network Sites’, *Trust and trustworthy computing*, 10, pp. 146–153. doi: 10.1007/978-3-642-21599-5_11.
172. Watson, J., Lipford, H. R. and Besmer, A. (2015) ‘Mapping user preference to privacy default settings’, *ACM Transactions on Computer-Human Interaction*,

22(6). doi: 10.1145/2811257.

173. Werthmann, T. *et al.* (2013) ‘PSiOS: bring your own privacy & security to iOS devices’, *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13*, p. 13. doi: 10.1145/2484313.2484316.
174. Westin, A. F. (1968) ‘Privacy and Freedom.’, *American Sociological Review*, 33(1), p. 173. doi: 10.2307/2092293.
175. Whitten, A. and Tygar, J. D. (1999) ‘Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.’, in *USENIX Security Symposium*, pp. 169–184.
176. Wisniewski, P. J., Knijnenburg, B. P. and Lipford, H. R. (2016) ‘Making privacy personal: Profiling social network users to inform privacy education and nudging’. doi: 10.1016/j.ijhcs.2016.09.006.
177. Wisniewski, P. J., Knijnenburg, B. P. and Lipford, H. R. (2017a) ‘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.
178. Wisniewski, P. J., Knijnenburg, B. P. and Lipford, H. R. (2017b) ‘Making privacy personal: Profiling social network users to inform privacy education and nudging’, *International Journal of Human Computer Studies*. Elsevier, 98(September 2016), pp. 95–108. doi: 10.1016/j.ijhcs.2016.09.006.
179. Wolak, J. *et al.* (2010) ‘Online “predators” and their victims: Myths, realities, and implications for prevention and treatment.’, *Psychology of Violence*. Educational Publishing Foundation, 1(S), pp. 13–35. doi: 10.1037/2152-0828.1.S.13.
180. Yang, Z. *et al.* (2016) ‘VoteTrust: Leveraging friend invitation graph to defend against social network sybils’, *IEEE Transactions on Dependable and Secure Computing*, 13(4), pp. 488–501. doi: 10.1109/TDSC.2015.2410792.

181. Yaprakli, T. S. and Unalan, M. (2017) ‘CONSUMER PRIVACY IN THE ERA OF BIG DATA: A SURVEY OF SMARTPHONE USERS’ CONCERNS’, *PressAcademia Procedia*, 4(1), pp. 1–10.
182. Yee, K.-P. (2002) ‘User interaction design for secure systems’, in *International Conference on Information and Communications Security*. Springer, pp. 278–290.
183. Zang, J. *et al.* (2015) ‘Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps’, *Technology Science*. Available at: <http://techscience.org/a/2015103001/>.
184. zdnet (2018) *Google shuts down Google+ after API bug exposed details for over 500,000 users | ZDNet*. Available at: <https://www.zdnet.com/article/google-shuts-down-google-after-api-bug-exposed-details-for-over-500000-users/> (Accessed: 25 September 2019).
185. Zhang, Nan and Zhao, W. (2007) ‘Privacy-Preserving Data Mining’, *Security, Privacy and Trust in Modern Data Management*, pp. 151–166. doi: 10.1145/335191.335438.
186. Zhao, B. (2015) ‘IDENTIFYING PRIVATE DATA LEAKAGE THREATS IN WEB BROWSERS A’, (August).
187. Zhou, A. T., Blustein, J. and Zincir-Heywood, N. (2004) ‘Improving intrusion detection systems through heuristic evaluation’, in *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No. 04CH37513)*. IEEE, pp. 1641–1644.
188. Zhou, Y. *et al.* (2011) ‘Taming Information-Stealing Smartphone Applications (on Android)’, *4th International Conference on Trust and Trustworthy Computing*, (2011), pp. 93–107.
189. ZoneAlarm (2015) *ZoneAlarm - Facebook Privacy Tips*. Available at: <http://www.zonealarm.com/security//en/support/privacy-tips.htm> (Accessed: 15

March 2017).

Appendix A – Ethical Approval (User Survey)

PLYMOUTH UNIVERSITY FACULTY OF SCIENCE AND ENGINEERING

Research Ethics Committee

APPLICATION FOR ETHICAL APPROVAL OF RESEARCH
INVOLVING

HUMAN PARTICIPANTS

All applicants should read the guidelines which are available via the following link:

<https://staff.plymouth.ac.uk/scienv/humanethics/intranet.htm>

This is a WORD document. Please complete in WORD and extend space where necessary. Clearly name any supporting documents and reference in the application.

Postgraduate and Staff must submit a signed copy to SciEngHumanEthics@plymouth.ac.uk

Undergraduate students should contact their School Representative of the Science and Engineering Research Ethics Committee or dissertation advisor prior to completing this form to confirm the process within their School.

School of Computing, Electronics and Mathematics undergraduate students – please submit to SciEngHumanEthics@plymouth.ac.uk with your project supervisor copied in.

1. TYPE OF PROJECT

1.1 What is the type of project?

Applicant	Type	Put X in 1 only
STAFF	Specific project	
	Thematic programme of research	

	Practical / Laboratory Class	
POSTGRADUATE STUDENTS	Taught Masters Project	
	M.Phil / PhD by research	X
UNDERGRADUATE STUDENTS	Student research project	
	Practical / Laboratory class where you are acting as the experimenter	

2. APPLICATION

2.1 TITLE of Research project
A Holistic Framework for Enhancing Privacy Awareness
2.2 Name, telephone number, e-mail address and position of applicant for this project (plus full details of Project Supervisor for postgraduate and undergraduate students)
1- Aziz Alshehri (Research student) aziz.alshehri@plymouth.ac.uk , +447453267227 2- Prof Nathan Clarke (Director of Studies) n.clarke@plymouth.ac.uk , +441752586226 3- Fudong Li (Supervisor) fudong.li@port.ac.uk
2.3 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives (no more than 200 words)
The purpose of this research is to develop novel approaches in order to help inform and manage privacy preference. The survey will look to identify what the current privacy preferences are, and how would like to manage privacy preferences. This will require conducting an online survey in order to collect data which includes the Demographic information, Privacy Concerns and Privacy Management. In addition, different initial interfaces will be evaluated by the participants.
2.4 Physical site(s) where research will be carried out
N/A – to be conducted online.
2.5 Does your research involve external institutions (e.g. other university, hospital, prison etc. see guidelines)
No
2.5a If yes, please give details:

3.3 Does your research involve deception?
No
Please explain why the following conditions apply to your research:
3.3a Deception is completely unavoidable if the purpose of the research is to be met
3.3b The research objective has strong scientific merit
3.3c Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures
3.3d Describe how you will debrief your participants

4. BREAKDOWN OF PARTICIPANTS

4.1 Summary of participants

Type of participant	Number of participants
<i>Non-vulnerable Adults</i>	Approximately 400
<i>Minors (< 16 years)</i>	
<i>Minors (16-18 years)</i>	

<i>Vulnerable Participants</i> <i>(other than by virtue of being a minor)</i>	
TOTAL	400

4.2 How were the sample sizes determined?
Based upon prior studies of this nature and in order to get a statistically significant sample for analysis.
4.3 How will subjects be recruited?
The participants will be recruited via e-mail and social network websites.
4.4 Will subjects be financially rewarded? If yes, please give details.
No

5. NON-VULNERABLE ADULTS

5.1 Are some or all of the participants non-vulnerable adults?
Yes
5.2 Inclusion / exclusion criteria
Participants who are 18 years old and above will be invited to answer the survey.
5.3 How will participants give informed consent?
Participants will be asked in the first page of the survey whether they agree to participate in the survey and give permission for their answers to be used in this study or not
5.4 Consent form(s) attached
Yes
If no, why not?

