Chapter 1: Introduction

1.1 Background to the study

The widespread use of online social networks has developed over the last decade, but recently this deployment has grown in a dramatic and rapid way. Hu and Ma (2010) named some of these applications that have grown and become popular around the world in the last few years, such as Facebook, Twitter, and MySpace. Social media has been developed to create highly interactive platforms through which individuals and different communities share, exchange files and discuss with others (Tang, Gu & Whinston 2012). The driving force behind the spread was to provide opportunities to build reputations and to offer simple chances to obtain money and careers, as discussed in Tang, Gu, and Whinston (2012).

While the main goal of using these applications is to link the user with as many friends as possible, this also has the effect of amplifying the processes of exchanging and sharing files between them. This can be clearly seen by following daily posting activity, whether sharing pictures, interests or information about themselves (Shin 2010). For example, Facebook showed that the daily average number of active users was about 699 million in June 2013 (Facebook 2013a).

The sheer number of users and dramatic increase in the rate of these applications yearly make it inevitable that more personal information details are posted in profiles (Fuchs 2010). Including more personal information details in profiles can help friends or families to search for and identify them (Fuchs 2010). Furthermore, this personal information may include some identifying information such as name, address, mobile number and more (Thelwall 2009). This will require users who use real identity information to trust in others who start new relationships with them (Valenzuela, Park & Kee 2009). However, information privacy issues and risks may prevent some users from disseminating such sensitive information (Dwyer, Hiltz & Passerini 2007).

Privacy has become a big challenge facing developers of internet applications. It is difficult to guarantee 100% privacy of personal information, especially on online social networking sites. Personal information can be misused by anonymous individuals, friends or others, and no single feature is responsible for protecting such data. Many features must work smoothly together to increase the degree of privacy protection, for example, user awareness, new privacy applications, and the use of simple tools to control privacy settings, decrease risks, etc..

Protection of information in the internet plays a significant role in today's networked society. Technology has created and impacted online interactions between users who are aware of security applications and implications. This leads to the need to develop better security mechanisms for different types of communication technologies, especially for mobile communications.

Beside the developments in the security of social networking sites, the current trend of these sites is also to develop mobile apps that provide the user with a real-time access to their accounts such as Facebook, Twitter and Instagram. Mobile social networking allows individuals to share interests and exchange files through their mobile phones or tablets. Several social networking sites use applications (Peng, Sun & Tsai 2014) that have enabled mobile users, companies and most developers of online applications to compete to acquire the largest number of users. Several features were provided by mobile applications that have contributed to the rapid spread of mobile social networking. Social networking sites were able to create or discover native communities by using the features and accessibility of internet mobile devices such as mobility, ease of use and access to online information (Peng, Sun & Tsai 2014). Lenhart et al. (2010) conducted a study that showed an increase in the number of people who use mobile devices to browse the internet, and this number will continue to grow over time. This encourages developers to design new technologies and applications for mobile networks to meet consumer demands. Although bringing practical and sustainable privacy to users by providing them with effective protection and privacy solutions is a key issue, privacy is still not being considered as an essential part of fundamental design for security mechanisms.

It is essential to improve privacy with these security mechanisms. In 1990, Cavoukian developed the term 'privacy by design', which shows the need to address privacy concerns and interests at the onset of technology development. The author defined this concept as a philosophy to enhance the design by adding and including privacy concerns as embedded requirements in such areas as technology design, business practices and physical design (Cavoukian 2009). This concept has become the main basis for technology designs. Moreover, different companies, such as Facebook, Google, Twitter and others that produce social network applications are competing to increase the level of privacy in their applications to meet the needs of their users. Thus, applying the concept of ‘privacy by design’ as a standard for designing social networking applications means that users will be given more authority to decide which types of information they want to share and with whom.

Knowledge of internet skills is not enough for solving privacy and trust concerns because there are different perspectives and opinions from internet users about privacy concerns (Dinev & Hart 2006). There are several research documents that have discussed different issues about privacy concerns and trust, but few studies have suggested or designed systems for protecting users' personal information details. In relation to online social networks, some studies have suggested systems or ways to protect location details for internet mobile devices, but no one has discussed or suggested techniques to facilitate the ability of internet mobile devices to control personal information privacy. Therefore, the main objective of this study is to suggest a framework to solve this issue:

With the high participation in each online social networking site, personal information distribution processes and the widespread use of mobile internet devices for browsing, what means can mobile technology designers provide to the user to help control effectively the process of distribution of his or her personal information, taking into account the increasing number of social networking sites and the use of internet mobile devices for browsing?

1.2 Recent research

Interest in information privacy issues has grown (Wu, Zhu & Ding 2014). Researchers in different sciences are still discussing and developing ideas and rules to increase the level of protection for personal information, both theoretically and practically. This issue in not limited to computer science and technology, but law, business, education and other fields are also able to contribute to development. Recently, different studies have focused on multiple dimensions of protecting online social networking sites

(SNS), including trust, privacy concerns, SNS privacy risks and others. This section will present some recent research on these topics.

According to Wang and Cui (2008), privacy is a state or condition of limited access to a person. Privacy regulations can be defined as a set of rules or policies set by users to achieve a certain level of privacy. In terms of location privacy, privacy regulations restrict access to information on a user’s location. Each privacy rule or policy can include some restrictions (Sadeh & Hong 2009). Although there is no policy mandating online personal information privacy, some types of privacy solutions do exist (Passant et al. 2009). The ability to control privacy options is essential to increasing users’ confidence in their social network providers. Users must have the ability to control their privacy options at any time. These privacy options allow users to accept or reject the dissemination of their information to others (Samavi & Consens 2010).

Gross and Acquisti (2009) found the probability of predicting the Social Security number (SSN) for participants in online social networks users is higher than for non-participants. This may create risks when brokers or other sites spread personal information (e.g. date of birth) related to SSN. Furthermore, a number of studies have discussed concerns about privacy and trust. Shin (2010) focused on privacy, trust and security concerns for SNS and found the predictability of SSN is an unexpected concern, and it cannot be removed by deleting the SSN from public profiles or concealing the first five digits. Moreover, trusting online transactions is another privacy concern facing individuals using electronic commerce (Rosenblum 2007; Xu 2009). On the other hand, some researchers have focused on the distribution process of personal information details within SNS. When users trust the service provider of the online social network site, they become more likely to share their personal information through it (Shin 2010). Fogel and Nehmad (2009) found that internet users who have experience about security are more likely to trust the current security mechanism in SNS as long as the company provides a clear contract about the procedure of protecting their privacy. For example, they found that Facebook users trust the privacy contract more than MySpace, and most of them are university students. In addition, online social network users who have experience are more concerned about privacy (Lo 2010), but users with less knowledge are more likely to distribute their information because they trust the online social network site and think only friends can see this information (DiMicco et al. 2008).

Similarly, protecting the privacy of personal information is one of the biggest challenges facing website developers, especially social network providers. Several researchers have discussed the issue of privacy. For example, a study conducted by Casarosa (2010) found that minors are interested in new technologies and the internet, and can be contacted online by strangers asking to form a friendship. Therefore, Bae and Kim (2010) suggested that, in order to achieve a high level of privacy, the user should be given the authority to control the privacy settings when he or she receives or requests a service related to his or her personal information. Dötzer (2006, p. 4) stated that 'once privacy is lost, it is very hard to re-establish that state of personal rights'. The nature and complexity of the internet create threats to web privacy (Bouguettaya & Eltoweissy 2003).

Different techniques have been designed to increase personal information privacy protection. Williams et al. (2009) listed some steps for online social network users to stay safe, and Fang et al. (2010) designed a privacy recommendation wizard based on user inputs to help users classify their friend list into sub-lists. In addition, configuring privacy settings so that only friends can see your posts is not enough to defend yourself from other threats such as those arising through applications and advertisements (Stutzman & Kramer-Duffield 2010). Lipford, Besmer and Watson (2008) found that showing an example of privacy settings will enable users to understand their privacy settings better and help them determine who can see their personal information.

The research reviewed briefly here showed a number of case studies among users who share personal information details with social networks sites. In short, they found that users either were aware of privacy concerns and ready to distribute the information or unaware of these concerns, which leads them into privacy risks. This issue will be the main key component of the proposed framework in this thesis.

1.3 Statement of the problem

With the widespread use of mobile internet services and the increasing number of SNS, different applications have been designed to attract more users. Some of them have gained fame around the world, such as Facebook and Twitter. These sites help users to connect more easily in social ways, but they also increase the distribution of personal information. Most of these applications or sites are open platforms for registration, which means they are free for everyone to sign in. Each application or site requires at least the entry of some personal information for identification purposes. Furthermore, in order to use the application or the site, it is not necessary for users to have extensive knowledge about their use. The apparent simplicity may affect privacy because some users are unaware of what will happen if this information is misused.

However, it has become clear that online social network use is not limited to adults; high numbers of children in some countries also have accounts. Livingstone, Ólafsson and Staksrud (2011) found that about 77% of European children 13–16 years of age have profiles in at least one social network. A survey by Ai Ho, Maiga and Aimeuer (2009), which included 200 participants, revealed some problems with privacy issues. The most pressing issue was that sites did not clearly inform users of the risk that divulged personal information could be misused. The very fact of the large number of SNS users may encourage an increase in the number of malicious attacks (Feldman et al. 2012), thus affecting privacy in various ways. While the use of online SNS offers many benefits such as finding friends and jobs, the placement of ever-more personal information on such sites can create privacy risks for some users; this is particularly the case if a user is not sophisticated (Alsalibi et al. 2013). Therefore, Yuan et al. (2010) emphasised that protection of user privacy is a responsibility of the service provider.

While communication has become easier with online social networks applications, protecting users' privacy has become more complicated, especially with the differences between these applications. Each online social network provider uses different settings and protection methods. Furthermore, trust is an important element for protecting privacy, and it can be divided into two parts: trusting the provider and trusting the user (Hughes 2009). Boyd (2011) found that people with internet knowledge are more aware of SNS privacy issues because of their general knowledge of security settings and privacy risks. A study done by Pavlou and Fygenson (2006) found that users with knowledge about using both SNS and online transactions have more privacy concerns, but their concern about online transactions is higher than about SNS. Moreover, there are simple ways to increase the knowledge of users about privacy concerns. Lipford, Besmer and Watson (2008) found that showing an example of privacy settings will enable users to understand their privacy settings better and help them find out who can see their personal information. In addition, Bae and Kim (2010) suggested that, in order to achieve a high level of privacy, the user should be given the authority to control the privacy settings when he or she receives or requests a service related to his or her personal information. As another practical solution, Bekara, Kheira and Laurent (2010) developed a framework for enhancing privacy in identity management by introducing a middle-ware privacy level to give users more control of personal information. In addition, Kolter and Pernul (2009) emphasised that design simplicity, especially of the interface and tools of a privacy program, allowed users to protect personal information optimally.

In recent years, internet mobile devices, which is a small internet communications unit designed to provide entertainment, information and location-based services and other web services for the user (Guan et al. 2011), have begun gradually pulling the rug from under desktop computers. The popularity of browsing the internet using mobile devices has increased. For this reason, different internet mobile companies such as Apple and Samsung have produced several types of mobile web device. The strong competition between them leads to the development of new devices with added hardware and software techniques that make using mobile devices for internet services easier and more effective. According to Lane et al. (2010), certain factors have affected the increased sales of internet mobile devices around the world. Some of those reasons include: the low cost of embedded sensors and chips; the availability of different kinds of internet mobile applications, and offering applications that support sharing real-time activities with others, such as Facebook or Twitter applications. Beach et al. (2010) pointed out that the online social networks such as Facebook, Twitter and MySpace will impact support for mobile web devices. A study done by Bullas (2012) showed that in August 2010, 30 million users of the Instagram application shared about 150 million photos. Various companies have developed mobile-specific internet browsers including versions of Opera, Internet Explorer, and Safari (Lewis & Moscovitz 2009). Today, most mobile internet browsers support various programming languages including HTML and JavaScript, but they do not browse as effectively as laptops or PCs do because the screens and keyboards are smaller (Guan 2011).

However, several studies have discussed different types of privacy risks related to personal information details in online social networks, and a few studies have discussed the usability of using internet mobile devices for browsing. None of them, however, have suggested a system or an idea to facilitate the use of internet mobile devices to control personal information privacy settings in order to protect the user from distributing his or her personal information in different online social network accounts. Thus, the current study focuses on designing a framework to keep pace with the development in internet mobile devices in order to enhance privacy awareness for users so that they can control their personal information privacy settings in internet mobile systems.

1.4 Goal and research objectives

Based on the previously outlined research problem, the main research question for this thesis will be:

How can online personal information privacy issues be addressed satisfactorily in an integrated services scenario, involving different types of mobile devices, in order that the confidence of users in the effective protection of their personal details from misuse can be increased?

Therefore, the main research objectives for this study that underpin the main research question are to:

- ❖ Propose a privacy-aware framework that supports most internet mobile devices to increase the confidence of mobile device users.
- ❖ Develop a privacy model that is suitable for controlling personal information settings through internet mobile devices.

- Develop a privacy management model to support users' ability to manage their personal information.
- Design a prototype system to verify the framework and models.

1.5 Methodology

This section provides an explanation and details of the methodology used in this study. The methodology applied includes four successive stages. The first part of the study was a hardcopy survey to collect data about the use of social networking sites and some privacy concerns. The purpose of it is to identify which sensitive personal information is important to the user and measure the awareness of controlling the privacy settings. The second part was designing a program to assist the user in creating a privacy policy for their social networking accounts. This program deals with developing a tool that assists the user in creating an access control policy for their personal information based on a wizard system. The third part was an online survey and implementation to test the designed program. This stage was tested by asking participants to evaluate the suggested access control policy for their information, and measuring privacy concerns and the visibility status for each item of their personal information. The last part was designing the whole framework system that links several internet sites with one access control site to allow each site to access some information based on a created privacy policy. Both the validity and reliability of the survey were examined and adopted by using SSPS v19.0.

1.6 Outline of thesis

This thesis consists of six chapters. The first chapter (Introduction) gives background and information about the research. It briefly describes the problem and recent research findings. While it is a brief description of the whole problem, it introduces the main problem, the research question and the objectives. In addition, it outlines the methodology used in this study to examine the research question.

Chapter 2 (Literature review) is a critical and an evaluative summary of other academic studies and research obtained from published articles, journals or books to discuss the research problem. It shows different findings and reviews about online social networks and privacy. This chapter focuses on SNS, online personal information details, privacy in SNS, internet mobile devices, access control models and the ways of selecting privacy settings for controlling personal information distribution.

Chapter 3 (Conceptual model) describes the theoretical concepts that support the framework for this study. It reviews privacy frameworks for protecting personal information in online systems from other studies. Furthermore, it presents all the hypotheses identified in the form of a practical model based on the literature review and the theoretical support.

Chapter 4 (Research design and methodology) provides the research with an outline of the methodology used and the study justifications. It explains the methods and the sample that have been used. It also describes the suggested mechanism for building the proposed framework and its stages.

Chapter 5 (Results and analysis) is a summary of the study findings. It presents the analysis and results for each hypothesis in this study. It summarises the analytical process and presents the key findings for these stages: the research survey; the suggested wizard system; the implementation results; and the final design for the system.

Chapter 6 (Findings, recommendation and conclusion) describes the study’s findings and provides conclusions. In this section, different aspects will be outlined and discussed, such as: the awareness of online social network privacy issues; the flexibility of controlling privacy settings; defining sensitive personal information; controlling privacy settings through internet mobile devices, and other aspects. The study results revealed that the widespread use of internet mobile devices and the number of online social network accounts require developing a new privacy system compatible with these developments. Therefore, this section presents the findings about implementing the proposed access control system and provides recommendations for future research, in addition to the limitations of this study.

1.7 Conclusion

This chapter outlined several parts of the study. It outlined the background of the research question by highlighting the rapid widespread use of online social networks and internet mobile devices. It showed how users are aware of privacy concerns in SNS and identifies the parties that should be involved in protecting personal information privacy, especially with the browsing of the internet through mobile devices. Following on the relative newness of SNS and surfing the web via internet mobile devices, this research demonstrates prospects for the development of social networking systems to fit the evolution in internet mobile device technologies. The research problem and the methodology for this study are presented, as are the contents of the study, starting with a review of the literature. Chapter 2 will discuss various research findings and recent solutions related to this study.

Chapter 2: Literature Review

2.1 Introduction

This chapter provides a review of the existing literature related to this study. It starts with a description of the concept of Web 2.0 and online social networks. After that, it provides background to all concepts used in this study, including online social networks, personal information privacy, privacy risks, centrality of personal information, security of personal information in centralised online systems, and advantages and disadvantages of centralised personal information details in online systems. It also provides a review of another existing body of literature related to mobile web systems, usability of internet mobile devices and applications, access control systems, and the control of privacy settings through internet mobile devices. In addition, the literature review shows the need to develop different privacy frameworks that support the rapidly expanding use of internet mobile devices and social network accounts. The focus of this chapter is to understand the true risks that surround personal information details and the distribution of these details on different websites. It will also show therights to control their personal information privacy and to decide which information can be shared with each site that users have.

The privacy of personal information became an issue after the rapid expansion of social networking sites, following which different mobile applications were developed to synchronise the development of internet mobile technology. As such, the main objective of this study is to review the current online privacy systems and develop a proposed access control system that provides an easy way to control the processes of sharing personal information details, even with internet enabled mobile devices.