5.5 Information sheet(s) attached
Delete as applicable: No
If no, why not?
Relevant details are explained in the first page of the survey
5.6 How will participants be made aware of their right to withdraw at any time?
It will be stated in the first page along with the consent form that participants have the right to withdraw at any stage up to the completion of the survey.
5.7 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
Participants will be informed that their data will be anonymous, securely stored and only used for the purpose stated in the briefing

6. VULNERABLE PARTICIPANTS (Minors <18 years, and Vulnerable Adults)

6.1 Are some or all of the participants:
(Delete as applicable)
Under the age of 16? No
Between the ages of 16 and 18? No
Vulnerable adults? (See guidelines) No
If no to all, please proceed to section 7. If yes, please continue and consult guidelines for working with minors and/or vulnerable groups.

6.2 Describe the vulnerability (for minors give age ranges)
6.3 Inclusion / exclusion criteria
6.4 How will minors and vulnerable adults give informed consent?

Please delete as applicable and explain below (See guidelines)		
For minors < 16 only:	Opt-in	Opt-out
If opt-out, why?		
6.5a Consent form(s) for minor/vulnerable adult attached		
Delete as applicable:	No	Yes
If no, why not?		
6.5b Information sheet(s) for minor/vulnerable adult attached		
Delete as applicable:	No	Yes
If no, why not?		
6.6a Consent form(s) for parent / legal guardian attached		
Delete as applicable:	No	Yes
If no, why not?		
6.6b Information sheet(s) for parent / legal guardian attached		
Delete as applicable:	No	Yes
If no, why not?		
6.7 How will parent/legal guardians, minors and/or vulnerable adults be made aware of their right to withdraw at any time?		
6.8 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?		

Investigators working with children and vulnerable adults legally require clearance from the Disclosure and Barring Service (DBS)		
6.9 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> DBS clearance? Please include photocopies.		
Delete as applicable:	No	Yes
If no, explain		

7. PHYSICAL RISK ASSESSMENT

7.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)? (See guidelines)		
Delete as applicable:	No (Go to Q8)	Yes
7.1a If yes, please describe		
7.1b What measures have been taken to minimise risk?		
7.1c How will you handle participants who appear to have been harmed?		

8. PSYCHOLOGICAL RISK ASSESSMENT

8.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)		
Delete as applicable:	No (Go to Q9)	Yes

8.1a If yes, please describe
8.1b What measures have been taken to minimise risk?
8.1c How will you handle participants who appear to have been harmed?

9. RESEARCH OVER THE INTERNET

9.1 Will research be carried out over the internet?
Delete as applicable: Yes
9.1a If yes, please explain protocol in detail, including how informed consent will be obtained, procedures concerning the right to withdraw and how confidentiality will be maintained. Give details of how you will guard against abuse by participants or others (see guidelines)
Qualtrics.com will be used as online survey tool to distribute the survey. The user will be asked to read a consent form on the first page and agree to begin the survey. The user has the right to withdraw at any time by closing the page. No personal information will be collected at any stage and the response will be stored anonymously. All of the results will be used only for this research.
9.1b Have you included the online version of questionnaire and information/consent form? This should be as close to the format which will be viewed on line as possible.
Yes

10. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS

10.1 Do any of the experimenters have a conflict of interest? (See guidelines)
Delete as applicable: No (Go to Q11)

<i>If yes, please describe</i>		
<i>10.1a Are there any third parties involved? (See guidelines)</i>		
Delete as applicable:	No	Yes
<i>If yes, please describe</i>		
<i>10.1b Do any of the third parties have a conflict of interest?</i>		
Delete as applicable:	No	Yes
<i>If yes, please describe</i>		

11. ADDITIONAL INFORMATION

<i>11.1 Give details of any professional bodies whose ethical policies apply to this research</i>
<i>11.2 Please give any additional information that you wish to be considered in this application</i>


12. ETHICAL PROTOCOL & DECLARATION

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the University of Plymouth and by any professional body specified in section 10 above.

This research conforms to the University's Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent.

Sign below where appropriate:

STAFF / RESEARCH POSTGRADUATES

	Print Name	Signature	Date
Principal Investigator: 20/07/2018	Aziz Alshehri		
Other researchers: _____	Prof Nathan Clarke	_____	
_____	Dr Fudong Li	_____	

Staff and Research Postgraduates should email the completed and signed copy of this form to scienghumanethics@plymouth.ac.uk

UNDERGRADUATE STUDENTS

Date	Print Name	Signature
Student: _____	_____	_____
Supervisor / Advisor: _____	_____	_____
_____	_____	_____
_____	_____	_____

Appendix B: User survey consent

I am a PhD candidate at the University of Plymouth in the School of Computing, Electronics and Mathematics and I am conducting this survey as part of my PhD research.

With the huge popularity of the mobile apps, the risk of privacy breaches has increased and attacks on digital computing have continued to be a problem. Therefore, this research seeks to develop novel approaches in order to help inform and manage privacy preferences. The survey will look to identify what the current privacy preferences are, and how would like to manage privacy preferences. The survey will also investigate your thoughts regarding the design of interfaces.

As a participant, you are invited to participate in this questionnaire which will require approximately 10-15 minutes to complete. At all stages of the study, your responses will remain anonymous since no personal information or IP addresses will be collected. You have the right to withdraw at any stage up until the completion of the survey. However, after completing the survey, due to the anonymized nature of the survey, your participation cannot be removed.

Your participation is voluntary, you must be over 18 years and owned a smartphone e.g(Android, iOS and Windows phone).

If you wish to take part, you will need to agree for participating by clicking the button below.

For information regarding the study, please contact: Aziz Alshehri
aziz.alshehri@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

Aziz Alshehri
PhD Researcher
The University of Plymouth
aziz.alshehri@plymouth.ac.uk

I consent, begin the study

I do not consent, I do not wish to participate

Start the survey

Appendix C: User survey

Section 1: Demographic Information

What is your gender?

Male

Female

What is your age?

18 - 24

25 - 34

35 - 44

45 - 54

55 - 64

65 or older

What is the highest level of school you have completed or the highest degree you have received?

Less than high school qualifications

High school qualifications

College certificate

Bachelor degree

Postgraduate degree

Occupation status

Student

Employed full time

Employed part time

Unemployed

Retired

General Questions about Privacy (please notice: all the questions are related to your privacy apps on your smartphone)

Please select the response representing the most appropriate answer for you. Please indicate to the best of your ability:

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1. In general, I am concerned about my privacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. When the app asks me personal information, I think twice before providing it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. It bothers me when an app requires unnecessary permissions that seemed irrelevant to its core function	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. I am concerned when any app shares my personal information to a third party	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



How would you rate your knowledge about the privacy of individual apps?

Read each statement carefully and indicate your **level of knowledge** about the privacy of apps : (all the statements are related to your privacy apps on your mobile)

	Extremely knowledgeable	Moderately knowledgeable	Somewhat knowledgeable	Slightly knowledgeable	Not knowledgeable
1- Understanding what permissions apps are seeking before installing.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- How to change privacy settings for the apps	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Understanding privacy policy for the apps	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Distinguish between necessary permissions for the app and unnecessary app permissions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Different types of applications capture and process a variety of different types of privacy-related information, the following questions will ask you how concerned you are about such privacy-related information being shared by different categories apps

Game and Entertainment Category



For example: Angry Birds, Candy Crush Saga, Roblox and Clash Of Clans.

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Exact location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Identity(Date of birth and name)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Health Category

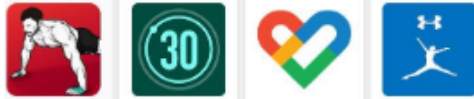


NHS App

Suppose you installed an application which is developed by a trusted medical provider eg NHS, could you please indicate your concern about letting the application send the following information.

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Health information (Heart rate, Blood pressure, ECG and skin temperature)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Exact Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Identity(Date of birth and name)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Phone (phone call and messaging)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Fitness Category:



For example: Home Workout, 30 Day Fitness Challenge, Google Fit: Health and Activity and MyFitnessPal

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Motion activity(steps, calories burned and sleep duration)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Identity(Date of birth and name)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Exact Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Social Networking



For example: Facebook, Tweeter, WhatsApp, and Instagram

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Identity(Date of birth and name)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Exact Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Calendar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7- Phone (phone call and messaging)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Shopping Category



For example: Amazon, eBay, and Argos

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Identity(Date of birth and name)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Exact Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Phone (phone call and messaging)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Productivity Category

Apps that make a specific process or task more organized or efficient.



For example: Gmail, google calendar and google drive

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Identity(Date of birth and name)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Calendar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Phone (phone call and messaging)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Lifestyle Category

Apps relating to a general-interest subject matter or service.



For example: Diary with Lock and MyDuty

	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Exact location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Calendar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6- Phone (phone call and messaging)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Navigation Category



For example Google map and near me app.

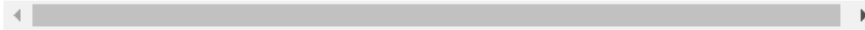
	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not concerned at all
1- Multimedia information (Photos and videos)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2- Contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3- Exact location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Approximate location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- Phone (phone call and messaging)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Privacy Control and management:

Read each statement carefully and indicate your **level of agreement** with the following statements about the privacy control and management.

Would it be useful to have the following settings:

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1. Ability to control information across different apps	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. Display multi-level privacy control e.g.(No access, Low access, and Full Access)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Ability to restrict the time period of sharing your data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4- Ability to change the privacy notification settings for different apps	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5- More help and support for the novice user to help him to understand the system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



In this section, we present a proposed system that seeks to better inform you about privacy-related information on your mobile in order to control this information and to raise your awareness about privacy threats.

The proposed system consists of three primary components:

- 1-Notification,
- 2- Help and support
- 3-Privacy Control
- 4- Historical view

Each component has two proposed designs, please see each interface and answer the questions.

Notification Interface:

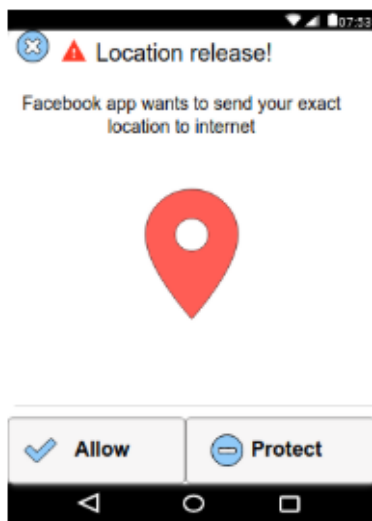
Two interfaces will be displayed to you. The first interface is full-screen notification whilst the second interface is short screen notification.

Notification Interface:

Two interfaces will be displayed to you. The first interface is full-screen notification whilst the second interface is short screen notification.

The First Proposed Design: Full-Screen Notification

The system displays the full-screen notification when there are ongoing privacy risks.

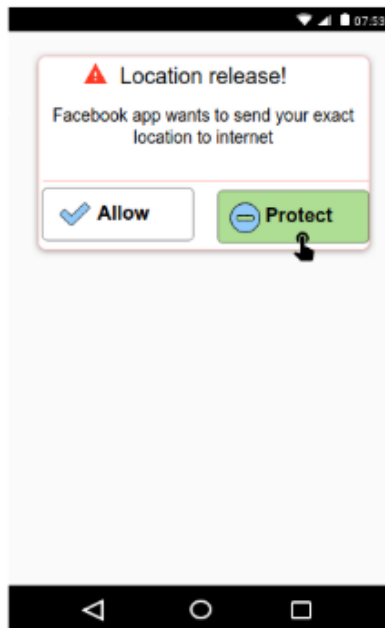


Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very good	Good	Fair	Poor
A. The icons used in the notification	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The understanding of the interface	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The ease of use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The Second Proposed Design