2.2 Social networking sites

2.2.1 Web 2.0 and social networking sites

Web 1.0 refers to an early stage of the World Wide Web, which was entirely made up of web pages connected by hyperlinks (Wu and Ackland 2014). Brake (2014) showed that content designers were limited in Web 1.0 as it was a set of static websites that were not providing interactive content. The current phase of communication services began with the creation of Web 2.0. This term was coined in 1999 and is now one of the famous internet vocabularies popular with internet applications worldwide, such as Wiki, RSS (Rich Site Summary) and SNSs (Lai & Turban 2008). O'Reilly (2007) defined Web 2.0 as the second generation of internet sites and services that transformed the traditional internet environment from normal websites to interactive sites that allowed participation between users, such as social networks, RSS and other tools. When all Web 2.0 characteristics worked together, they shaped a new class of technology that challenged IT research in this field (Beck 2008). This does not mean that Web 2.0 is an independent environment, but that there are some similarities and also improvements on Web 1.0 standards that have provided more social orientation. Li and Turbaned (2008) argued that the improvements in the interactivity with users by generating content on the sites have made Web 2.0 more advanced than Web 1.0. In addition, Madden and Fox (2006) mentioned that the interactivity services in Web 2.0 have contributed to users being able to create online content rather than restricting them to specific services and applications. A sense of participation via writing what the user wants is the main objective of Web 2.0 (Andersen 2007, p. 14). Recently, many sites and internet applications have begun using Web 2.0 standards for different purposes, whether commercial, educational, administrative or others, such as YouTube, Facebook and Twitter. All these sites support Web 2.0 activities such as blogging, posting and sharing media with others, which have helped users add new online social behaviours beside their real-world behaviour (Bonhard & Sasse 2006). While Web 2.0 has several tools, the focus of this study is on social networks.

Recently, online social networks have become an essential part of everyday life. Millions of users share their activities with others to satisfy their social needs, whether for sociability or other reasons (Ganley & Lampe 2009). The concept of online social networks was defined by The Pew Internet & American Life Project as a private space for online users to create their own profiles and share the content with others (Lenhart 2009, p. 1). Different social network companies promote their services by using promotional blurb to popularise their applications. For example, the Yahoo Group used this phrase: "With millions of groups at your fingertips, it's easy to find the group that's best for you—whatever your interest." (Yahoo 2013), and Facebook used

“Facebook helps you connect and share with the people in your life.” (Facebook 2013b).

While the Web 2.0 environment offered a place for exchanging information in a voluntary way, information technology experts warned of the risks of this technology, especially from people with malicious intent (Mansfield-Devine 2008). The author attributed this risk to the enormous size of the information database which results from information-sharing processes. Such information can be personal details, photos or other types of information. Gross and Acquisti (2005) pointed out that most common information items are included in users’ profiles, such as home address, educational history, likes and dislikes, interests, mothers’ name, and some specifications regarding partners, and they warned that some of these details may be used as answers for security questions related to accounts or banking operations. From time to time, the media announced some issues relating to security and privacy issues in social networks. For example, In May 2008, Bedo (one social network website) announced that their system had a malfunction that negatively impacted users’ profile view, and about 40 million users switched to other users’ accounts (Eriksen 2008). Despite the existence of these risks, this has not prevented millions of users from sharing their information and pictures through social networks.

The sharing of personal information content should be built on the basis of trust between users and service providers. It is difficult for users to predict all the risks surrounding the issue of dissemination of information in social networks, and if there is leaking information, this may cause users damage in the case of misuse by other people (Milne & Culnan 2004). Obviously, Web 2.0 has changed the current life style, particularly with social networks, and has become another form of social communication. Consequently, several questions present themselves, but one of the most important deals with how to harness Web 2.0 as a technology to provide more trust for social network users and to reduce the risks resulting from the spread of personal information in social networks.

2.2.2 Background of social networking sites

Online social networking sites have become an influential element in changing life behaviours. Chiu, Cheung and Lee (2008) described it as the top web application, and

Bruns, Highfield and Burgess (2013) showed how social networking sites such as Facebook and Twitter have changed the political system in Egypt. They have become a medium of communication between people, and each user has his/her own list of followers who can see his/her profile (Dar & Shah 2013). Each social network site is defined as a web-based service that allows users to create new personal profiles in the server, whether public or private, to share the connection with others and allow them to view their personal information with a group of friends or public followers (Boyd & Ellison 2010). Most social networking sites have default privacy settings to contain the content of users' profiles. For example, Facebook has default privacy settings, and users have the ability to configure these settings based on their need (Hoy & Milne 2010; Staksrud & Lobe 2010). The reason social network providers have been encouraged to add privacy tools is because users' personal information is not only seen by friends, but various parties may also look at them, particularly potential employers, lawyers or medical specialists (Buote, Wood & Pratt 2009).

The differences in the features and services granted to users by social network providers have contributed to an increase in the number of users of their applications. Some of them have great popularity, such as Facebook and MySpace, which were registered as the largest two websites with the most registered users for 2010 and 2011 (Boyd 2011; Shin 2010). In June 2013, Facebook showed that the daily average number of active users was about 699 million (Facebook 2013a). A paper presented by Crane (2013) showed that in 2012 MySpace had over 100 million active users. However, in some websites, the application owners limited the use of social networks to a specific class of society, such as employees of an organisation (DiMicco et al. 2010). Therefore, social networking sites can be used and defined in different ways based on a variety of factors.

2.2.3 Defining social networking sites

In general, a social network can be defined as a set of active relationships between users, whether these relations are close or general (Brass, Butterfield & Skaggs 1998). Web 2.0 sites have the ability to allow users to interact and collaborate with each other in a virtual community, and these features are named by social networking sites as blogs, wikis, web applications, folksonomies and video sharing sites (Churcher, Downs & Tewksbury 2014). These relations can be between users, users and organisations, or other entities, for friendship, business, affiliation, information exchange or any other reason (Andrews, Preece & Turoff 2001; Andrews 2002). The social network providers are responsible for managing and maintaining the process of finding these relationships, and their acts emerge in managing the process of finding friends based on similarities in interests, religion, nationality, location and other information (Mislove et al. 2007). Furthermore, social networking sites are not limited to this aspect of services; there are other aspects that can be provided to support a wide range of interests and practices, such as emailing, blogging, sharing photos or videos and instant messaging (Ellison 2007).

According to Boyd and Ellison (2010), an online social network site is defined as a web-based service that allows a user to (1) create their profile and set it as a public or semi-public profile, (2) connect them with other profiles and indicate them in a list, and (3) view and allow the connections made by others within the website. The identification names for the services may change from one service provider to another, but the main concepts are the same. In this study, a social network site means any site that allows a user to create their own profile and set policies on that profile to control the connection process for reaching their profile.

2.2.4 User awareness in social networking sites

Users awareness is one of the non-hardware security measures that the company can implement to make users aware of all the potential risks that can occur (Mishra et al. 2014). It is a formal process for educating the users about the company policies, users' rights and the implemented security procedures (Lebek et al. 2014). User awareness is an important step for online social network society. It can provide more security experience to deal with the exchange of personal information. Awareness of social networking sites is a part of internet knowledge and experiences (DiMicco et al. 2008). While reading about internet services will enhance users' awareness level, visiting different websites and using various services will increase this knowledge and add an experimental experience besides theoretical knowledge (Chang and Chen 2008). In addition, expansion in the area of internet knowledge plays a significant role in evaluating SNS (Binder, Howes & Sutcliffe 2009). Furthermore, repeated usage will enhance users' knowledge of a service and make them more experienced (Dahlen 2002; Gefen, Karahanna & Straub 2003). As an example, Luan et al. (2005) found that people with internet knowledge are more willing to try the online shopping experiment. Hence knowledge, whether practical or theoretical, is a helpful way to educate people about online risks and give them experience protecting their personal information privacy, particularly in online social networks.

2.3 Privacy

Technology, and information and communication technology (ICT) in particular, plays a significant role in today’s networked society. Technology has affected online interactions between users who are aware of its security applications and implications (Grieco et al. 2014). This leads to the need to develop better security mechanisms for different types of communication technologies, particularly for mobile communications. Although a key issue is bringing practical and sustainable privacy to users by providing them with effective protection and privacy solutions, privacy is still not being considered as an essential part of the fundamental design of security mechanisms (Hoepman 2014). Today, it is generally believed to be essential to add privacy to these security mechanisms. In 1990, Cavoukian developed the term “privacy by design”, which showed the need to address privacy concerns and interests at the onset of technology development. The author defined this concept as a philosophy to enhance the design by adding and including privacy concerns as embedded requirements into such areas as technology design, business practices and physical design (Cavoukian 2009). Recently, the "privacy by design" issue has become the main basis for technology designs. Moreover, different companies, such as Facebook, Google, Twitter and others that produce social network applications, are competing to increase the level of privacy in their applications to meet the needs of their users. Thus, applying the concept of "privacy by design" as a standard for designing the social networking application means that users will be given more authority to decide which types of information they want to share and with whom (Hoepman 2014).

2.3.1 Definition of privacy

According to Wang and Cui (2008), privacy is a state or condition of limited access to a person. Different definitions of privacy protection exist, and each has some relevance to mobility. Bünnig and Cap (2009) described privacy as protecting personal information from being misused by malicious entities and only allowing certain authorised entities to gain access to that personal information, making it visible to them. Additionally, Taheri, Hartung and Hogrefe (2010) claimed that, in relation to mobility and location privacy, privacy is especially important in a wide range of applications that seek to protect location information for users and hide some details from others. Ni et al. (2010) defined privacy as a set of privacy policies that force the system to protect private information.

Consequently, no single definition of privacy or privacy protection encompasses all aspects of this term. Each definition is suitable for a specific purpose, which means that the concept of privacy is diverse. In regard to the area of mobile networks, privacy can be categorised into the following types: information privacy, location privacy and physical privacy. Based on Bünnig et al. (2009), this study is concerned primarily with information privacy.

2.3.2 Social media privacy

In conjunction with the proliferation of various online sites, social media privacy issues have become a source of concern for many people. It has become the greatest internet issue facing internet application developers and users (Lo 2010). This issue has made people fearful about privacy and security problems, and some of them have become reluctant to use the Internet (Paine et al. 2007; Ramgovind, Eloff & Smith 2010). Thus, when discussing a privacy issue, one must take into account two important issues: the objective of the exchange of information and the extent of the expectation to remain private (Hodge 2006). The same author stated that when a user sets their privacy settings for their profile, they will expect that all the hidden items should be private.

Most internet sites provide all users, whether new or current, with privacy statements or terms about protecting their personal information privacy. This can be seen clearly in online social networking sites. For example, Facebook and MySpace provide users with clear information about the process of maintaining shared information. Based on the privacy statements in Facebook (2013) and MySpace (2013), the statements do not include who can access the posted information, but they outline the items that can be shared with a third party. In addition, they inform users about their roles relating to posting personal information on their profiles and protect them by adjusting privacy settings. On the other hand, the difference between age groups may be an obstacle to understanding these rules, a challenge that internet sites face in enhancing the protection of internet privacy.

In 2011, it became clear that the use of online social networks is not limited to adults; high proportions of children in some countries also have accounts. Livingstone, Ólafsson and Staksrud (2011) found that about 77% of European children 13–16 years of age have profiles in at least one social network. The survey spanned 25 countries and, in each country, many users were within this age bracket. Also, 38% of children aged 9–12 years have social network accounts; this indicates that social network usage will become even more common in the future. The cited authors examined parental restrictions on the use of networks by children. About 32% of children are not supervised, and about 20% are supervised to some extent. About half of all parents did not restrict their children’s activities. The survey did not study whether restrictions were related to privacy concerns or whether other considerations were in play.

A survey done by Ai Ho, Maiga and Aimeuer (2009), which included 200 participants, revealed some problems with privacy issues. The most pressing issue was that sites did not clearly inform users of the risk that divulged personal information might be misused. In addition, few tools were available to protect personal information. Finally, users could not control what others might publish about them.

The cited authors classified personal information into five categories:

- identification: details identifying a user, such as a name, address or telephone number.

- demography: any personal information on appearance or characteristics such as age, gender, weight or political view.
- activity: user activities such as writing comments, adding friends, or changing one’s current status.
- social networking: relationships between the user and others on the network, such as friends.
- added content: pictures, videos and music.

The large number of social network users may stimulate an increase in the number of malicious attacks (Feldman et al. 2012), thus affecting privacy in various ways. For instance, application programming interfaces (APIs) may violate user privacy. Allowing such applications to run may allow third-party access to personal information; application developers can access user data. Thus, social network hosts should protect user data and supervise all APIs requesting access to such data (Felt and Evan 2008).

The use of online social networking offers many benefits. Friends and jobs may be found, interests and information shared and comments exchanged. However, the placement of ever more personal information on such sites can create privacy risks for some users; this is particularly the case if a user is not sophisticated (Alsalibi, Zakariah & Elmadhoun 2013). Yuan, Chen and Yu (2010) emphasised that protection of user privacy is a responsibility of the service provider.

Confirming the above, Chris Hughes, a co-founder of Facebook, mentioned that Facebook as a social network site offers several tools that have a set of privacy controls for protecting personal information privacy, but the user is directly responsible for the use of these tools to provide privacy for his/her personal information (Timm and Duven 2008).

2.3.3 Privacy concerns

Users’ uneasiness about having their submitted personal information on the Internet misused results in privacy concerns (Dinev et al. 2006). The significant amount of personal information about users existing on social networking sites make that concept widely used in terms of privacy, and the risks are unpredictable (Dwyer, Hiltz

& Widmeyer 2008). Indeed, the misuse of such information may generate an opportunity for some people to exploit individuals' information in different ways, such as identity theft, financial transaction and extortion (Son & Kim 2008). However, with the widespread use of online social networks, internet literacy plays a significant role in privacy concerns, and these concerns can be decreased with high levels of internet knowledge (Lo & Riemenschneider 2010). Furthermore, there are several factors that make information privacy variable from time to time based on the differences in laws, culture and technical development (Xu 2009). Therefore, the literature review in this subsection will focus on other research related to internet personal information privacy.

In 2009, the privacy systems of online social networks were not trustworthy when millions of people were on the system (Baden et al. 2009). Over 25% of children aged 9–16 years old set their profile pages to "public", allowing general viewing (Livingstone et al. 2011). Thus, various laws have been promulgated to protect children's personal information. In 1998, the US passed a federal Children's Online Privacy Protection law applicable to those 13 years of age or younger. The law states that no website may collect personal data from children unless parents so permit. However, the commercial pressures are strong; children are receptive to specific advertisements, and high school details (for example) would be of value to advertisers and college recruiters (Ding, Yuan & Ross, 2012). These authors also explained that although some websites such as Facebook and Google+ seek to comply with the law by preventing all children under 13 years of age from registering, some beat the system by giving false birthdates. However, websites such as Facebook do apply privacy policies relevant to minors. For example, children can receive messages only from their own friends or from people who give contact details such as an email address or a phone numbers, but adults can receive messages from anyone. These restrictions also apply (inter alia) to the posting of pictures and the addition of friends (Facebook, 2013). Baden et al. (2009) developed a technique termed Persona, which can be used to hide personal information by combining attribute-based encryption with a traditional public access key.

In recent times, most users have (somewhat) restricted access to their online social network profiles. In a study conducted by Madden (2012), about 58% of users (48%

of males and 67% of females) allowed their profiles to be seen only by friends. Males were found to restrict access to a limited extent, but females were more concerned about privacy profiles. Also, about 67% of females have deleted some people from their friends lists compared to about 58% of males. However, the ability to control privacy settings varies among networks. About 48% of participants found it difficult to change settings; the ease of changing improved with higher educational levels. Moreover, Livingstone et al. (2011) found that the website “Hyves” was rated highly by most users in terms of the availability and ease of use of privacy features. Privacy settings were easily changed and other users blocked.

Social network users can share different pieces of personal information with others; however, these details may still be misused by friends. Gross and Acquisti’s study (2005) of Facebook users’ privacy concerns found that 91% of users uploaded their pictures, 88 percent shared their date of birth, 40% showed their phone number and 51% wrote their current address. The earlier results of Gross and Acquisti's study will be compared with the results of this study in later chapters. Sharing personal information such as this can lead to the misuse of data, whether intentional or not. For example, some people share profile details such as their full name, gender and phone number with their friends. If the social network account of one of the user’s friends is hacked, the spammer or the hacker can misuse these details to blackmail the user (Rosenblum 2007). Another example is the misuse of data on relationship status. If user X is engaged to user Y, and user X hides his/her relationship status from his/her profile but user Y does not, then other users who are able to see his/her profile details can see the relationship status for user X through user Y’s profile (Gundecha, Barbier & Liu 2011).

Williams et al. (2009) found that older users are more careful about posting personal information details such as their date of birth, friend lists and school information on their social network accounts than younger users. Similarly, Zukowski and Brown (2007) found that older Internet users are more concerned about the privacy of personal information than younger users. Some younger users publish their own information without knowledge of the risks that may occur from the misuse of these data. The online environment may be dangerous for users, regardless of age, because of the possible leakage of personal information details. George (2006) cited the case of United States college athletes whose pictures, which they posted online, were misused by a website that publishes stories about scandals in sport. The author pointed out that the issue of privacy has not gone unnoticed by social network providers.

Gross and Acquisti (2005) conducted a study on a sample of 4,000 students from Carnegie Mellon University who use social network accounts. They found that a large proportion of students did not care about the privacy risks that might increase the chance of a third party misusing a student's personal information. Another study by the same authors claimed that more than 77 percent of the respondents did not read privacy policies (Acquisti & Gross 2006).

The ability to control privacy options is essential to increasing users' confidence in their social network providers. Since Internet users represent a range of different cultures and ages, privacy options should be clear, simple and easy to use. Users must have the ability to control their privacy options at any time. These privacy options allow users to accept or reject the dissemination of their information to others. For example, some users do not want to publish sensitive information such as health or medical information (Samavi & Consens 2010). These users are aware that people with less than honourable intentions can harm adults or children by misusing their personal information. For instance, Casarosa (2010) found that minors are interested in new technologies such as the internet and can be contacted by strangers online asking to form a friendship. When a website publishes the personal information of a minor without giving the child's parents (or the child's guardian) the authority to select privacy options, potential predators can use some of the minor's personal information, such as a mobile phone number, to engage in sexual contact (Casarosa 2010).