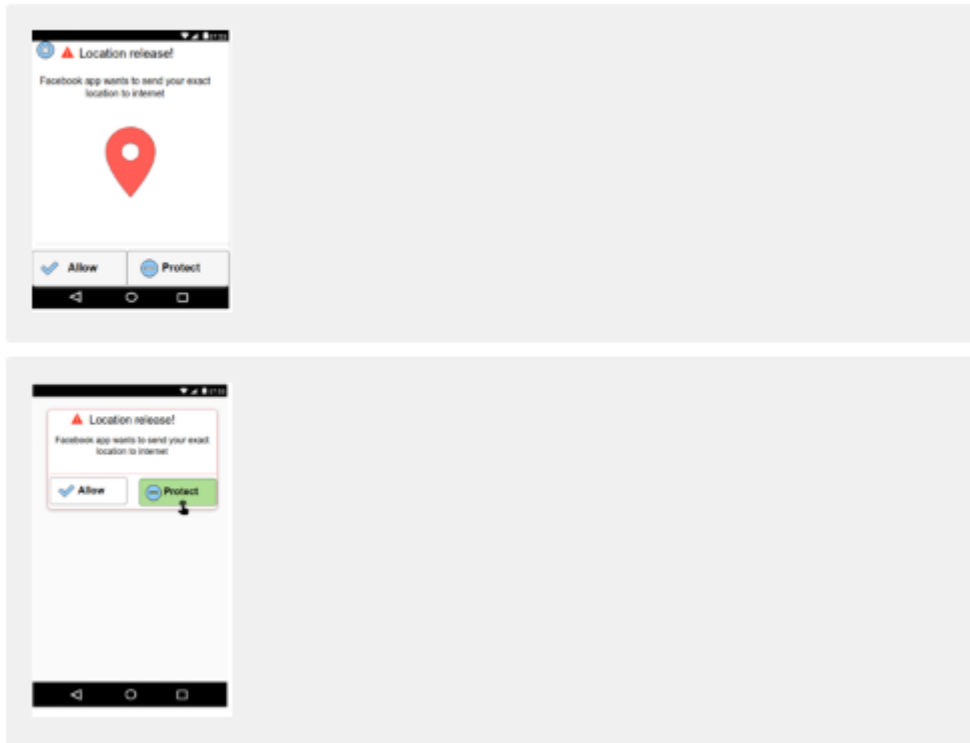
Short Notification



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very Good	Good	Fair	Poor
A. The icons used in the notification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The understanding of the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The ease of use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

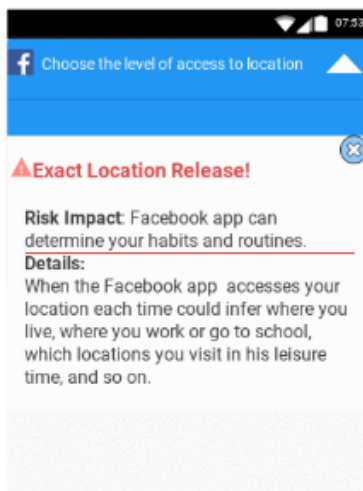
Which interface would you prefer?
Just select by clicking on the interface you prefer



Help and support:

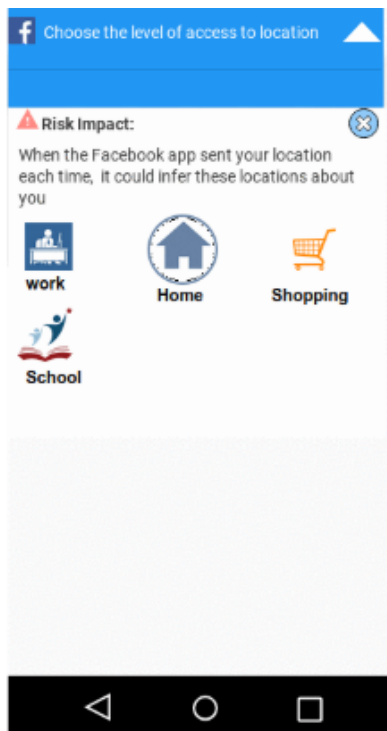
The First Proposed Design:

From this interface, you can understand the risk impact when the app sends your personal information each time. For example, when the Facebook app wants to send your location each time, it could infer the location of your work, home, and school.



Please, read each statement carefully and rate each point based on the above interface:

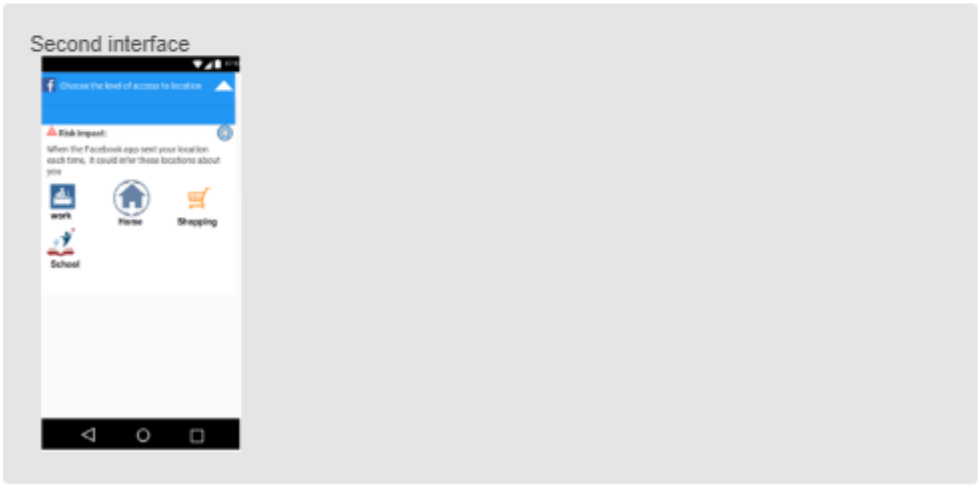
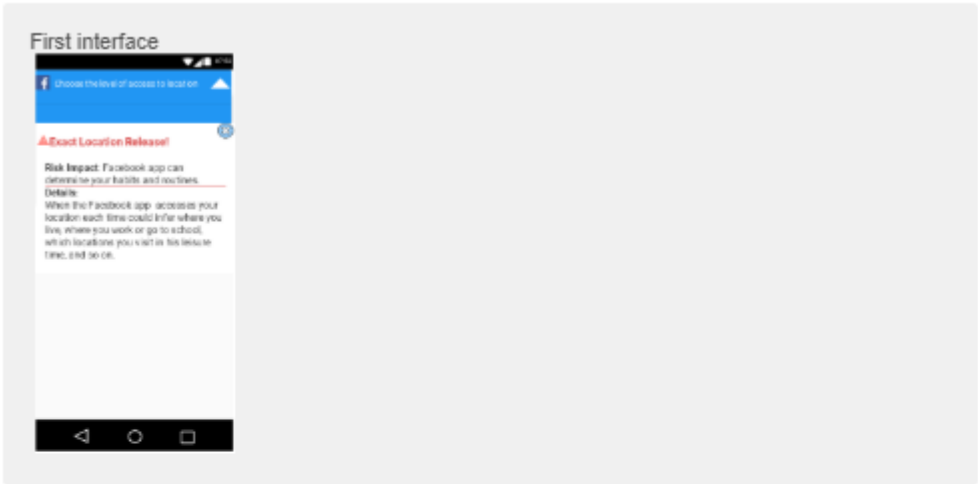
	Excellent	Very Good	Good	Fair	Poor
A. The icons used in the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The understanding of the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The text font used in the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very Good	Good	Fair	Poor
A. The icons used in the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The understanding of risk impact from pictures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The text font used in the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Which interface would you prefer?



Privacy control:

The First Proposed Design:

From the interface, you can select a certain level of privacy to help you control your personal information easily.