Several researchers have discussed the issue of online personal information privacy. Bae and Kim (2010) suggested that, in order to achieve a high level of privacy, the user should be given the authority to control privacy settings when he/she receives or requests a service related to his/her personal information. The authors noted the importance of designing a privacy policy to protect personal information by blocking some people from seeing all or part of the user's personal information. Dötzer (2006, p. 4) stated that "once privacy is lost, it is very hard to re-establish that state of personal rights”. This shows that privacy is essential to the construction of all communication systems, particularly mobile systems. The concept of self-representation enables users to interact and introduce themselves based on the data placed on profile pages such as name and pictures with others. Privacy is an important aspect of self-representation on online social networks since people share certain information with the public and receive information or comments from others.

The nature and complexity of the Internet threatens web privacy (Bouguettaya & Eltoweissy 2003). Each privacy rule or policy can include some restrictions (Sadeh & Hong 2009). A recent study done by USC (University of Southern California) (2013) shows that in 2012, about 91% of respondents had some levels of concern (somewhat concerned and very concerned) about personal information privacy when buying through the Internet.

Although there is no policy mandating online personal information privacy, some types of privacy solutions do exist (Passant et al. 2009). These solutions can be classified into protective technologies, social awareness and legislative support. Protective technologies, such as strong authentication and access control, have developed quickly and have evolved over time. These rely on encryption as a way to solve privacy concerns. The second type of solution, social awareness, involves educating people about the possible risks of personal information misuse when they provide data such as their home address and mobile phone number. Lastly, legislation can be enacted to clarify aspects of the agreement with users to protect the collection of personal information under the framework of the law (Campisi, Maiorana & Neri 2009).

However, as seen from the previous research, there is a relationship between the demographic of users and internet privacy concerns, particularly when submitting some personal information details. Hence, security procedures should reduce these concerns by providing them with confidence and secure protection for their personal information and keep pace with the developments of internet technologies and devices.

2.3.4 Trust

Trust is the main factor for the success of any procedure between users and service providers, particular in a technology environment (Fukuyama 1996). Schoorman, Mayer and Davis (2007) defined trust as believing in another party. Liu et al. (2004) defined it as "in electronic commerce, trust can be viewed as a perceptual belief or level of confidence that someone respects the intentions, actions, and integrity of another party during an online transaction". Furthermore, Grabner-Krauter and Bitter (2013) mentioned that trust in social networking sites is a stable factor between individuals or groups with social networking providers.

In social networking sites, trust is an important element that can determine the success of online social networks and other business websites. Web 2.0 technology and social networking sites together can be objects of trust (Grabner-Kra¨uter 2009). It can be noticed in social networking sites by observing purchase behaviours (Lo & Riemenschneider 2010). Indeed, two studies done in 2010 and 2011 reported that users of social networking sites exhibited a very low level of trust towards the service provider and had considerable privacy concerns (Hargittai 2010; Boyd, 2011). Social network providers and other service providers have to increase users' confidence and push them to trust their services by providing a secure and easy system for users' personal information privacy protection. Spam removal applications are the most trusted applications for users (Hameed et al. 2011; Grier et al. 2010). In social networking sites, the lifecycle of trust can be constructed in three stages: the initial stage of trust, when users entered and create accounts in the site; the stabilizing stage of trust, when users already use the site's services and trust it, and the last stage is dissolution, when the users lose trust with the service provider (Grabner-Krauter and Bitter 2013). Users may also trust communications between their computers and the Internet websites more than online social network providers in terms of leakage of personal information (Cutillo, Molave & Strufe 2009). Indeed, two studies done in 2010 and 2011 reported that users of social networking sites exhibited a very low level of trust towards the service provider and had considerable privacy concerns (Boyd and Hargittai 2010; Boyd, 2011).

PayPal is an example of a trusted system. It is used to complete electronic transactions between a seller and a buyer, both of whom have to trust the system. Each user needs to create an account using authentic personal information and credit card details (Lutz 2012). One of the main reasons for customers’ confidence in the electronic payment system is their trust in the service provider’s ability to maintain their privacy and security (Ally, Teleman & Cater-Steel 2010).

2.3.5 Online privacy risks and protection

There are several privacy risks surrounding the posting of personal information details on social networks. These threats can be caused by hackers or spammers who obtain users’ personal information details. Identity theft, when someone steals the user's personal information, is one of the major risks that users face (Williams et al. 2009). Access to sensitive information may also lead to terrorism risks, financial risks and physical or sexual extortion (Gharibi & Shaabi 2012).

Gao et al. (2011) discussed the common privacy breach attacks in online social networks. First, users usually upload their personal information when they trust the service provider. However, the provider can use these details for business purposes such as advertising. In addition, it is not only the service providers who can see users’ personal information. Some online social networks provide users with policies to determine the list of authorised persons who can see their personal information. These policies vary from one provider to another; some providers give users more flexibility than others, and some provide encryption for their data. The second privacy breach can be caused by users’ friends, who can share users’ personal information details with others. Friends who have access to users’ personal information can copy and publish this information. The third breach is due to spammers. When spammers see a user’s friend list, they can see other users’ personal information by sending them a friend request, impersonating one of his/her friends by using the friend’s name or picture. Lastly, breaches can be caused by third party applications installed by users. These applications can be a threat to users, particularly if they are not from a trusted provider. When the application accesses the users’ personal information, others can obtain this information.

Novak and Li (2012) also stressed that privacy breaches can be caused by friends, applications and the exploitation of personal information details by service providers for advertising. The authors added that understanding privacy settings is not enough to protect users, especially from friends and other online social network users. Thus, social networking websites such as Facebook prioritise the development of tools to protect privacy. This is manifested in the social network providers' requests for new users to create new privacy settings. However, some users do not realise the risk of personal information leakages (Lee et al. 2011). Therefore, sensitive information such as users' home address and date of birth should not be published online, in order to avoid risks to online privacy. Increasing user awareness of these risks, providing a privacy management system for users to control their personal information details and constantly updating privacy policies, can lead to a decline of these risks (Gharibi & Shaabi 2012).

On the other hand, privacy settings that allow the user to control the profile view and distribution of personal data vary across social networking websites, and there is no privacy standard for controlling a user's personal information settings. Although privacy settings should be chosen carefully, most online social network providers have complex privacy settings (Novak & Li 2012). These complex privacy settings may cause confusion among users (Gundecha, Barbier & Liu 2011).

Different techniques have been designed to increase personal information privacy protection. Williams et al. (2009) listed some steps for online social network users to stay safe. These include being aware of the risks of social networks, limiting the posting of personal information details and being careful when dealing with strangers online or when reading any information from any sender.

Most social networking sites have given their users more authority to control privacy settings. Users of some social networking sites are now able to classify their friend list into sub-lists, which allow some personal information details, such as users' birthday or relationship status, to be visible to one sub-list and hidden from others. Fang et al. (2010) designed a privacy recommendation wizard based on user inputs to help users classify their friend list into sub-lists. The wizard gives users two options: to allow the friends in their sub-list to see their personal information or to deny them access to this information.

Configuring privacy settings so that only friends can see one's posts is not enough to defend oneself from other attacks such as applications and advertisements (Stutzman

& Kramer-Duffield 2010). Lipford, Besmer and Watson (2008) found that showing an example of privacy settings will enable users to understand their privacy settings better. It will also help them determine who can see their personal information. For instance, Facebook allows users to see their profiles from their friends' point of view; this allows users to see what personal information their friends can see. This technique helps users understand privacy settings but does not provide security to protect them from neighbourhood attacks, or attacks such as viruses or spam.

Fang et al. (2010) designed a privacy wizard system to make it easier for users to control their privacy settings. It was designed based on friends' classification into groups and asking questions. It guides users in choosing privacy settings for groups or individual users by allowing the users to see or hide an item. For example, if Alice is Bob's friend, then Bob can identify which items of his profile Alice can see. Bob can hide some details such as his date of birth and mobile number from Alice, and can do the same for his other friends.

2.4 Centrality of personal information details in online systems

Today, organisations that process information online use a centralised system to relate and compute data depending on the required outcome (Brown and Institute 2010). Joe Smith, who is a member in Effective Database Management (EDM), defined the centralised system as "there is only one place a user has to go to find his name, primary address, and activities within the association" (EDM 2014).In addition, Babu, Singh and Sachdeva (1997) defined it as "a completely centralised information system handling all processing at a single computer site, maintains a single central database, has centralized development of applications, provides central technical services, sets development priorities centrally, and allocates computer resources centrally". Having personal information stored in a centralised place greatly simplifies retrieval and management of data (Craig & Ludloff 2011). Thus, creating a centralised system as a central control of sharing personal information will assist the user to set standards of collecting and releasing information.

For example, an online credit card transaction can involve various parties such as merchant organisations like eBay, payment companies like PayPal, and customer and merchant banks. If a customer wins an auction in eBay, the customer may wish to pay through PayPal. This means that PayPal must contain the customer's credit card information. In addition, the customer bank also must contain the same information about the credit card. The centrality of personal information will enable PayPal's servers to communicate with merchant servers and banks' servers to effect the payment. Centralised personal information in various databases is usually backed up to avoid information loss in case of system failures (Thampi et al. 2012). Applications that use the centrality of personal information include payment systems (such as PayPal, Skrill and Amazon), online library systems, social networks (such as Facebook, Twitter and LinkedIn), online mail systems (such as Yahoo, Google, and Hotmail), online merchant systems like eBay and many other online applications. The following sections will discuss centrality processes in PayPal, the largest online payment system.

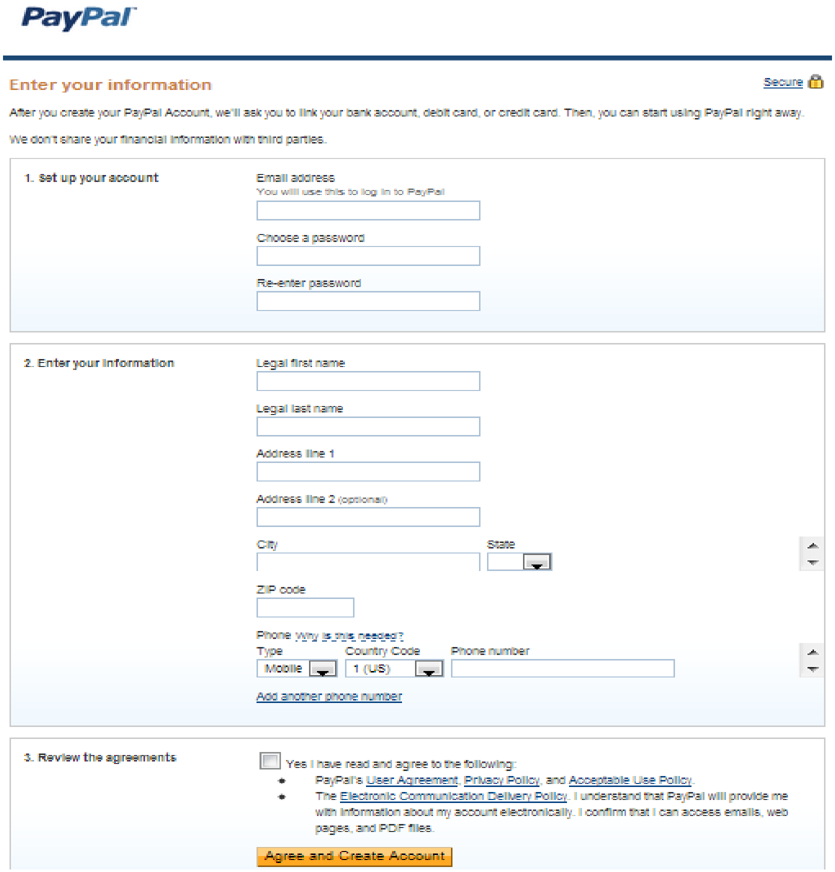
2.4.1 Centrality of personal information in PayPal

One of the online applications using centralised personal information is PayPal. PayPal is the most popular company that acts as a middleman for online purchases (Shadlou, Kai & Hajmoosaei, 2011). PayPal is a broker for online financial transactions. It allows individuals and business organisations to transfer money electronically through each other's email addresses. For individuals and business organisations to transfer money online, they have to fulfil certain PayPal requirements. The requirements include registration for a PayPal account using a valid email address and a valid credit card or bank account (Ford 2009).

For instance, creating a personal PayPal account requires an individual to submit valid basic information (Figure 2.1). This information includes user's name, address, telephone number and email address. This process also involves two security questions that are produced randomly in a sequence of letters and numbers (Savage 2012). The two security questions are important for password retrieval and fraud prevention. A confirmation email is then sent to the email address and the sign-up process completed by following the instructions in the email. Once an account is created with PayPal, personal information submitted is stored in a centralised database.

After successfully creating an account, PayPal requires verification of the account by adding a valid and current credit card to the account. If the account address matches the address from where credit card statements are received, the account is successfully verified (Ford 2009). This verification procedure ensures that buyers and sellers are legitimate and eliminates the likelihood of scammers. PayPal has an Expanded User Service, which allows one to draw money from the credit card, instead of using a bank account. However, one can add funds into PayPal account from a checking account or from PayPal to a checking account. This requires one to add and verify a bank account with PayPal. Adding a bank account requires one to enter an account number and routing number (Shadlou, Kai & Hajmoosaei, 2011). The verification procedure requires the specification of two micropayment amounts made by PayPal to the bank account.

Thus, PayPal creates the centrality of personal information by forming a central database containing individual and business accounts (Figure 2.2). These accounts contain sensitive personal information including names, addresses, phone numbers, email addresses, credit card and bank account details. This information is online; that is, an individual can access personal information from the system at any time by login into the account using valid login credentials (Savage 2012). As long as an individual has valid login credentials, the correct username and password and an internet connection, s/he can access personal information and perform transactions online.



PayPal

Enter your information

Secure

After you create your PayPal Account, we'll ask you to link your bank account, debit card, or credit card. Then, you can start using PayPal right away.

We don't share your financial information with third parties.

1. Set up your account

Email address
You will use this to log in to PayPal

Choose a password

Re-enter password

2. Enter your information

Legal first name

Legal last name

Address line 1

Address line 2 (optional)

City

State

ZIP code

Phone Why is this needed?

Type	Country Code	Phone number
Mobile	1 (US)	

Add another phone number

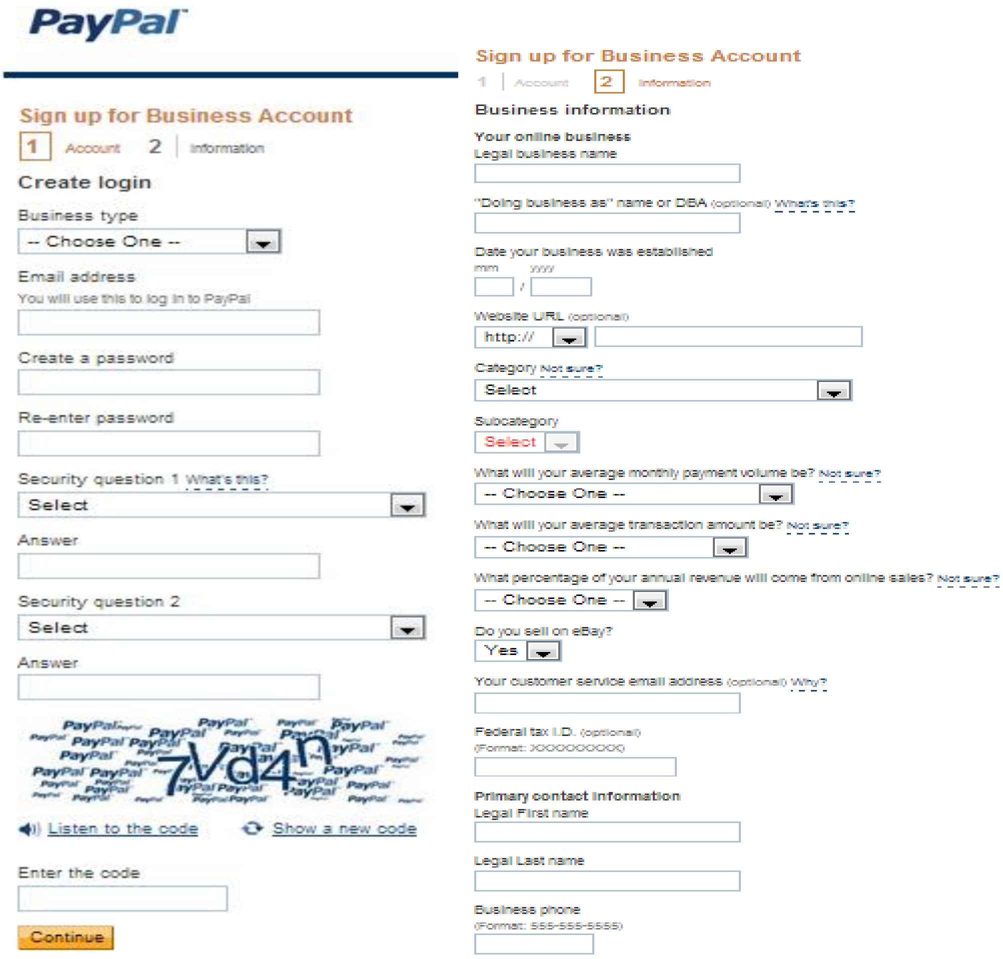
3. Review the agreements

□ Yes I have read and agree to the following:

- PayPal's User Agreement, Privacy Policy, and Acceptable Use Policy.
- The Electronic Communication Delivery Policy. I understand that PayPal will provide me with information about my account electronically. I confirm that I can access emails, web pages, and PDF files.

Figure 2.1. Personal information for opening a PayPal personal account.

Source: www.paypal.com



PayPal

Sign up for Business Account

1 Account 2 Information

Create login

Business type

-- Choose One --

Email address

You will use this to log in to PayPal

Create a password

Re-enter password

Security question 1 What's this?

Select

Answer

Security question 2

Select

Answer

Listen to the code   Show a new code

Enter the code

Continue

Sign up for Business Account

1 Account 2 Information

Business information

Your online business

Legal business name

"Doing business as" name or DBA (optional) What's this?

Date your business was established

mm / yyyy

Website URL (optional)

http://

Category Not sure?

Select

Subcategory

Select

What will your average monthly payment volume be? Not sure?

-- Choose One --

What will your average transaction amount be? Not sure?

-- Choose One --

What percentage of your annual revenue will come from online sales? Not sure?

-- Choose One --

Do you sell on eBay?

Yes

Your customer service email address (optional) Why?

Federal tax I.D. (optional)

(Format: XXXXXXXXX)

Primary contact information

Legal First name

Legal Last name

Business phone

(Format: 555-555-5555)

Figure 2.2. Information required for opening a PayPal business account.

Source: www.paypal.com

2.4.2 How other websites access users' personal details in PayPal

PayPal provides a payflow gateway that is used by other websites, known as merchants (e.g., eBay), to access personal information stored in PayPal (Shadlou, Kai & Hajmoosaei, 2011). This information is not visible, and customers can safely carry out transactions through the merchant websites. A payflow gateway is a server that handles sessions between the merchant websites and PayPal processors (Norris, 2010). The available gateway solutions include Payflow Link, Payflow Pro, PayPal Payments advanced and PayPal Payments Pro. Each one of these solutions uses HTTP (Hypertext Transfer Protocol), SSL (Secure Sockets Layer) or HTTPS (Hypertext Transfer Protocol Secure) protocols to securely transmit data from merchant websites to the PayPal processors.

For instance, Payflow Pro utilises client-server architecture to transmit data from a merchant website to PayPal's processing network (Norris, 2010). PayPal's secure servers process the transaction through acceptance, authorisation, processing and management (Figure 2.3). Transactions are real-time and most of the financial processing centres will process the transaction within a short time. In this client-server architecture, the merchant website is the client, while PayPal processor is the server. The transaction request is encrypted by the client using the latest SSL, and a secure link is established with the gateway server (payflow server) over the Internet (Shadlou, Kai & Hajmoosaei, 2011).

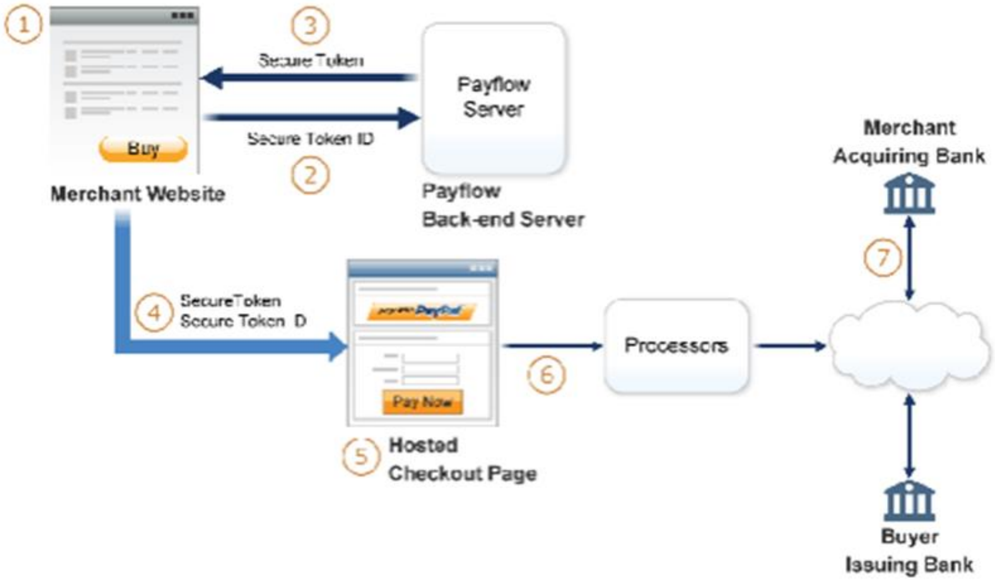


Figure 2.3. PayPal client/server architecture.

Source: Montague (2011).

The transaction request is received by the gateway server, which transmits it to the appropriate financial processing network. The transmission is carried out over a secure private network (Buffington 2010). The financial network provides real-time payment authorisation. The financial network returns a response over the same secured private network into the gateway server. The gateway server then returns the same response to the client over SSL in the same session. To complete each transaction session, the client transparently sends a transaction receipt to the gateway server before disconnecting the session (Montague 2011). The entire transaction takes place synchronously in real-time. Once the transaction process is initiated, it is immediately processed and the response is returned within a few seconds.

2.4.3 Personal information security in PayPal

According to PayPal (2013) requirements, it is the responsibility of the merchant website to ensure that it complies with Payment Card Industry (PCI) standards to protect personal information. The merchant website is also supposed to ensure that it implements security safeguards when processing payment card transactions. To ensure that merchant websites comply with PCI standards, PayPal’s gateway solution provides a secure token and hosted checkout pages. A merchant website is required to use its own means to meet PCI compliance if it does not use secure token or hosted pages.

Personal data might be compromised if parameter data are allowed to be displayed in a hosted checkout page. In order to eliminate the need to resend parameter data, request transaction data is stored on the gateway server using a secure token. Another method used by PayPal to help merchant websites to achieve PCI compliance is hosted checkout pages (Ford 2009). PayPal’s gateway server enables the use of such pages (Figure 2.4). Customers are able to transmit transaction data securely to the gateway server and collect credit card acceptance data by hosted checkout pages.

The figure below illustrates the transaction flow for merchant websites using hosted pages and a secure token (Montague 2011).

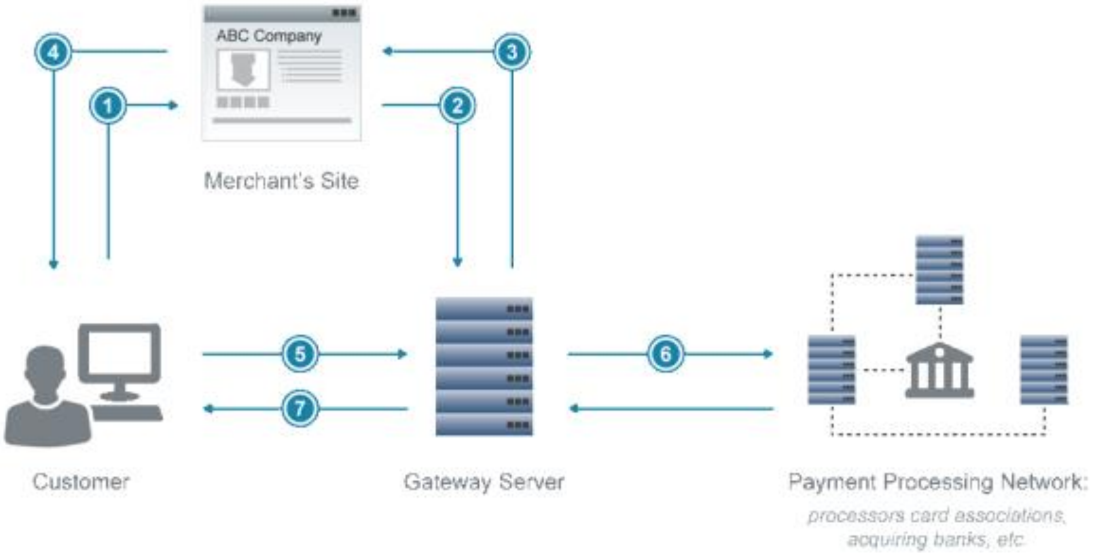


Figure 2.4. Transaction flow for merchant websites using hosted pages.

Source: Montague, (2011).

When a customer wins an auction in a merchant website, for instance in eBay, the customer clicks on the buy button to purchase the merchandise. This link requests a secure token by passing a token ID to the gateway server (Montague 2011). A secure token and token ID are returned to the website by the gateway server. The customer's browser is then redirected to hosted pages by submitting the secure token and token ID in an HTTP post to pages hosted on the gateway server. Using the secure token, the gateway server retrieves the transaction details. The customer's personal and sensitive data are not submitted to the merchant website in this case (Shadlou, Kai & Hajmoosaei, 2011). Instead, the customer submits personal information directly into pages hosted by the gateway server. This greatly helps the merchant website meet the PCI compliance requirements. The gateway server communicates with the customer and merchant banks through a secured private network and processes the payment (Nahari & Krutz, 2011). The transaction results are then displayed on the merchant website for the customer.

- ***Transparent Redirect***

In this case, a customer is transparently redirected to PayPal's website or the gateway server (Montague 2011). Therefore, the customer does not enter sensitive personal information on the merchant’s website. Transparent redirect therefore protects personal information and enables the merchant’s website to meet the PCI compliance requirements.

- ***Fraud Protection Service***

PayPal has a fraud protection service that can be used by merchant businesses to protect themselves from costs and damages resulting from fraud. Fraud protection service uses fraud protection filters, which merchant businesses can use to detect fraudsters using stolen or fake credit card information (Montague 2011). When a fraudulent activity is detected by the fraud protection service, the merchant is notified and decides whether to proceed or reject the transaction. This service also helps merchants to minimise the risk of their customer database being hacked.

2.4.4 Challenges regarding centralised personal information in online systems

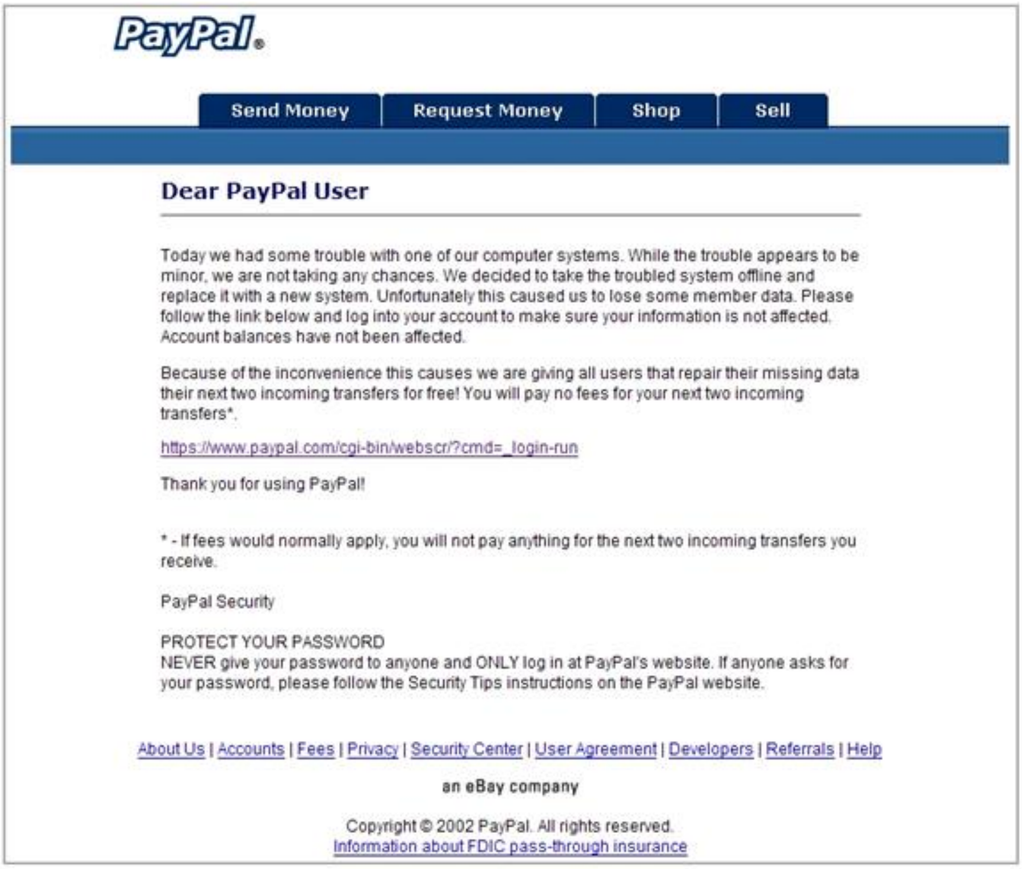
One of the major challenges for online systems is the security of personal information. For example, cybercrime in E-commerce targets classified personal information, thereby exposing individuals to risks of fraud that may lead to significant uninsured losses (Panigrahi 2009). IC3.gov, which is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center, registered over a quarter of a million complaints related to internet crime in the year 2009. A security company called Mandiant reported that in 2013 the average time for detecting security breaches decreased from 243 days in 2012 to 229 days and the number of companies that detected their own breaches declined from 37% to 33% (Mandiant 2014). In addition, there is a growing underground marketplace that trades on stolen personal information.

The most common security threats to personal information in centralised online systems are widespread. The security threats are discussed in brief in this section. Malicious codes, which include viruses, worms, bots and Trojans affect online security (Berlatsky 2013). Viruses duplicate themselves and spread into files containing personal information. These viruses, macro viruses, file-infecting viruses and script viruses invade computer systems. Worms can spread from one computer system to another while infecting files on their way (Seth, 2009). The third type of malicious code, bots, is installed in computer systems and allows the system to respond to external commands by an attacker. This is known also as a Trojan horse which contains malicious code to execute specific actions based on its nature. Malicious codes invade and steal, destroy or alter classified personal information in online systems (Solms & Solms, 2009).

The second category of security threats to centralised online systems is unwanted programs. These programs are installed in users' browsers without their consent. These programs have the ability to monitor and alter the settings of a user's browser, cause unwanted pop-ups and steal personal information (Corporation 2011). Unwanted programs called browser parasites can monitor and undetectably alter the settings of a user's browser. Another program called adware causes unsolicited pop-up ads in a user's browser. Spyware program can be installed in a user's browser to steal personal information through user's emails, keystrokes and so on (Nahari & Krutz 2011).

Another security threat, which is considered the fastest growing form of e-commerce crime, includes phishing and identity theft. In phishing, an attacker will deceitfully mimic a legitimate website and lure users into a fake website (Forte 2009). A user will be prompted for personal information without knowledge that the website is false. This enables a third party to acquire the user's private and confidential information for financial or other gains. The most popular phishing attack is email scam letters, in which a user receives an email appearing to be from a legitimate website urging him/her to follow a given link and log into his/her accounts. The message contains a link that looks like that of a legitimate website. However, the user is then redirected to a website that is different from the legitimate one.

For instance, in the year 2002, a group of PayPal users received an email shown below.



Dear PayPal User

Today we had some trouble with one of our computer systems. While the trouble appears to be minor, we are not taking any chances. We decided to take the troubled system offline and replace it with a new system. Unfortunately this caused us to lose some member data. Please follow the link below and log into your account to make sure your information is not affected. Account balances have not been affected.

Because of the inconvenience this causes we are giving all users that repair their missing data their next two incoming transfers for free! You will pay no fees for your next two incoming transfers*.

https://www.paypal.com/cgi-bin/webscr/?cmd=_login-run

Thank you for using PayPal!

* - If fees would normally apply, you will not pay anything for the next two incoming transfers you receive.

PayPal Security

PROTECT YOUR PASSWORD
NEVER give your password to anyone and ONLY log in at PayPal's website. If anyone asks for your password, please follow the Security Tips instructions on the PayPal website.

About Us | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Help

an eBay company

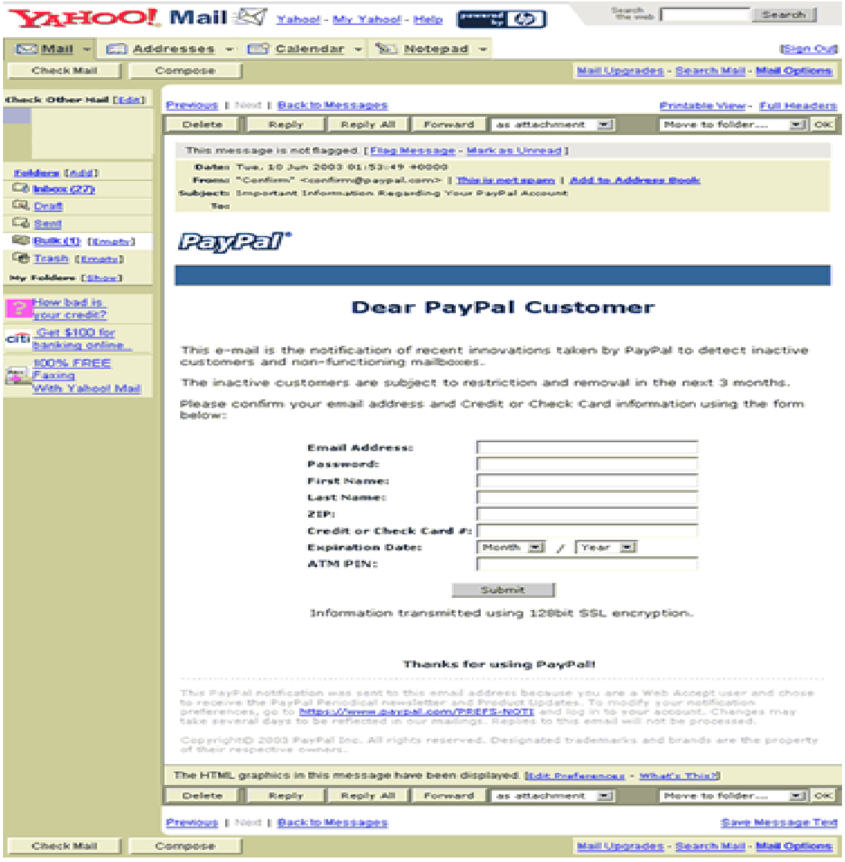
Copyright © 2002 PayPal. All rights reserved.
Information about FDIC pass-through insurance

Figure 2.5. Email scam with link.