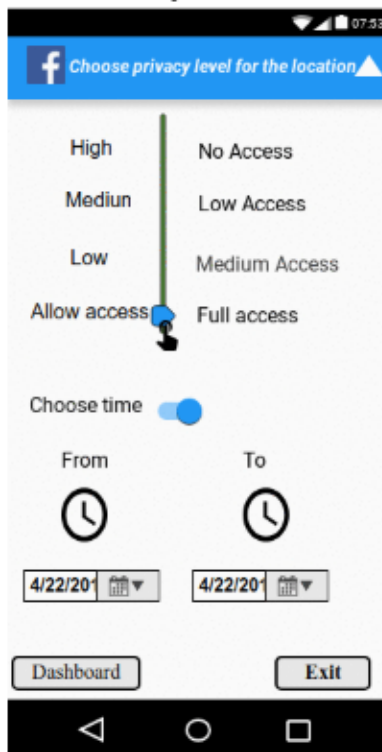


Please, read each statement carefully and rate each point based on the above interface:

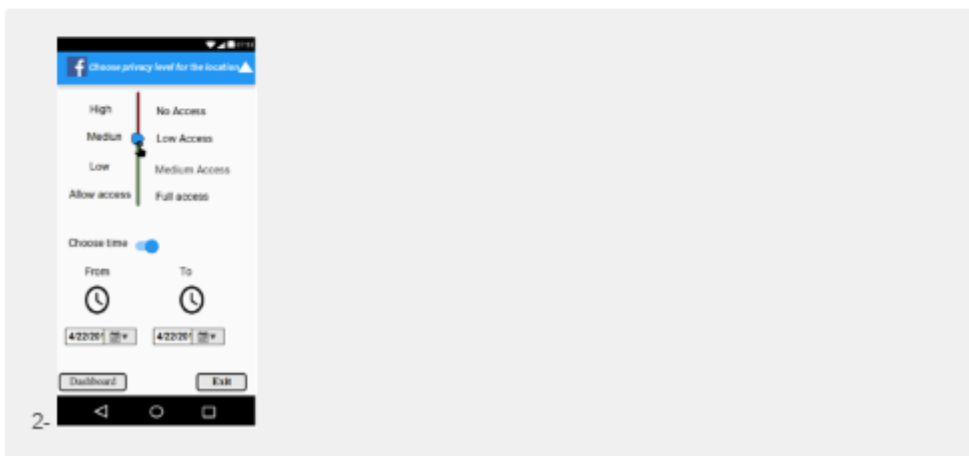
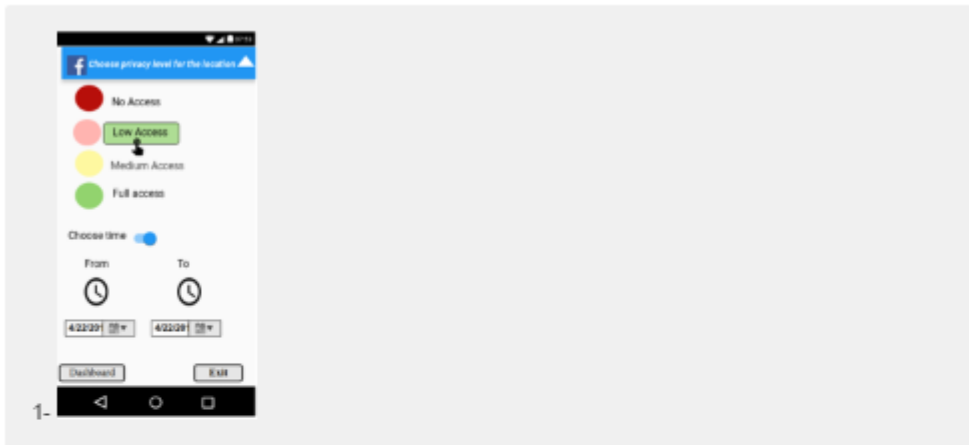
	Excellent	Very Good	Good	Fair	Poor
A. The understanding of the interface	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The icons used in the interface	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The ease of use	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The Second Proposed Design:

From the interface, you can select a certain level of privacy to help you control your personal information easily.



Which interface would you prefer?



Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very Good	Good	Fair	Poor
A. The understanding of the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The icons used in the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The ease of use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

History Interface:

The First Proposed Design:

Please note the interface is not for the novice user but for the intermediate and advanced user. It presents data history to help you to know who has accessed data, when and at which degree of granularity.

Filter by date: Last week

Actions History			
▼ Data Type	▼ App	▼ Actions	▼ Time
All	Facebook	No access	2 hours ago
All	eBay	Full access	23 hours
Exact Location	Puzzle game	No access	1 day ago
Email	Ebay	Full access	2 days ago

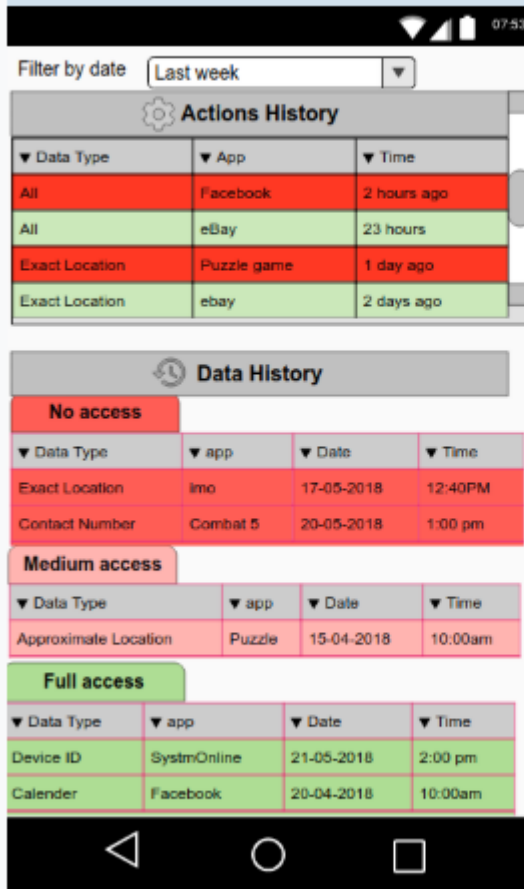
Data History				
▼ Data Type	▼ app	▼ Date	▼ Time	▼ Actions
Exact Location	imo	17-05-2018	12:40PM	No access
Approximate Location	Puzzle	17-05-2018	10:00am	Medium access
Contact Number	Combat 5	20-05-2018	1:00 pm	No access
Device ID	SystemOnline	21-05-2018	2:00 pm	Full access
Calendar	Facebook	22-05-2018	10:00am	Full access
Approximate Location	Budget app	23-05-2018	5:00 pm	No access

Please, read each statement carefully and rate each point based on the above interface:

	Excellent	Very Good	Good	Fair	Poor
A. The colour used in the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. The understanding of the interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. The text font and size	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The Second Proposed Design:

it presents data history with color to help you to know the level of the privacy risk.



Which interface would you prefer?

First interface



Second Interface



Appendix D – Consent Form for the System Evaluation

UNIVERSITY OF PLYMOUTH

FACULTY OF SCIENCE AND ENGINEERING

Human Ethics Committee Sample Consent Form

CONSENT TO PARTICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Aziz Alshehri

Title of Research

A Holistic Framework for Enhancing Privacy Awareness

Brief statement of purpose of work

You are invited to participate in focus group discussion conducted by Aziz Alshehri as part of his project concerning the enhance privacy awareness in the mobile and how to manage privacy app in the mobile. The main purpose of the research is to design a system that considers users' preferences and needs.