Source: Savage, (2012).

The above email may look legitimate, but it can be used by the hacker to obtain the user’s password. The hacker then uses the password obtained to log into the user’s accounts and steal his/her money. In reality, the address behind the link provided is not PayPal’s but an address sending the user to the hacker’s website.

Another form of advanced email scam does not provide any link for the user to click, and thus it is difficult to tell whether it is legitimate or not. In this scam, the email sent directly to the user’s inbox contains a form. The email prompts the user to provide personal details to confirm some information in his/her account. The email may further threaten to cancel the user’s account if the information is not provided. The user will then be required to submit the form to a fake email address that is made to look legitimate. An example of an email scam with a form is shown Figure 2.6 below.



This message is not flagged. [Flag Message - Mark as Unread]

Date: Tue, 10 Jun 2003 01:53:49 +0000
From: "Confirm" <confirm@paypal.com> | This is not spam | Add to Address Book
Subject: Important Information Regarding Your PayPal Account
To:

PayPal®

Dear PayPal Customer

This e-mail is the notification of recent innovations taken by PayPal to detect inactive customers and non-functioning mailboxes.

The inactive customers are subject to restriction and removal in the next 3 months.

Please confirm your email address and Credit or Check Card information using the form below:

Email Address:	
Password:	
First Name:	
Last Name:	
ZIP:	
Credit or Check Card #:	
Expiration Date:	Month / Year
ATM PIN:	

Submit

Information transmitted using 128bit SSL encryption.

Thanks for using PayPal!

This PayPal notification was sent to this email address because you are a Web Accept user and chose to receive the PayPal Periodical newsletter and Product Updates. To modify your notification preferences, go to https://www.paypal.com/PREFS-NOTI and log in to your account. Changes may take several days to be reflected in our mailings. Replies to this email will not be processed.

Copyright© 2003 PayPal Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

The HTML graphics in this message have been displayed. [Edit Preferences - What's This?]

Figure 2.6. Email scam with a form.

Source: Savage, (2012).

The email above is certainly from PayPal; however, the user is directed to a website that looks like a legitimate PayPal website. This form of scam where the hacker's website resembles a legitimate website is called web spoofing.

Furthermore, personal information in centralised online systems is threatened by hacking and cybervandalism. Hackers utilise security flaws in online systems to gain access and tamper with information contained within them (Buffington 2010). In cybervandalism, a hacker intentionally disrupts, defaces or destroys the online system or website. Hackers have successfully attacked reputable online companies such as Google, Yahoo, Microsoft and PayPal among others all over the world (Portela & Cruz-Cunha, 2010). The hackers use security flaws present in these systems. For instance, security flaws in SSL expose PayPal's system to hackers, as it heavily depends on SSL as a means to obtain security.

For instance, PayPal was attacked by hackers who realised that the “address confirmation process” involving PayPal’s customers’ accounts had serious security flaws (Plotkin 2012). The hackers were from Russia, and their activity was detected by those on the Internet familiar with Russian. According to reports, PayPal experienced some technical hitches in solving the problem, an indication that many PayPal accounts with confirmed addresses could have been hacked into (Plotkin 2012).

Another form of security that threatens personal information in online systems is credit card fraud (Panigrahi, 2009). Many customers are discouraged from undertaking online purchases for fear of their credit card information being stolen. Usually, merchant servers are faced with a risk of getting hacked into and exposing credit card files and other confidential customer information files.

Other security threats to personal information in centralised online systems include sniffing, insider jobs and poorly designed or configured server and client software. Sniffing targets the communications channel through an eavesdropping program. The program monitors information transfer over a network, enabling hackers to steal confidential data from any point in the network (Towle 2009). Today’s servers involve a complex set of software programs. If these software programs are poorly designed or configured on the client or server, confidential personal data becomes vulnerable, giving an opportunity to exploit it.

Online companies have put in place mechanisms to protect their clients’ confidential information and safeguard their companies’ reputation. There are three key points that make an online company vulnerable to attacks and the exposure of confidential personal information. These points are the client, server and communication channel (Lee 2011). Figure 2.7 below shows a typical model of an online transaction.

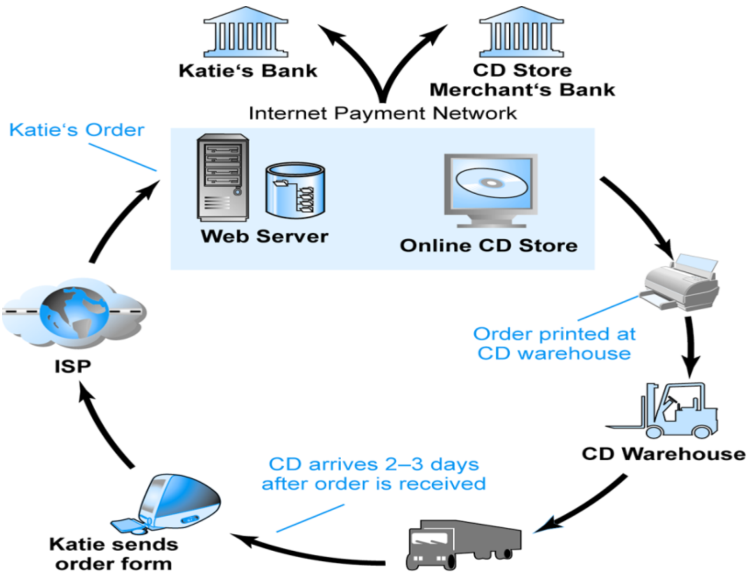


Figure 2.7. A typical online transaction model.

Source: Lee (2011).

In this online transaction, the vulnerable points are shown in the diagram below:

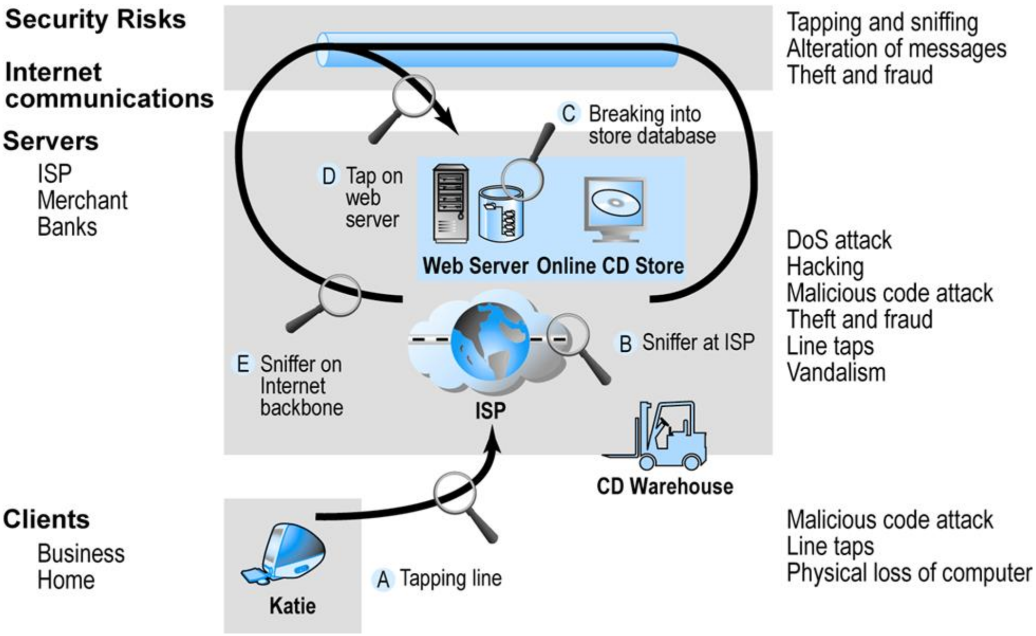


Figure 2.8. Vulnerable points in a typical online transaction network.

Source: Lee (2011).

To strengthen the security of personal information, online companies adopt new technologies, enhance strict organisational policies and procedures and follow the industry standards and government laws (Lee 2011). Online companies also tend to consider other factors such as the value of time, money and the cost of security compared to the potential loss and their weakest links. However, there are certain challenges these companies face in their attempt to achieve the highest degree of security. The challenges arise from tension between security and other values. For instance, when a company or an online organisation adds more security features to its website, customers find it difficult to use the site. In addition, the site becomes slower. The other challenge is tension between security and the desire of individuals to act anonymously.

2.4.5 Security of personal information in centralised online systems

Various technological solutions are available for achieving site security. They include encrypting information over communication channels, securing communication channels through various protocols (SSLs and VPNs (Virtual Private Network)), protecting information systems through firewalls and protecting servers and clients (Whitman, Mattord & Green 2012). The following diagram shows various tools available for achieving the security of confidential information in online systems.

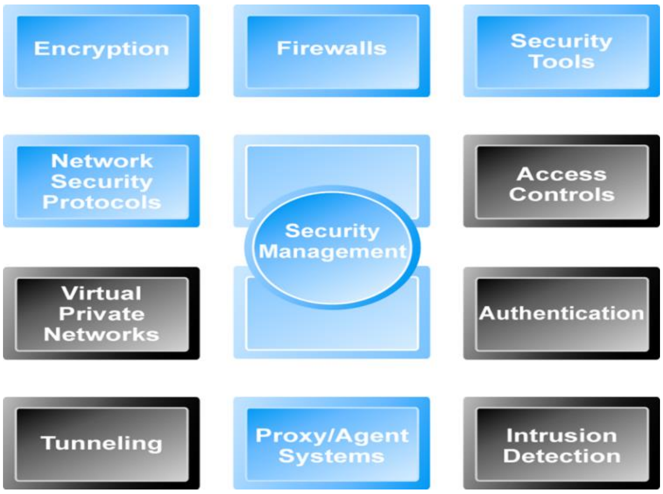


Figure 2.9: Tools for achieving the security of information in online systems.

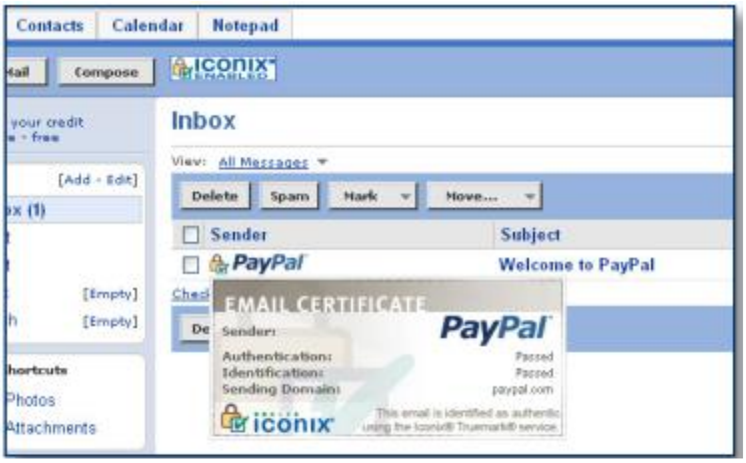
Source: Corporation (2011).

- ***Information Encryption***

Data encryption involves transforming plain text data into cipher text that is only understood by the sender and the receiver systems. The data become useless to individuals if they cannot decrypt them. Thus, data encryption protects stored information and data transmission over communication channels (Burdon, Reid & Low 2010). Encryption provides message integrity, non-rejection, authentication and confidentiality of personal information. Data can be encrypted using various methods. Symmetric key encryption is where data are encrypted at the sender and decrypted at the receiver end using the same digital key (Zhang 2009). This method of encryption requires each transaction to use a different set of keys.

Public key encryption uses two digital keys, a public and private key, which are mathematically interrelated. Both keys are used to encrypt data at the sender and decrypt data at the receiver end. In this encryption method, data encryption and data decryption use different keys, where the recipient's public key is used to encrypt data at the sender end and a private key is used to decrypt the message at the receiver end. Public key encryption can use digital signatures and hash digests or digital envelopes. The receiver can use a hash digest of data, which is sent along with the message, to verify its integrity. In this method, data and hash message are encrypted with the recipient's public key. The recipient's private key then encrypts the whole cipher text. This procedure creates a digital signature, which helps in authentication and nonrepudiation at the receiver end (Zhang 2009).

Public key encryption increases the processing time, reduces the data transfer speed and is computationally slow, whereas symmetric key encryption is less secure. Digital envelopes are designed to address the weaknesses presented by the public and symmetric key encryption techniques. Digital envelopes use a symmetric key to encrypt data and public key encryption to encrypt and send the symmetric key. To ensure a company's identity to its customers and to reduce the chances of spoofing, digital certificates are used. Digital certificates and public key infrastructure includes the company's name, the company's public key, the serial number of the digital certificate, issuance and expiration dates, the third party company that issues the certificate and other identifying information (Forte 2009). Client certificates can also help in curbing web spoofing, but they are rarely used. An example of a digital certificate is shown in Figure 2.10 below.



□ Sender	Subject
□ PayPal	Welcome to PayPal

EMAIL CERTIFICATE

Sender: PayPal

Authentication: Passed
Identification: Passed
Sending Domain: paypal.com

This email is identified as authentic using the Iconix® Truemark® service

Figure 2.10. Icontix digital signature in Yahoo! Mail client.

Source: Forte (2009).

The use of public key infrastructure to protect personal information in centralised online systems has certain limitations. Public key infrastructure only protects information during transmission and is ineffective against inside attackers. In addition, it may be dangerous to allow the protection of private keys by individuals. Further, there is no assurance verifying that the merchant's computer is secure. CAs certificates are not regulated and are from self-selecting organisations (Zhang 2009).

- ***Securing Channels of Communication***

There are a few protocols that are currently used to secure confidential information. The most common methods used for online security are SSL and VPNs. Other mechanisms include TLS and SET.

SSL is a protocol used to secure a communication channel by maintaining client and server authentication. In SSL, the client and server certificates are used to encrypt communication between the server and client. This encryption mechanism creates virtual information that is difficult for others to hack (Tomei 2011). Figure 2.11 below shows how SSL works.

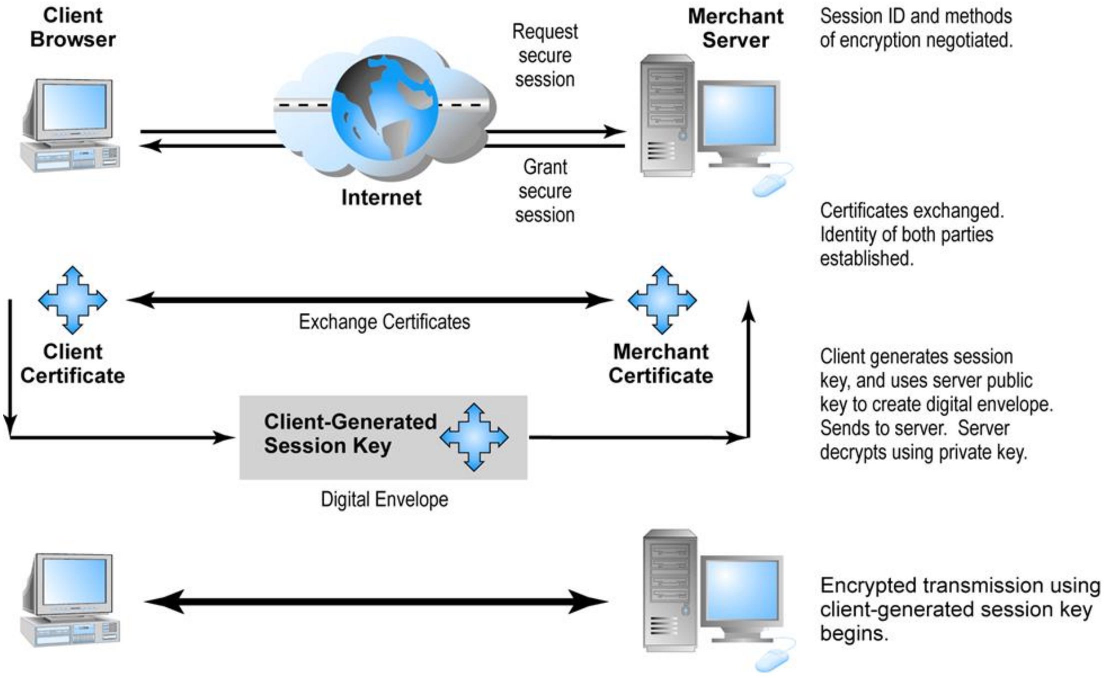

Client Browser
Request secure session
Merchant Server
Session ID and methods of encryption negotiated.
Internet
Grant secure session
Certificates exchanged. Identity of both parties established.
Exchange Certificates
Client Certificate
Merchant Certificate
Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.
Client-Generated Session Key
Digital Envelope
Encrypted transmission using client-generated session key begins.

Figure 2.11. Secure negotiated sessions using SSL.

Source: Zhang (2009).

VPNs form a communication system that permits access to an internal database in a secure connection over the Internet. Virtual private networks use point to point tunnelling protocol (PPTP) (Whitman, Mattord & Green, 2012). TLS refers to a transaction layer protocol. This protocol is based on SSL, but it has some variations in its Media Access Control (MAC) layer. This protocol may soon succeed SSL, as its specifications are stronger and more precise since it does not involve a client certificate and is more flexible. SET refers to secure electronic transaction. SET provides a mechanism through which the client’s credit card number is sent to authorising banks. This method lacks sufficient market support to allow for effective implementation (Polgar 2013).