This interview will be recorded as a reference used.

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations)

Under these circumstances, I agree to participate in the research.

Name:

Signature:

Date:

Appendix E –Ethical Approval for the System Evaluation (End-Users)

PLYMOUTH UNIVERSITY FACULTY OF SCIENCE AND ENGINEERING

Research Ethics & Integrity Committee

APPLICATION FOR ETHICAL APPROVAL OF RESEARCH
INVOLVING

HUMAN PARTICIPANTS

All applicants should read the guidelines which are available via the following link:

<https://liveplymouthac.sharepoint.com/sites/u40/Human%20Ethics/Forms/AllItems.aspx>

This is a WORD document. Please complete in WORD and extend space where necessary. Clearly name any supporting documents and reference in the application.

Postgraduate and Staff must submit a signed copy to SciEngHumanEthics@plymouth.ac.uk

Undergraduate students should contact their School Representative of the Science and Engineering Research Ethics & Integrity Committee or dissertation advisor prior to completing this form to confirm the process within their School.

School of Computing, Electronics and Mathematics undergraduate students – please submit to SciEngHumanEthics@plymouth.ac.uk with your project supervisor copied in.

4. TYPE OF PROJECT

1.1 What is the type of project?

Applicant	Type	Put X in 1 only
-----------	------	-----------------

STAFF	Specific project	
	Thematic programme of research	
	Practical / Laboratory Class	
POSTGRADUATE STUDENTS	Taught Masters Project	
	M.Phil / PhD by research	X
UNDERGRADUATE STUDENTS	Student research project	
	Practical / Laboratory class where you are acting as the experimenter	

5. APPLICATION

2.1 TITLE of Research project
A Holistic Framework for Enhancing Privacy Awareness
2.2 Name, telephone number, e-mail address and position of applicant for this project (plus full details of Project Supervisor for postgraduate and undergraduate students)
1- Aziz Alshehri (Research student) aziz.alshehri@plymouth.ac.uk , +447453267227 2- Prof Nathan Clarke (Director of Studies) n.clarke@plymouth.ac.uk , +441752586226 3- Fudong Li (Supervisor) fudong.li@port.ac.uk
2.3 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives (no more than 200 words)
The purpose of this research is to develop a novel approach to inform and manage privacy preferences in mobile applications. This study aims to present the approach to end user for evaluation. This would be achieved through a focus-group based activity lasting for an hour approximately
2.4 Physical site(s) where research will be carried out
The University of Plymouth
2.5 Does your research involve external institutions (e.g. other university, hospital, prison etc. see guidelines)
Delete as applicable: No
2.5a If yes, please give details:
2.5b If yes, you must provide letter(s) from institutional heads permitting you to carry out research on their clients, and where applicable, on their sites(s). Are they included?

Delete as applicable: No <i>If no go to section 4</i>
Please explain why the following conditions apply to your research:
3.3a Deception is completely unavoidable if the purpose of the research is to be met
3.3b The research objective has strong scientific merit
3.3c Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures
3.3d Describe how you will debrief your participants

4. BREAKDOWN OF PARTICIPANTS

4.1 Summary of participants

Type of participant	Number of participants
<i>Non-vulnerable Adults</i>	7
<i>Minors (< 16 years)</i>	
<i>Minors (16-18 years)</i>	
<i>Vulnerable Participants (other than by virtue of being a minor)</i>	

TOTAL	7

4.2 How were the sample sizes determined?
Based upon prior studies of this nature.
4.3 How will subjects be recruited?
The participants will be recruited via e-mail or face-to-face invitation
4.4 Will subjects be financially rewarded? If yes, please give details.
No

5. NON-VULNERABLE ADULTS

5.1 Are some or all of the participants non-vulnerable adults?
Delete as applicable: Yes
5.2 Inclusion / exclusion criteria
Participants who are 18 years old and above will be invited to participate in the focus group session.
5.3 How will participants give informed consent?
It will be stated in the briefing along with the consent form that participants have the right to withdraw at any stage up to the completion of the session. Should any participant wish to withdraw from the session, their discussion will be securely removed from the records and completely destroyed.
5.4 Consent form(s) attached
Delete as applicable: Yes
If no, why not?
5.5 Information sheet(s) attached
Delete as applicable: Yes
If no, why not?

5.6 How will participants be made aware of their right to withdraw at any time?
It will be stated in the briefing along with the consent form that participants have the right to withdraw at any stage up to the completion of the session. Should any participant to withdraw from the session, their discussion will be securely removed from the records and completely destroyed.
5.7 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
No names will be used in the written report. Interviewees' information will be kept confidential and be used by the researcher only.

6. VULNERABLE PARTICIPANTS (Minors <18 years, and Vulnerable Adults)

6.1 Are some or all of the participants:	
	(Delete as applicable)
Under the age of 16?	No
Between the ages of 16 and 18?	No
Vulnerable adults? (See guidelines)	No
If no to all, please proceed to section 7. If yes, please continue and consult guidelines for working with minors and/or vulnerable groups.	

6.2 Describe the vulnerability (for minors give age ranges)
6.3 Inclusion / exclusion criteria
6.4 How will minors and vulnerable adults give informed consent?
Please delete as applicable and explain below (See guidelines)
For minors < 16 only: Opt-in Opt-out
If opt-out, why?
6.5a Consent form(s) for minor/vulnerable adult attached

Delete as applicable:	No	Yes
<i>If no, why not?</i>		
<i>6.5b Information sheet(s) for minor/vulnerable adult attached</i>		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
<i>6.6a Consent form(s) for parent / legal guardian attached</i>		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
<i>6.6b Information sheet(s) for parent / legal guardian attached</i>		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
<i>6.7 How will parent/legal guardians, minors and/or vulnerable adults be made aware of their right to withdraw at any time?</i>		
<i>6.8 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?</i>		
Participants will be informed that they will be anonymous and the session will be recorded, securely stored within the Centre for Security, Communications and Network Research (CSCAN). They will also be only used for the purpose stated in the briefing.		
<i>Investigators working with children and vulnerable adults legally require clearance from the Disclosure and Barring Service (DBS)</i>		

6.9 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> DBS clearance? Please include photocopies.	
Delete as applicable:	No
<i>If no, explain</i>	

7. PHYSICAL RISK ASSESSMENT

7.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)? (See guidelines)	
Delete as applicable:	No (Go to Q8)
7.1a If yes, please describe	
7.1b What measures have been taken to minimise risk?	
7.1c How will you handle participants who appear to have been harmed?	

8. PSYCHOLOGICAL RISK ASSESSMENT

8.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)	
Delete as applicable:	No (Go to Q9)
8.1a If yes, please describe	
8.1b What measures have been taken to minimise risk?	

8.1c How will you handle participants who appear to have been harmed?