- ***Protecting Networks***

Networks are usually secured from intrusion using well-configured firewalls and proxy servers. A firewall involves hardware and software that filters and stops some packets from entering the network depending on the security policy of an organisation (Whitman, Mattord & Green, 2012). There are two main techniques, namely packet filters and application gateways, that are used in firewalls. Proxy servers handle all the communication between an organisation's systems and the Internet.

- ***Protecting Servers and Clients***

Online systems need to be protected from unauthorised access, which may lead to the alteration, destruction or theft of confidential personal information. Servers and clients are usually protected through operating system controls that provide strict authentication and access control mechanisms. In addition, antivirus software that detects and eliminates malicious codes provides a cheap way of preventing threats to system integrity. Since different malicious codes are produced daily, antivirus software needs daily updates (Diogenes & Shinder 2010).

2.4.6 Advantages and disadvantages of centralised personal information details in online systems

Centralised personal information has several advantages related to information storage and access in online systems. The greatest advantage of centralised personal information details in online systems is convenience. Individuals can perform transactions from any location and at any time as long as they are connected to the Internet and the system is functioning properly (Montague 2010). There are no physical queues or waiting for a merchant or business to open. For instance, if individuals are on vacation and need to pay for their utility bills, they can securely log into their online accounts and pay their bills while away.

Another advantage of centralised personal information in online systems is that it saves time. Online transactions happen very quickly. Once the system is set-up, captures and stores an individual's personal details, the individual can carry out online transactions in a flash (Lee 2011). This means that individuals can concentrate on other activities instead of spending time performing offline transactions, which involve many procedures and a lot of time. For instance, according to Norris (2010), electronic payment methods have reduced bill management or payment by over 60% in the 2010 in the United States.

Another benefit of the centrality of personal information is cost. The cost of performing transactions online is minimal. For example, the majority of merchants, vendors and businesses do not charge their clients for online payments. For those who charge online transactions, the fee is very small (Lee 2011). This means that an individual can save hundreds of dollars per year through online transactions. This is an important consideration in this financial era where individuals are trying to reduce their expenses.

As technology is improving, online transactions are becoming more secure than other transaction methods. This means that centralised personal information is becoming more secure, as there are a limited number of people who have access to such information. Manual systems are more susceptible to identity theft, for instance from an individual's mail box or discarded trash. In online systems, security mechanisms such as data encryption ensure that confidential personal information is protected from unauthorised individuals (Barthe, Batta & Etalle 2011). Centralised personal details also eliminate or lower the risk of human errors, as few individuals are involved in handling online transactions.

One of the disadvantages associated with centralised personal information in centralised systems is identity theft. Online companies find it difficult to authenticate or verify whether the person entering the information online is the owner of the account. It is difficult to request picture identification or even a signature. For instance, an individual can perform transactions online using stolen credit card information. Currently, there are no online mechanisms to identify individuals performing transactions online, and transactions can be successfully undertaken online using stolen information (Ford 2009).

Another disadvantage associated with online systems is that many of the merchant websites require registration to open accounts with them. To be authorised to perform transactions online, one undergoes a series of cumbersome procedures (Corporation 2011). These procedures are put in place to ensure customers' security but end up discouraging potential customers from registering. The overall process of online transaction is efficient, but initial registration can be time consuming. Centralised personal information requires one to have a username and a password. This requires password protection in order to maintain an account at each organisation. This process becomes extremely cumbersome for customers having and operating multiple accounts.

Maintaining a high level of trust is also another risk associated with centralised information in online systems. Sandeep and Jeffrey (2001) found that "trust in the provider is one of the most important determinants in the purchase decision", also they found that "trust [in the provider] is rated higher than performance and price-related variables". However, the excessive trust in the online system could be a reason for failure to take security measures by protecting personal information. In 2013, Adobe's security team discovered a sophisticated attack on their servers. The attacker was able to reach IDs and encrypted passwords for customers which contributed to access of over 2.9 million of users' profiles (Adobe, 2014). One of the main procedures that Adobe recommended was that all customers who use the same ID and password for other sites to change them to avoid other accounts being hacked (Adobe, 2014).

2.5 Mobile web systems

Mobile networks, which are generally defined as the use of mobile devices to communicate with others, have recently become more popular as they are an effective means to share information and files between users. They combine mobile phone and Internet services. They consist of the hardware and software that facilitates access to and use of online applications, such as Facebook, Twitter and other social networking venues. Furthermore, these applications have enabled mobile users, companies and most developers of online applications to compete to acquire the largest number of users. The mobile network is formed by mobile devices, such as tablets, mobile phones, laptops and other devices that enable users to communicate over wireless links. Several features have contributed to the rapid spread of this network, including mobility, the smallness of the size, ease of use, access to online information and other features. According to Lane et al. (2010), some factors have affected the increased sales of internet mobile devices around the world. Some of these reasons include the low cost of embedded sensors and chips and the availability of different kinds of internet mobile applications and applications that support sharing real-time activities with others, such as Facebook or Twitter applications. Lenhart et al. (2010) conducted a study that showed an increase in the number of people who use mobile devices to browse the Internet, and this number will continue to grow over time. As a result, these advantages and challenges encouraged developers to design new technologies and applications for mobile networks to meet consumer demands.

This network is a set of tablets, mobile devices, laptops and other devices that communicate with each other using the services provided by the network operator, such as an internet service provider, which enables the users to move from one place to another while maintaining internet connectivity (Ernst 2007, p. 2–3). According to Ernst, there are several types of mobile network:

- personal area networks: mobile networks used for communication among the cell phone interface and personal devices themselves, including mobiles, Bluetooth devices and others, in proximity to an individual’s body,
- networks of sensors in vehicles,
- access networks deployed in public transportation, and
- ad-hoc networks connected to the Internet via mobile routers.

According to Xiang, Magnini, and Fesenmaier (2015) the owners of smartphones in Europe have the same priorities of using mobile applications, including social networking applications and search engines, with basic mobile services. In contrast , a study done by ARD/ZDF-Medienkommission showed that in Germany most of smartphone owners used messaging and social networking applications more than other mobile services (Berry and Schleser 2014). For further comparison, a study done in France by SFR stated that 58% of smartphone users accessed social networking sites and 56% used map and GPS applications (Prunel and Lees Perasso 2014).

2.5.1 Mobile web

The mobile web is no longer distinct from the desktop environment, especially with regard to web browsing. Different access issues have been improved, such as bandwidth and multimedia evaluation. Dhar and Varshney (2011) discussed the present and the future high-speed networks used by the mobile web; for instance, 4G technology offers high-speed access for the mobile web, and it will create new market opportunities. The authors also mentioned an important point related to this research topic. Because a difference exists in the size of mobile phone screens and the size of screens on other mobile and stationary devices, the ability of mobile browsers to display different data formats (web pages, text, font sizes or images) is affected. Consequently, advertisements should be designed based on the end user's mobile device, i.e. either tablets or smartphones. Hence, this research will address the previous point, and it will be adopted as a base for designing a privacy model.

At present, the use of mobile web networks has become more commonplace, as has the use of social networks, electronic transactions and voice and video communications. Different researchers have discussed different areas of the mobile web. Lenhart et al. (2010) showed that approximately 55% of adults use their mobile phones to connect to the Internet. Furthermore, Schmiedl, Seidl and Temper (2009) suggested that, in the future, mobile phones, rather than desktop computers, will be the main device for browsing. Additionally, they measured several aspects related to using mobile phones to browse the Internet in Austria. They asked people to note the type of mobile phone they use to browse the Internet, to identify the sites they most often visit and to name the sites that offered a special version for viewing on mobile devices. Their findings show that most of the users between the ages of 19–29 years visit sites related to news, weather, social networking and entertainment. Only six out of 100 websites offered a special version for mobile phone access viewing. Of the 100 websites, 55% were information services, 20% were social websites and 18% were search engines and online shops. Moreover, about 40% of the users who visited websites that offer mobile access versions reported that access to these sites was faster than browsing websites that do not offer a mobile viewing version (Schmiedl et al. 2009).

Furthermore, mobile devices are characterised by several physical and technical advantages. These advantages have led to an increase in the percentage of people around the world who use these devices. A research study conducted by Want (2009) showed that mobile devices are preferred over desktop computers and laptops. In 2013, the percentage of people using cell phones and smart phones is expected to be greater than the percentage of people using laptops. Indeed, mobile applications and services need to be improved in order to fit smaller screens.

Vaughan-Nichols (2008) discussed several mobile web issues including the capacity of a mobile device to be used as a web browser. The author showed that some mobile device features, such as high-speed Internet access via wireless application protocols, access to 3G cellular networks and email and other web-based services, make it possible to use mobile devices as web browsers. On the other hand, mobile devices face several difficulties before they can be considered fully functional browsers. These include the need to improve existing internet services and applications to meet users' desire to use touch screens and to adapt the size of the mobile device screen to address future capabilities. Additionally, a relationship exists between a mobile device's screen size and its display capabilities. This can be seen in the relationship between the size of the screen and the viewing distance. When the screen's size becomes larger, the view becomes clearer (Knoche, McCarthy & Sasse 2005). Hence, the size of the screen is an important element for viewing, and the web content accessed by browsing on a mobile screen should be clear and easy for users to read. Therefore, any recommended privacy model should take this point into consideration so that the privacy options are more clearly presented to users.

Competition exists between mobile web developers, such as Apple, Google and others, to achieve an expanding "view" on the mobile web. This leads to the creation of two types of mobile browser paradigms: server transcoding and direct delivery. The difference between these paradigms is that the server transcoding option requires a server in the middle ("a proxy server") to receive the requested URL from the mobile user, whereas the direct delivery option has direct access to the Internet and can provide HTML from a web server. The direct delivery option is already used on desktops and in some mobile browsers, such as the iPhone and the Android smart phone. Mobile web browsers have also been developed to lead the way to integrate web viewing into the mobile web framework. Some applications, such as Opera, Google and Safari, support features such as zoom in/out and touch (Hernandez 2009). Therefore, it is necessary for developers to implement the web view concept, and when mobile device web viewing is simple and clear, the percentage of users will increase.

Cui and Roto (2008) identified how people use the web on mobile devices. Based on some related research and methodologies, they examined the taxonomy of users' activities when using the mobile web. The study results show that the mobile web can be used in several different ways. Users can download a train timetable site to their mobile devices to minimise connection expenses; they can use their mobile device to find facts, especially when looking for specific information that requires immediate access to the Internet. Mobile devices can also be used for information gathering and casual browsing. The same study also showed related communication uses, such as checking and sending messages via mobile mail, communicating online via discussion forums or any online platform where people post or connect with other via social networks, such as Facebook, where people share information and capture public data. People also use mobile devices to read the news, select ring tones and download applications. Therefore, because the mobile web browser can offer a variety of different web-based services, the authors suggest that a browser be developed that makes it easy to surf the Internet through a mobile device.

However, there were several recent studies that showed some important developments to smartphones which facilitate the use of web services via them:

- In 2014, some smartphones, such as LG G3, used high definition quality for their screens that are similarly used in some televisions and computer monitors 2K (2560*1440 pixel) which is a significant improvement compared with Apple iphone 5S (Bolster and Giardini 2014).
- In 2013, the design of some smartphones was provided with some security identities and encryption methods (Etherington 2013).
- Wifi networks are much more used than before in smartphones and have become more prevalent and easier to connect to (Dhondge et al. 2014).

2.5.2 Usability of internet mobile devices

The widespread use of internet mobile devices has encouraged companies and internet software developers to prioritise usability. A recent study carried out by Accenture Company (2012) states that in the last year, 69% of participants used internet mobile devices for accessing the web, and the research team recommended that the sites' owners support their websites for use in smaller mobile devices. In further evidence for the increased use of internet mobile devices for accessing the web, StatCounter Global Statistics (2013) showed the upward trend in the use of internet mobile devices compared to desktop computers. In 2010, 98.44% of web traffic came from desktop computers and 1.56% from mobile devices, but in 2013 this changed to 86% for desktop computers and 14% for mobile devices. Furthermore, Rosenthal (2013), who is a member in the International Internet Preservation Coalition General Assembly 2012 at the Library of Congress, declared in his blog page about the workshop of the web future that the old goals are no longer possible and they have to be updated based on user experiences.

In the last decade, mobile phones have been developed to be minicomputers, which are now known as Smartphones. Several challenges are apparent. Some are hardware-based and others use copious software. One important question is screen size: the image fit differs between desktop computers and mobile phones and, of course, phones do not have a full-sized keyboard or mouse. Various companies have developed internet-specific mobile browsers including Opera, Internet Explorer and Safari (Lewis & Moscovitz 2009). Today, most mobile internet browsers support various programming languages, including HTML and JavaScript, but they do not browse as effectively as do laptops or PCs because the screens and keyboards are smaller (Guan, Xiong & Chen 2011). A recent statistical report done by KPCB (2012 a) and (2012 b) showed that these days internet users spend about 50% of their time using the Internet to browse and the percentage of users who use internet mobile devices has surpassed the number of desktop computer users. In addition, social networks played a significant role in this percentage.

Developments in this field are not confined to commercial purposes. In the educational field, for example, Ijtihadie et al. (2010) designed a tool allowing quizzes to be answered using a mobile phone. Also, recent improvements in display quality and zooming have found applications in health sciences. Today, several software packages allow the manipulation and internet transfer of radiological images using different protocols (Drnasin & Grgic, 2010).

Touch screen technology has gained wide acceptance and is used in mobile phones, IPods, music players, and other devices (McGookin, Brewster & Jiang, 2008). In addition, some mobile phone companies, including Apple and Samsung, have developed internet-capable mobile phones that use this technology. This does not make the technology inaccessible to the blind. For example, "Voice Over" and "Siri" from Apple are voice services that read screen content and execute some spoken orders (Krajnc et al. 2011).

On the other hand, several studies have focused on the usability of internet mobile devices based on information needs and the diversity in the use of internet services. Sohn et al. (2008) conducted a study about mobile information needs and found that about 72% of participants used internet mobile devices to collect information about activities, locations, time and conversation with others. Similarly, Church and Smyth (2009) found that 67% of participants used internet mobile devices for collecting information about locations, time, activities and social communication. A recent study done by Chua et al. (2011) confirmed that mobile information needs centred on these aspects: locations, activities, time and social interactions. Furthermore, a four-week diary study done by Heimonen (2009) demonstrated that specific internet mobile applications such as social network applications are often used more than using web search engines in mobile information needs. Moreover, Church and Oliver (2011) carried out a study that was based on measuring the behaviours of 18 participants who actively use internet mobile devices for browsing. The results showed that participants used different internet mobile tools such as maps, mobile search, browsing, email, social networks applications and other tools. Social network applications achieved the highest percentage of the daily distribution of these tools (27%), while email and browsing sequentially achieved 18.8% and 14.9%.

To understand the usage of internet mobile devices, Hinman, Spasojevic and Isomursu (2008) highlighted that some people with PC experience have tried to use this knowledge to create a port for PCs through internet mobile devices, but in many cases these attempts have failed. Another study done by Nylander, Lundquist and Brannstorm (2009) showed that about 38% of internet mobile usage is at home and many users prefer to browse the Internet through their internet mobile devices rather than computers. Indeed, browsing on internet sites has been developed to suit different types of internet mobile devices. Several companies have developed their own sites to adapt internet mobile devices by using different techniques or applications such as RSS or mini browsers. The content of the site was minimised to facilitate browsing through small screens (Blekas, Garofalakis & Stefanis 2006). Some people prefer having the full website view, and the others prefer browsing sites using a mobile browsing version. Kaikkonen (2008) conducted a study in different countries, and the results showed that American and European participants chose viewing the full content of a website, but participants from Asia opted to browse the site through a mobile version that has specific information.

Recently, competition has begun among internet application developers to develop internet applications that are suitable for browsing via mobile devices. For example: in August 2010, there were about 30 million users of the Instagram application who shared about 150 million photos, which makes it superior to other image-sharing applications (Bullas 2012). Beach et al. (2010) pointed out that online social networks such as Facebook, Twitter and MySpace will increase support for mobile web devices. Various companies have developed mobile-specific internet browsers including versions of Opera, Internet Explorer, and Safari (Lewis & Moscovitz 2009). Today, most mobile internet browsers support various programming languages, including HTML and JavaScript, but they do not browse as effectively as laptops or PCs because the screens and keyboards are smaller (Guan 2011).

2.6 Internet privacy systems

As mentioned before, privacy regulations can be defined as sets of rules or policies set by users to achieve a certain level of privacy. For example, in terms of privacy location, privacy regulation means providing privacy policies and access to others to identify a user’s location. Each rule or policy can include some restrictions (Sadeh & Hong 2009). Therefore, different privacy policies may be applied depending upon the user’s needs and the type of personal information collected. Furthermore, Wang and Cui (2008) claimed that privacy is a state or condition of limited access to a person. This encourages this study to examine two dimensions for privacy. First, it will address the importance of individual rights, which means users are able to determine who, how, when and what information will be released to other people. Second, it will also address the purpose of using information by answering such questions as: Does the organisation provide access to the information? What is the information used for and who are the recipients? This can be seen after reviewing some of the previous research in this area.

2.6.1 Wizards and privacy systems

In most current social networking sites, users can customise privacy settings and policies. They may restrict access to photographs, videos or other personal data (Dwyer et al. 2010). Several techniques are available to simplify systems used to select privacy settings. Some ideas have come from work with filtering systems. Schafer et al. (2007) defined collaborative filtering as a process of filtering based on opinion. For example, the latest movies may be sorted by evaluation, and each movie may be ranked (1–5 stars). Any user can input a ranking, and the overall opinion will be calculated and displayed. Recently, several websites have used this approach to optimise their sites by presenting the most important news based upon user evaluations. Such sites can suggest other information that users might like to view. Three types of collaborative filtering systems are recognised.