9. RESEARCH OVER THE INTERNET

9.1 Will research be carried out over the internet?
Delete as applicable: No (Go to Q10)
9.1a If yes, please explain protocol in detail, including how informed consent will be obtained, procedures concerning the right to withdraw and how confidentiality will be maintained. Give details of how you will guard against abuse by participants or others (see guidelines)
9.1b Have you included the online version of questionnaire and information/consent form? This should be as close to the format which will be viewed on line as possible.
Delete as applicable: No Yes

10. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS

10.1 Do any of the experimenters have a conflict of interest? (See guidelines)
No
Delete as applicable: No
If yes, please describe
10.1a Are there any third parties involved? (See guidelines)
Delete as applicable: No (Go to Q11)
If yes, please describe

10.1b Do any of the third parties have a conflict of interest?		
Delete as applicable:	No	Yes
<i>If yes, please describe</i>		

11. ADDITIONAL INFORMATION

11.1 Give details of any professional bodies whose ethical policies apply to this research
11.2 Please give any additional information that you wish to be considered in this application


12. ETHICAL PROTOCOL & DECLARATION

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the University of Plymouth and by any professional body specified in section 10 above.

This research conforms to the University's Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent.

Sign below where appropriate:

STAFF / RESEARCH POSTGRADUATES

	Print Name	Signature	Date
Principal Investigator:	Aziz Alshehri		_____

Other researchers: Prof Nathan Clark _____

 Dr Fudong Li _____

Staff and Research Postgraduates should email the completed and signed copy of this form to scienghumanethics@plymouth.ac.uk

UNDERGRADUATE STUDENTS

Date	Print Name	Signature
Student: _____	_____	_____
Supervisor / Advisor: _____	_____	_____
_____	_____	_____
_____	_____	_____

Undergraduate students should pass on the completed and signed copy of this form to their School Representative of the Science and Engineering Research Ethics Committee.

	Signature	Date
School Representative on Science and Engineering Faculty Research Ethics & Integrity Committee _____	_____	_____

Faculty of Science and Engineering Research Ethics & Integrity Committee List of School Representatives

School of Geography, Earth and Environmental Sciences Dr Sanzidur Rahman

School of Biological and Marine Sciences Dr Gillian Glegg (Chair)

Dr Victor Kuri

School of Biomedical Sciences Dr David J Price

School of Engineering

Dr Asiya Khan

Mr Chris Pollard

School of Computing, Electronics & Mathematics

Dr Mark Dixon

Dr Yinghui Wei

Doctoral College, Deputy Director

Prof Steven Furnell

External Representative

Dr Satish B K

Lay Member

Rev. David V. Evans

Committee Secretary: Mr Steven Neal

Email: steven.neal@plymouth.ac.uk

Tel: 01752 584877

Appendix F – End Users Questions for the System Evaluation

1. To what extent do you think the proposed system enhances your awareness about privacy-related information?
2. To what extent do you feel the main dashboard allow you to quickly control and track the privacy-related information?
3. To what extent do you think that the structure of the proposed design is convenient and usable?
4. To what extent do you feel the layout and the format are convenient and usable?
5. To what extent are you satisfied with the used colours?
6. To what extent do you think the proposed system are easy to use?
7. To what extent do you feel that it is easy to understand components and features of each interface of the system?
8. What do you feel are the particular strengths & weaknesses of the developed system?
9. Would you like to suggest anything you feel is missing from the system?
10. Is there anything else you would like to add?

Appendix G– Experts Questions for the System Evaluation

Experts Questions

1. What are your thoughts of the identified research problem?
2. To what extent do you think the proposed system is feasible /achievable /practical?
3. What do you think about the three-level approach? That is; novice, intermediate and advanced? More/less levels?
4. What do you feel are the key barriers or issues in using this approach?
5. To what extent do think the utilisation of the following functions in the proposed approach could enhance the user’s awareness about privacy-related information?
 - a. Historical privacy
 - b. Controlling privacy
 - c. Notification
6. What do you think about monitoring users privacy-related information?
7. The privacy-related information is prioritised based on users privacy preferences. To what extent do you think this prioritisation could make the system more flexible and usable?
8. To what extent do you feel the main dashboard allow you to quickly control and track the use of privacy-related information?
9. To what extent do you think that the structure of the proposed design, the layout and the format are convenient and usable?
10. To what extent are you satisfied with the used colours?
11. To what extent do you think the proposed system is easy to use?
12. To what extent do you feel that it is easy to understand components and features of each interface of the system?
13. What do you feel are the particular strengths & weaknesses of the developed system?
14. Would you like to suggest anything you feel is missing from the system?
15. Is there anything else you would like to add?

Appendix H –Ethical Approval for the System Evaluation (Experts)

PLYMOUTH UNIVERSITY FACULTY OF SCIENCE AND ENGINEERING

Research Ethics & Integrity Committee

APPLICATION FOR ETHICAL APPROVAL OF RESEARCH
INVOLVING

HUMAN PARTICIPANTS

All applicants should read the guidelines which are available via the following link:

<https://liveplymouthac.sharepoint.com/sites/u40/Human%20Ethics/Forms/AllItems.aspx>

This is a WORD document. Please complete in WORD and extend space where necessary. Clearly name any supporting documents and reference in the application.

Postgraduate and Staff must submit a signed copy to SciEngHumanEthics@plymouth.ac.uk

Undergraduate students should contact their School Representative of the Science and Engineering Research Ethics & Integrity Committee or dissertation advisor prior to completing this form to confirm the process within their School.

School of Computing, Electronics and Mathematics undergraduate students – please submit to SciEngHumanEthics@plymouth.ac.uk with your project supervisor copied in.

7. TYPE OF PROJECT

1.1 What is the type of project?

Applicant	Type	Put X in 1 only
STAFF	Specific project	

	Thematic programme of research	
	Practical / Laboratory Class	
POSTGRADUATE STUDENTS	Taught Masters Project	
	M.Phil / PhD by research	X
UNDERGRADUATE STUDENTS	Student research project	
	Practical / Laboratory class where you are acting as the experimenter	

8. APPLICATION

2.1 TITLE of Research project
A Holistic Framework for Enhancing Privacy Awareness
2.2 Name, telephone number, e-mail address and position of applicant for this project (plus full details of Project Supervisor for postgraduate and undergraduate students)
4- Aziz Alshehri (Research student) aziz.alshehri@plymouth.ac.uk , +447453267227 5- Prof Nathan Clarke (Director of Studies) n.clarke@plymouth.ac.uk , +441752586226 6- Fudong Li (Supervisor) fudong.li@port.ac.uk
2.3 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives (no more than 200 words)
The purpose of this research is to develop a novel approach to inform and manage privacy preferences in mobile applications. This study aims to present the approach to experts in the field for evaluation. This would be achieved through a focus-group based activity lasting for an hour approximately.
2.4 Physical site(s) where research will be carried out
The student is attending and presenting a paper at HAISA 2019 conference and will use the opportunity to host a focus-group whilst present (with the assistance of the supervision team in making appropriate contact with delegates).
2.5 Does your research involve external institutions (e.g. other university, hospital, prison etc. see guidelines)
Delete as applicable: No
2.5a If yes, please give details:
2.5b If yes, you must provide letter(s) from institutional heads permitting you to carry out research on their clients, and where applicable, on their sites(s). Are they included?

3.2 How long will the procedures take? Give details
One 1 hour approximately
3.3 Does your research involve deception?
Delete as applicable: No <i>If no go to section 4</i>
Please explain why the following conditions apply to your research:
3.3a Deception is completely unavoidable if the purpose of the research is to be met
3.3b The research objective has strong scientific merit
3.3c Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures
3.3d Describe how you will debrief your participants

4. BREAKDOWN OF PARTICIPANTS

4.1 Summary of participants

Type of participant	Number of participants
<i>Non-vulnerable Adults</i>	6
<i>Minors (< 16 years)</i>	
<i>Minors (16-18 years)</i>	

<i>Vulnerable Participants (other than by virtue of being a minor)</i>	
TOTAL	6

4.2 How were the sample sizes determined?
Based upon prior studies of this nature.
4.3 How will subjects be recruited?
The participants will be recruited via e-mail or face-to-face invitation
4.4 Will subjects be financially rewarded? If yes, please give details.
No

5. NON-VULNERABLE ADULTS

5.1 Are some or all of the participants non-vulnerable adults?
Delete as applicable: Yes
5.2 Inclusion / exclusion criteria
The participants will be recruited via e-mail and face-to-face invitation.
5.3 How will participants give informed consent?
The participants will be given the consent to sign at the beginning of the session, should they wish to carry out the study. It will be also ensured that they understand their right to withdraw from the session at any time up until the end of their participation.
5.4 Consent form(s) attached
Delete as applicable: Yes
If no, why not?

5.5 Information sheet(s) attached	
Delete as applicable:	Yes
If no, why not?	
5.6 How will participants be made aware of their right to withdraw at any time?	
It will be stated in the briefing along with the consent form that participants have the right to withdraw at any stage up to the completion of the session. Should any participant wish to withdraw from the session, their discussion will be securely removed from the records and completely destroyed.	
5.7 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?	
No names will be used in the written report. Interviewees' information will be kept confidential and be used by the researcher only.	

6. VULNERABLE PARTICIPANTS (Minors <18 years, and Vulnerable Adults)

6.1 Are some or all of the participants:	
	(Delete as applicable)
Under the age of 16?	No
Between the ages of 16 and 18?	No
Vulnerable adults? (See guidelines)	No
If no to all, please proceed to section 7. If yes, please continue and consult guidelines for working with minors and/or vulnerable groups.	

6.2 Describe the vulnerability (for minors give age ranges)	
6.3 Inclusion / exclusion criteria	
6.4 How will minors and vulnerable adults give informed consent?	
Please delete as applicable and explain below (See guidelines)	
For minors < 16 only:	Opt-in Opt-out
If opt-out, why?	

6.5a Consent form(s) for minor/vulnerable adult attached		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
6.5b Information sheet(s) for minor/vulnerable adult attached		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
6.6a Consent form(s) for parent / legal guardian attached		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
6.6b Information sheet(s) for parent / legal guardian attached		
Delete as applicable:	No	Yes
<i>If no, why not?</i>		
6.7 How will parent/legal guardians, minors and/or vulnerable adults be made aware of their right to withdraw at any time?		
6.8 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?		
<p>Experts will be informed that they will be anonymous and the session will be recorded, securely stored within the Centre for Security, Communications and Network Research (CSCAN). They will also be only used for the purpose stated in the briefing.</p>		

Investigators working with children and vulnerable adults legally require clearance from the Disclosure and Barring Service (DBS)
6.9 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> DBS clearance? Please include photocopies.
Delete as applicable: No
If no, explain

7. PHYSICAL RISK ASSESSMENT

7.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)? (See guidelines)
No Delete as applicable: No (Go to Q8)
7.1a If yes, please describe
7.1b What measures have been taken to minimise risk?
7.1c How will you handle participants who appear to have been harmed?

8. PSYCHOLOGICAL RISK ASSESSMENT

8.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)
No Delete as applicable: No (Go to Q9)
8.1a If yes, please describe

8.1b What measures have been taken to minimise risk?
8.1c How will you handle participants who appear to have been harmed?

9. RESEARCH OVER THE INTERNET

9.1 Will research be carried out over the internet?
No Delete as applicable: No (Go to Q10)
9.1a If yes, please explain protocol in detail, including how informed consent will be obtained, procedures concerning the right to withdraw and how confidentiality will be maintained. Give details of how you will guard against abuse by participants or others (see guidelines)
9.1b Have you included the online version of questionnaire and information/consent form? This should be as close to the format which will be viewed on line as possible.
Delete as applicable: No Yes

10. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS

10.1 Do any of the experimenters have a conflict of interest? (See guidelines)
No Delete as applicable: No
If yes, please describe
10.1a Are there any third parties involved? (See guidelines)

Delete as applicable:	No	(Go to Q11)
<i>If yes, please describe</i>		
<i>10.1b Do any of the third parties have a conflict of interest?</i>		
Delete as applicable:	No	Yes
<i>If yes, please describe</i>		

11. ADDITIONAL INFORMATION

<i>11.1 Give details of any professional bodies whose ethical policies apply to this research</i>
<i>11.2 Please give any additional information that you wish to be considered in this application</i>

12. ETHICAL PROTOCOL & DECLARATION

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the University of Plymouth and by any professional body specified in section 10 above.

This research conforms to the University's Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent.

Sign below where appropriate:

STAFF / RESEARCH POSTGRADUATES

Print Name

Signature

Date

Principal Investigator:

Aziz Alshehri



Other researchers:

Prof Nathan Clark

Dr Fudong Li

Staff and Research Postgraduates should email the completed and signed copy of this form to scienghumanethics@plymouth.ac.uk

UNDERGRADUATE STUDENTS

Date

Print Name

Signature

Student:

Supervisor / Advisor:

Undergraduate students should pass on the completed and signed copy of this form to their School Representative of the Science and Engineering Research Ethics Committee.

Signature

Date

School Representative on Science and
Engineering Faculty Research Ethics & Integrity
Committee

**Faculty of Science and Engineering Research Ethics & Integrity Committee List
of School Representatives**

School of Geography, Earth and Environmental Sciences Dr Sanzidur Rahman

School of Biological and Marine Sciences Dr Gillian Glegg (Chair)

Dr Victor Kuri

School of Biomedical Sciences Dr David J Price

School of Engineering

Dr Asiya Khan

Mr Chris Pollard

School of Computing, Electronics & Mathematics

Dr Mark Dixon

Dr Yinghui Wei

Doctoral College, Deputy Director

Prof Steven Furnell

External Representative

Dr Satish B K

Lay Member

Rev. David V. Evans

Committee Secretary: Mr Steven Neal

Email: steven.neal@plymouth.ac.uk

Tel: 01752 584877