- Recommended items. If users like an item, the system will present other similar items for evaluation and possible purchase. For example, Amazon suggests items similar to recently purchased items.
- Predicted items. Specific items of interest are identified by calculating predicted ratings based on user input. This system is more popular than the recommendation system.
- Constrained recommendations. The items shown come with constraints, for example, a list of all movies suitable for children.

In evaluating a "recommender" system, questions such as the following are important: Does the system work? Are items that meet average ratings indeed recommended (Schafer et al. 2007)? As an example of the use of a recommender system in the privacy context, Abdesslem et al. (2011) explored mobile location sharing. The system used the recommender technique to control personal information ("Where am I now"?) based on the collected behavioural data of friends. The system allows users to disable the location service during specified times (for example, at night) and to hide location data from parents.

Toch, Sadeh and Hong (2010) suggested the development of a wizard allowing users to decline to share their locations with others. For example, on a university campus, a user can allow some other users, but not all, to locate him or her, then or later. Further, Shehab, Mohamed and Touati (2012) developed a privacy system enabling a user to choose different privacy settings for each friend. A user can allow or deny his/her friend access to some personal data. The system was about 90% effective, but the list of friends studied was small and it is worth investigating whether this system would work if a user has a large number of friends.

As an example of a privacy system, Gorp et al. (2012) suggested another privacy system that provides patients with more authority for sharing health information records with others. The main idea of this suggestion is to use a cloud-based system that works to develop the current patient health records systems and make the user an essential element in this system. Furthermore, Enck, Gilbert and Chun (2010) warned about the challenges regarding the privacy of sensitive information on smartphones and suggested a framework that allows users to monitor what happens to all the information handled by a third party (mobile applications). They summarised them in four points.

- Smartphones have resource limitations especially for tracking systems that track heavyweight information for security purposes such as Panorama (a program to detect the malware files in the system), which make it a constrained resource.
- Distrust of the use of third-party applications from accessing sensitive information.
- Third-party applications can share information without monitoring.
- The dynamic nature of the context-based privacy-sensitive information increases and the level of difficulty in identifying whether information has been sent or not.

The authors suggested a framework called TaintDroid to monitor the sensitive information that is based on the integration of four levels (variable, message, method and file levels) in Android’s virtualised execution environment. The results showed that using TaintDroid can provide more security services for identifying the misbehaving applications that transmit sensitive information through the web.

However, the sharing of location information is another important part of internet personal information privacy. Most of the latest models of mobile devices contain a built-in GPS system. This system can detect the location coordinates and users are able to use these values for different purposes. Several companies offer several applications that let users track the location information of other users (e.g. Latitude, Locaccino and Find My Friends) or let users share their location information with others (e.g. Facebook and Whatsapp) (Wilson et al. 2013). Some of these applications may create a source of concern for users. A study carried out by Consolvo et al. (2005) with 16 participants related to examining the relationship between sharing locations and social relations indicated that the responses of the participants focused on who was requesting their location information, what level of location information was being requested (e.g. country, city only or location coordinates) and why the requester needed such information. Wilson et al. (2013) proposed an approach for measuring the satisfaction of users on the difference tools for controlling the privacy settings of sharing locations. They divided the participants into two groups based on the method of use for these tools, and both of them used a wizard for this experiment (profile wizard or rule wizard). The first group used the wizard to select one profile from pre-existing sharing locations profiles, and the second group used the wizard to create rules directly without exposing these profiles. After receiving feedback, the authors worked to evaluate the results and they arrived at this conclusion: simplicity in the design can influence the control procedure for selecting privacy settings, which in turn impacts users’ satisfaction level.

2.6.2 Design of privacy systems

In social networking, the concept of privacy is divided into several sub-concepts, all of which focus on attack and defence (Soryani & Minaei 2012; Fig 2.12). It is important to assist users to set privacy policies. This allows them to know who is seeing their personal data and to control data visibility. Users should also be informed of their privacy rights and the consequences of leaking personal information.

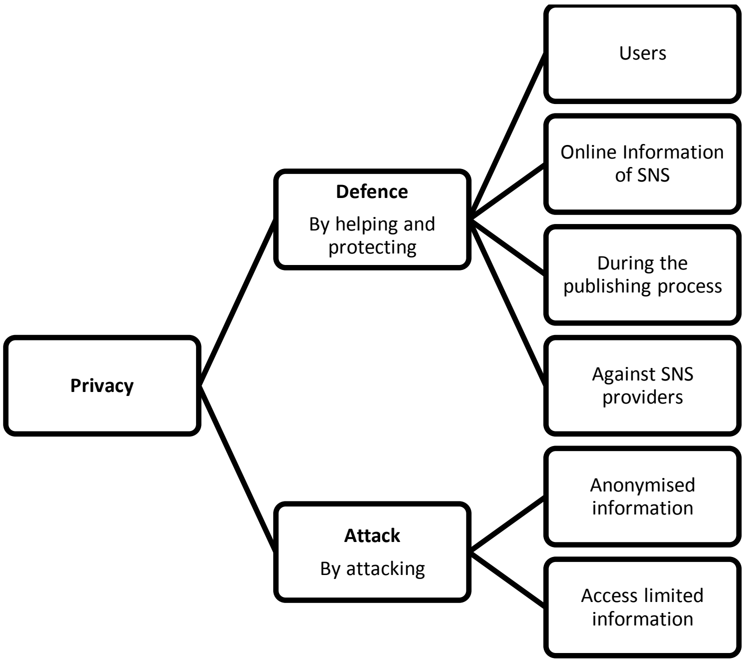

Privacy
Defence
By helping and protecting
Attack
By attacking
Users
Online Information of SNS
During the publishing process
Against SNS providers
Anonymised information
Access limited information

Figure 2.12. Privacy components and ramifications.

Several privacy systems have been designed to protect personal information. For example, Bekara, Kheira and Laurent (2010) developed a framework enhancing privacy issues in identity management by introducing a middle-ware privacy level to give users more control of personal information. The new level could be set by users. The simplicity of some network tools, such as the addition of friends, uploading of photos, or commenting, has increased users' chance of (accidentally) adding anonymous friends (Staksrud et al. 2012). These authors found that use of privacy settings could reduce such risks. Further, Kolter and Pernul (2009) emphasised that design simplicity, particularly of the interface and tools of a privacy program, allowed users to optimally protect personal information. These authors used red, yellow and green to indicate high-, medium- and low-level privacy.

One of the most famous examples of using wizards for controlling privacy settings is Locaccino (2013), which was designed by Locaccino Mobile Commerce Lab at Carnegie Mellon University. It works on all types of internet mobile devices that run on iOS or Android operating systems and is used to control the process of sharing location. The difference between Locaccino and other sharing location applications is that Locaccino provides users with more authority for sharing location details with others. It is distinguished from the others by providing users with two different types of wizards to control the process of sharing location details. The first type is called a profile wizard and the other one is a rule wizard. The basis of designing these types is to set a user as an administrator of all actions that take place involving location information. A rule wizard system has been designed to allow users to create different rules related to who, when and/or where to share, and to review the parameters before sharing information (Figure 2.13).

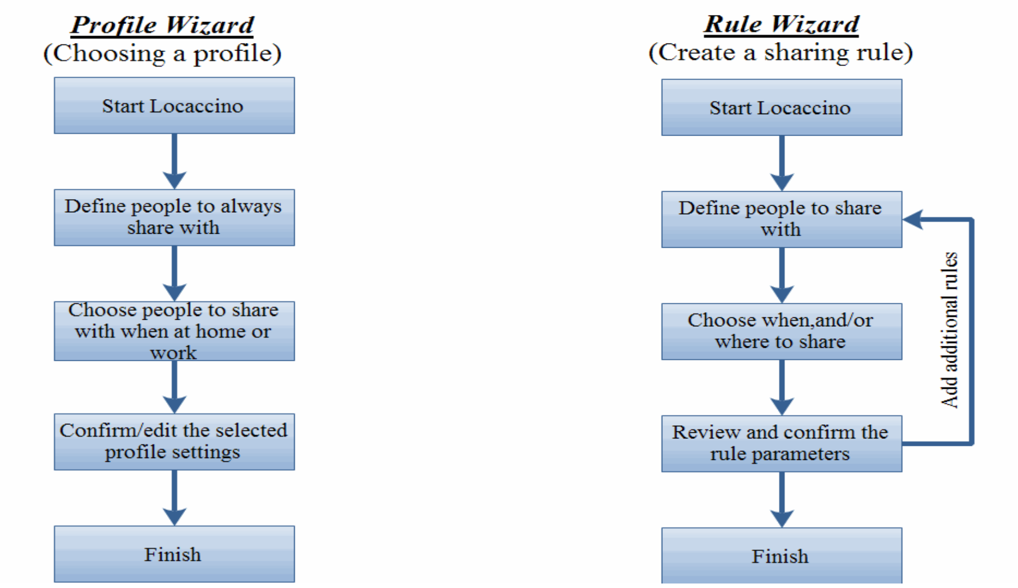

Profile Wizard
(Choosing a profile)
Start Locaccino
Define people to always share with
Choose people to share with when at home or work
Confirm/edit the selected profile settings
Finish
Rule Wizard
(Create a sharing rule)
Start Locaccino
Define people to share with
Choose when,and/or where to share
Review and confirm the rule parameters
Finish
Add additional rules

Figure 2.13. A comparison of the structures of the rule wizard and the profile wizard.

On the other hand, Figure 2.13 shows that the profile wizard guides a user to the process of selecting a profile to apply when sharing location information. It is based on two main tasks: identifying the people with whom a user wants to share location information and identifying when s/he wants to share such information, e.g. sharing this information when s/he is at work (Wilson et al. 2013).

Moreover, Toch et al. (2010) summarised the design of the Locaccino user interface as a web page or mobile application that facilitates the selection and creation of privacy rules for sharing location information by providing secure access to third-party applications. Moreover, they pointed out that a user can define the time and the place to initiate the sharing of location information by creating rules that answer the three questions (related to friends, time and locations): "Who can access the location information?", "When do users have to see the location information?", "Where will that information will be shared with users?".

As seen from this chapter, protecting the privacy of personal information, especially in social networking sites, has become an important research area that needs more research and development of applications to enhance the level of privacy protection. While the existing privacy models have solved some privacy risks, they are inadequate for many aspects of the rapid development in social networking sites. This can be seen in the differences of the used privacy models and the risks that were caused by the weakness of some privacy policies. With the increase of these sites, the difficulty and the features of controlling privacy settings could lead the user to neglect the management of the privacy policies for all these sites. This neglect could cause a leakage of the user's information and set his privacy at risk. Therefore, this study focused on designing a framework that facilitated the process of controlling personal information privacy settings through internet mobile devices and minimised the risks resulting from distribution of personal information details over many websites. It also works to unify the privacy models among these sites to increase the level of the user's awareness about the shared information in each site.

2.7 Conclusion

In this chapter, a number of topics were reviewed that related to this study. In the beginning, this study dealt with the evolution of web services and the rapid spread of social networking sites. A background was provided about the current competition between social networking sites and distinguished the types of services provided. The issues related to internet privacy and the risks resulting from sharing personal information over the Internet were also discussed. In addition, this chapter showed some implemented security procedures for one of the famous financial sites (PayPal), which is interested in protecting the privacy of users’ personal information and how this site allows other sites to obtain permission to gain access to such information. While the main idea of this study is to facilitate the process of controlling privacy settings through mobile devices, the widespread use of internet mobile devices was discussed, and the recent research results and the expected forecasts for the development of sites’ content to permit mobile phone browsing were reviewed.

However, the positive relationship between the growth in the use of internet mobile devices and the number of social networking sites requires different actions to be taken by site developers to enhance their services. The distribution of personal information details through the web requires site developers to create new models, applications or systems to protect users from misusing their details and take into account the suitability of mobile devices. Few empirical studies have focused on developing privacy applications for internet mobile devices, but most of them have focused on sharing location privacy. This research discusses another security issue related to protecting users' personal information by developing a new framework that works to enhance privacy awareness. It does this by decreasing the process of distributing personal information details through the web while attending to the suitability of the designs for internet mobile devices.

Chapter 3: Conceptual Model

3.1 Introduction

This chapter describes in detail the theoretical support of the suggested framework for this study. The theoretical support in this study is used to argue the theoretical design of the proposed framework with other privacy models. It reviews the privacy frameworks for protecting personal information in online systems from other studies. Describing different access control systems can help to explain the purpose and design of the putative framework. Several access control models and systems are described in this chapter, such as: Discretionary Access Control (DAC); Mandatory Access Control (MAC); Role-Based Access Control (RBAC); Access Control List (ACL); Usage Control Model (UCON) and Remote Authentication Dial-In User Service (RADIUS). Moreover, this chapter will explore the research question and describe the conceptual model design for this study. It will also discuss the hypotheses that arise out of this study.

3.2 Privacy-Aware Access Control Models and Systems

There are several security solutions available to overcome the privacy concerns associated with personal information details. For instance, the use of cryptographic technologies can secure the transmission between different terminals via an insecure medium through the use of Public Key Infrastructure to encrypt and decrypt messages (Demuynck & Decker 2005). While these solutions work to transmit data confidently, they do not address the issues of who has access to the data at the receiving and sending ends, or what kind of data should be transmitted.

Among the security solutions there are many developments that can enhance the integrity and confidentiality of data. Access control models represent one of these solutions that help to limit access processes to users' data and files (Park & Sandhu 2002). On the other hand, these developments are still not sufficient to meet the all the requirements of personal information privacy, such as those needed for electronic health records (Finance & Medjdoub 2005). Most of these models have been designed or modified to satisfy the authorisation requirements of the organisation, not for customers’ concerns.

The limitations in the previous solutions encouraged developers to overcome them by designing different access control principles and standards. DAC, MAC and RBAC are examples of models that work to overcome the limitations found in their processes. DAC is the first model that was introduced to secure access to information based on the authority given by the user. MAC is the second access control model that provides an authentication classification on objects (users) and subjects (files). Finally, RBAC is the third model that lets users set different rules and policies to gain database access (Jin, Krishnan & Sandhu 2012). In this section, the study briefly describes some existing access control models and protocols that present a conceptual data model to simplify the understanding of the work for the suggested privacy-aware access control model.

3.2.1 Discretionary Access Control (DAC)

Discretionary Access Control (DAC) is a means of restricting access to objects based on the given identity of the subject (Ferraiolo & Kuhn 2009). Ferraiolo and Kuhn (2009) summarised the modus operandi for DAC as follows: The object owner creates rules for accessing the object, determines which operations can be performed on the object and decides which subjects are allowed. These rules will be implemented through Access Control Lists (ACLs). The operating system should be built based on whether MAC or DAC functionality is present. Moreover, the level of protection in this access control model is not as high as in a MAC environment. This is due to some DAC characteristics, such as a lack of security labels, using ACLs for implementation and the object owner defining who can access objects.

This model is based on using the ACL. It is a permission system used to set different access restrictions on a specific object for specific members based on a verified permission list. It uses a matrix to set a list of access permissions for the object for each user. Each row acts as the access permission for the users, and each column acts as the object (Carmichael & Smerdon 2012; Ferraiolo & Kuhn 2009). Table 3.1 shows an example of an ACL and the accessing authority for each object.

Subject	File 1	File 2	File 3	File 4
Alice	Read, Write	Read	No Access	Full Control
Bob	Full Control	Read, Write	Read, Write	No Access
John	Full Control	Read	Read	Read, Write

Table 3.1. An example of using an access control list

When the operating system receives a request from a subject for access to objects, it checks the table to determine what objects the subject can access and what permissions the subject has for the objects.

Although this type of access control model tends to be flexible and widely used, it has two sources of weakness (Ferraiolo & Kuhn 2009; Hu, Ferraiolo & Kuhn 2006; Sandhu & Samarati 1994). The above authors describe the two sources of weakness as follows:

1- The right to access the file is transitive. For example, when Alice allows Bob to access a file for read only, nothing will stop Bob from copying the file, and Bob may then allow others to access Alice's file without having permission from Alice.

2- The possibility exists of changing the original content of the file and writing a hacking code to spy, commonly called a Trojan horse. For example, if Bob has access to write to Alice’s files, then he can modify the content and add a harmful programming code that works to destroy the victim’s files.

However, there are several studies that refer to security weaknesses using DAC in systems that deal with personal information details as shown below (Baker, Barnhart & Buss 1997).

- In a DAC system, there is no owner of data. Accessing personal information can be done by different parties. For example, in the Electronic Health Records (EHR) system that use DAC as an access control system, different parties (e.g. doctors, administration staff and patients) have access to this information (Gunter & Terry 2005).

- There is a lack of a property creating specific permissions to request access to specific data, for example, requesting an EHR from another hospital or an emergency doctor (Gunter & Terry 2005).
- Increasing the amount of personal information data in the matrix leads to difficulty in maintaining and managing processes for the DAC system (Ferraiolo, Kuhn & Chandramouli 2007).

3.2.2 Mandatory Access Control (MAC)

Mandatory Access Control (MAC) is controlled by a security policy administrator who gives each subject, such as a process or thread, specific authorisation to objects such as files or TCP/UDP ports. When the subject attempts to access an object, an authorisation rule will be applied by the operating system on the subject to determine the authorisation attributes and access specifications that are allowed for this object (Blanc et al. 2014). This model solves the issue of Trojan horses mentioned in the previous model, 'DAC', by preventing any attempt to access the file and write a harmful programming code (Ferraiolo & Kuhn 2009; Sandhu & Samarati 1994). Ferraiolo and Kuhn (2009) explained that the existence of a central authority will prevent both individuals and object owners from changing access rights to the objects. This is because the central authority is the only party that can set access decisions to the objects. This distinguishes using MAC from DAC in two main points, especially when the system security requires more observation of access processes:

- All access decisions will be made by the system, not by the object's owner, and
- The system must apply protection decisions for preventing unauthorised access.

This type of access control model can be used in several areas. Stamp (2011) pointed out that in MAC, setting interfaces and security-labelling mechanisms will help organisations to define the access policies for their data. For example, Figure 3.1 shows an example of using MAC in military security.

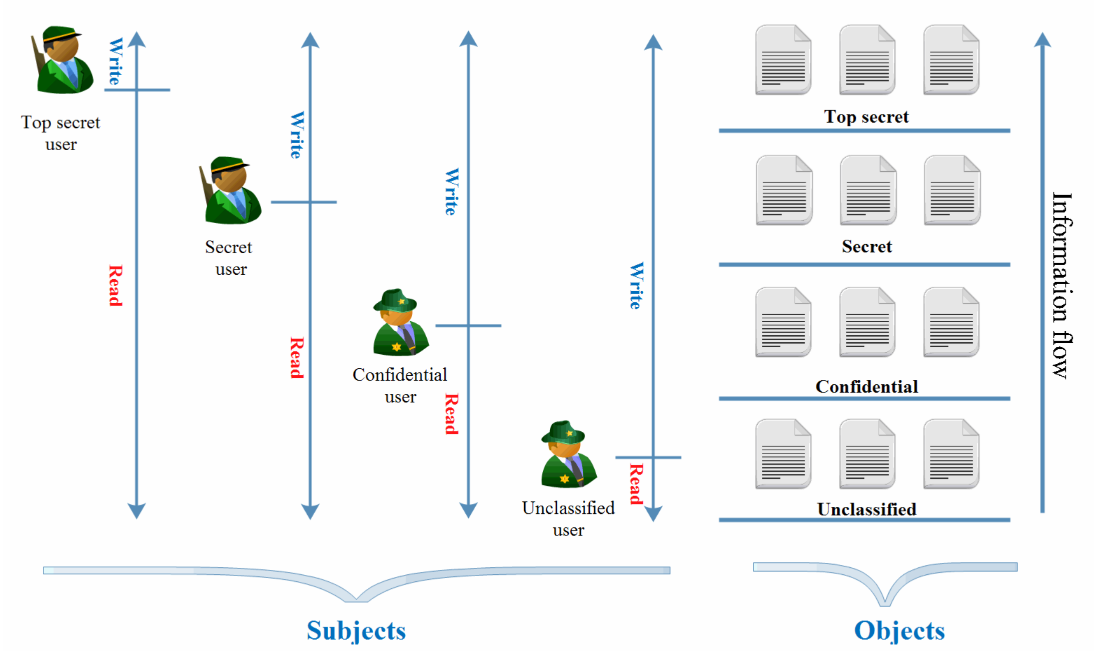


Figure 3.1. An example of using MAC in a military access control system.

In Figure 3.1, the user who is working at a lower security level is not allowed to read any file classified as a higher security level, and this rule is known as ‘no read up’. In contrast, all users at a higher security level are not allowed to write a document with a label of secret or any lower security level, and this rule is known as ‘no write down’. These access rules can be applied at all levels of the organisation. On the other hand, there are other MAC policies used in military access systems for multilevel security such as Biba Integrity models and Bell-La Padula Confidentiality (Muthukumaran et al. 2008; Bell 2005).

Although MAC provides security access, this level of controlling access to files is not enough for a high level of security. Some procedures can be added to enhance the security, such as files may be passed through secure channels and only the destination can decipher the content (Hu, Ferraiolo & Kuhn 2006).

In social networking sites, there is no typical standard of MAC security levels for allowing access to personal information details. This variously could be related to several factors that affected the design of the MAC policy such as the purpose of the site's activity, the stored information of users, the way of sharing personal information, the number of users and other factors. However, using MAC mechanisms at present is likely to be very difficult, especially with the magnitude of the content of social networking sites and the large number of users. Nevertheless, dispensing with the use of MAC mechanisms in online social networks is unthinkable, but consideration can be given to developing them to suit the current situation of social networks.

3.2.3 Role-Based Access Control (RBAC)

In RBAC, individual users are a key factor in addition to the organisation for building the system access control policies (Ferraiolo, Kuhn & Chandramouli 2007). Recently, the RBAC model has been widely used in large companies that need to control data access processes for their employees or departments. They can create new permissions for new employees and provide employees with specific authorisations for data or customise access to certain information for each department from the database.

In this model, Ferraiolo, Kuhn and Chandramouli (2007) pointed out that the administrator creates different roles and assigns access rights and permissions for roles rather than for users. All access rights for the roles will be given to the user once the user is assigned that role. This model also supports flexibility by allowing the implementation of DAC and MAC at the same time. Therefore, RBAC roles and subjects offer flexible features: a role may have multiple permissions and subjects; permissions can be set for many roles and operations; and operations can be applied for many permissions. In this case, the permissions will be grouped by role and by users, as shown in Figure 3.2.

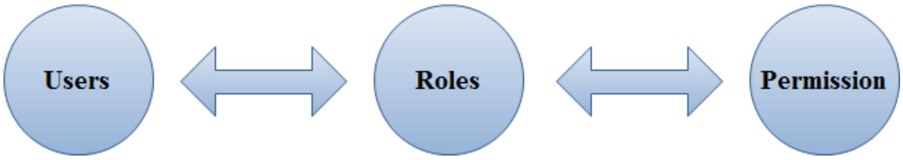


Figure 3.2. Role-Based Access Control relationships

For example, within some online sites that give users authority to control personal information privacy settings (e.g. Facebook and Twitter), the role of users can include major security operations to perform hiding or showing some items, whereas the role of the site can be limited to general privacy security. Under RBAC, users are a main part of this system, and the modification of these roles can be revoked easily and updated with new roles (Hu, Ferraiolo & Kuhn 2006).

It should be noted that giving users unnecessary privileges is not recommended and might cause problems such as unauthorised access to the system. This drives the process to introduce the concept of 'least privilege', which has been defined by Ferraiolo, Kuhn and Chandramouli (2007) as giving users the minimum privileges for performing the required functions.

3.2.4 Usage Control model (UCON$_{ABC}$)

The Usage Control model has been developed to support users' privacy in online social networks, and it differs from other models in several ways. Park and Sandhu (2010) pointed out some examples that must be considered when developers work to design a framework to support privacy in online social networks. These considerations are:

- The user may want to create a privacy role (on his/her child's profile) to allow or forbid a certain group of people to access the child's personal information page.
- The user may not want the public or a specific group to access certain information such as pictures.
- The user may want to block the receiving of certain services or information from certain people.
- The user may want a policy that works to remove social notifications.
- The user may want a policy that allows the disabling of some functions such as sharing locations.

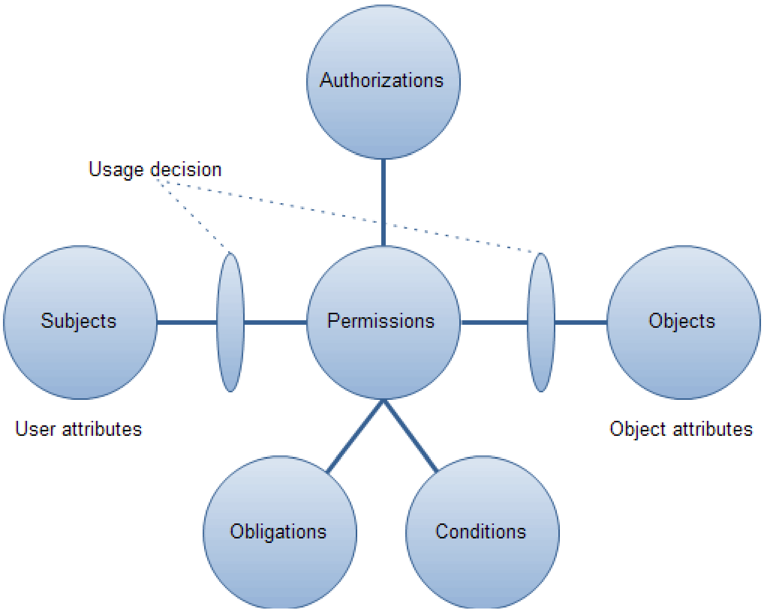


Figure 3.3. UCON$_{ABC}$ model components

These considerations encourage the system to be given a mechanism that gives users the authority to create different policies. Therefore, the UCON$_{ABC}$ model provides a way to control access permissions. In this model, three factors were added to traditional access controls: ***A***uthorization, o***B***ligations and ***C***onditions – this is the reason for its name of UCON$_{ABC}$ (Park & Sandhu 2010). According to Suhendra (2011), the concept of attributes in design refers to any information relevant for data access such as location information or the number of times that access to the resource has been allowed, and this value can be updated after an access process. The same author argued that allowing access for a particular object requires permission from the system, and this permission will be valid when all attribute values meet and achieve the access conditions. Therefore, control of permissions for accessing the resource can be created without needing to provide a full set of potential users for the system. After meeting the conditions and fulfilling the obligations, such as agreeing to terms and conditions, users can perform actions to access the object after passing the authorisation step that may apply during or before the access.

When comparing this model with the RBAC model, the complexity in the design will be noticed in the UCON$_{ABC}$ model, and it may cause a tendency to error in heterogeneous environments. Sometimes the complexity in the system requires adding an extra functionality to the database and if one function has an error it will cause a loophole or an error in the system (Suhendra 2011).

3.2.5 Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a client/server protocol and a piece of software. It is used to establish and authenticate access to a remote central server by inputting login details (username and password) for dial-in users and authorising their access requests for specific services or data (Deshmukh 2012). This allows companies to create different access policies; each policy can be applied at one administered network point (Aboba & Calhoun 2003).

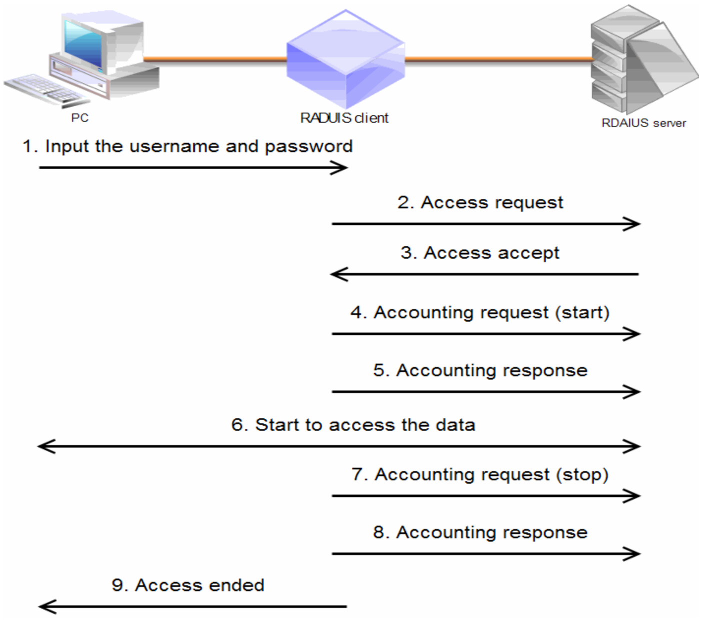


Figure 3.4. RADIUS authentication messages

As shown in Figure 3.4, obtaining authenticated access to a RADIUS server requires the user to enter the login details (username and password) in the login window. These details are transferred to the RADIUS server through the RADIUS client by the software, but first the RADIUS client needs to have access to the server. Therefore, the client sends an access request to the RADIUS server and stands by to receive the reply. If the request is accepted, then the session begins for a limited time and the user can access the specified resource. If the request is rejected, the session will not be created, or other information may be needed to confirm the login details, such as a PIN or the answer to a security question. When the session ends, the software informs the user that access has ended (Deshmukh 2012).

The RADIUS protocol has several features that provide secure communication. The first is responsibility. The RADIUS client is responsible for passing and returning all access requests between the RADIUS server and the PC. However, the RADIUS server is responsible for receiving all connection requests from the user, authenticating them and then returning all configuration information to establish the connection (Congdon et al. 2003). Furthermore, all transactions at this stage are secured; however, RADIUS offers more flexibility in supporting other methods of authenticating users (Aboba & Calhoun 2003). On the other hand, the RADIUS client can handle varying numbers of RADIUS servers by adding or removing them through the Application Programming Interface (API) (Matsunaga et al. 2003).

3.3 Research Question (RQ)

Based on the previously outlined research problem in the literature review and the information given in this chapter, the main research question for this thesis will be the following:

How can online personal information privacy issues be addressed in an integrated services scenario, via different types of mobile devices, in order that the confidence of users in the protection of their personal details from misuse can be increased?

To answer the previous research question, there are several sub-questions that will be addressed:

Q1: What framework of personal information privacy will increase the users' confidence in online systems?

Q2: What type of privacy access control model is suitable for the mobile web?

Q3: What type/types of information needs/need to be protected as private on the online systems in the area of sharing personal information details with others?

Q4: How are users able to manage and control their information privacy so as to be satisfied that their personal information is secure?

Integrate all the answers of the sub-questions will contribute to find a clear answer for the main research question and the answers for these questions will be presented in Chapter 5.

3.4 Conceptual Model

In this study, the conceptual model is developed based on the previous access control models to solve the issue of protecting users' personal information privacy, and minimise the distribution of personal information through different websites. It works to facilitate the process of selecting privacy settings through internet mobile devices.

However, the main idea of the conceptual model is based on combining MAC, RBAC and UCON_{ABC} to facilitate the selection processes and to provide different options for creating access control policies for users' data. It has been designed to satisfy most common users' needs for protecting their personal information privacy through the web. This can be accomplished by providing them with additional tools that authorise and assist them to adjust the privacy settings regardless of the number of sites. Furthermore, users of the suggested system will have various privileges that distinguish them from other systems. This is because the conceptual model was built based on others' research suggestions in different fields. These recommendations were identified as follows:

1- Related to protecting personal information details in Individual Electronic Health Record (IEHR), the National E-Health Transition Authority Ltd pointed out that the service provider should provide flexibility in options to secure a particular document (NEHTA 2008).

2- The decision to design and enforce internal security policies should be a prerogative of the organisation itself (Ray & Wimalasiri 2006).

3- Each user should have the rights to control his or her personal information items and to grant access for others to reach these items (Ardagna & Cremonini 2008).

4- Each user should have the right to hide some items of his or her personal information profile (Ardagna & Cremonini 2008).

5- Managing the access policy for the profile should be an easy task for users (Ardagna & Cremonini 2008).

In this study, the author was interested in developing a framework that works to protect the personal information privacy of users and help them to manage the access policies from different internet devices, especially internet mobile devices such as iPhone, iPad or others. As seen from Figure 3.5, the conceptual model consists of four parts (an internet mobile device, data server, wizard and various internet sites). The main idea of the study, based on the author's suggestion, is to design a system that unifies all different privacy systems in one system that allows other websites to communicate with the data server for obtaining access permission to users' personal information and to let the user create different privacy policies to identify the suitability of granting access for this site through any internet mobile device by using the Wizard system. The main goal of this suggestion is to reduce the distribution of personal information and use simple tools that suit internet mobile devices.

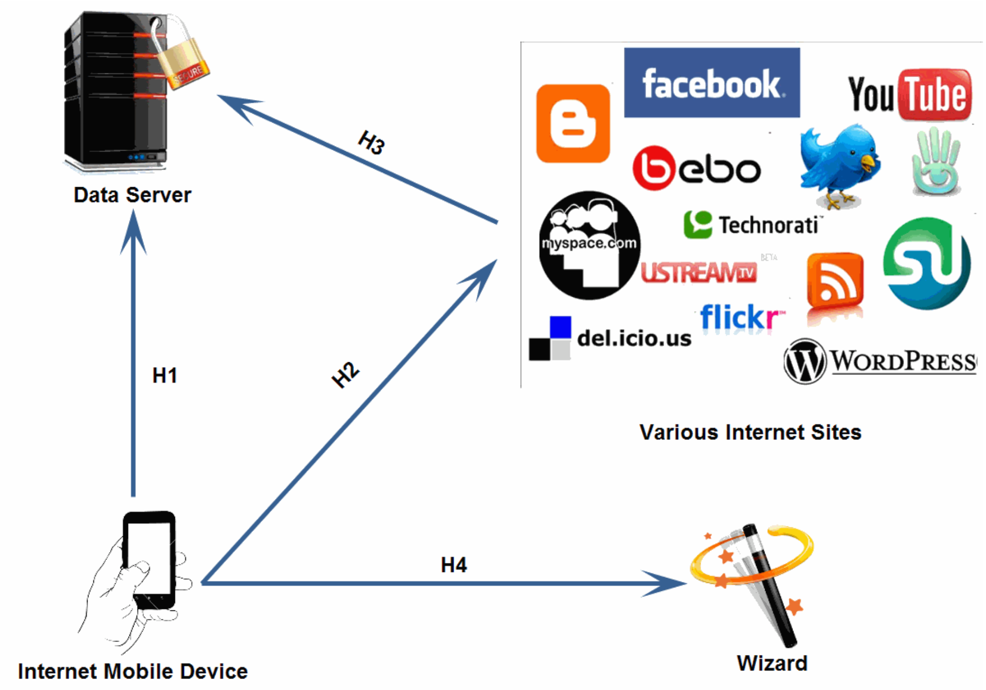


Figure 3.5. A General description of the conceptual model – Key factors of the suggested design

Hence, there are several hypotheses derived from the conceptual model:

H1: Users can manage their created privacy policies through internet mobile devices and add a new privacy policy at any time in a simple way.

H2: Users have the authority to set a privacy policy for any internet site to have access to their personal information.

H3: Each internet site has limited access to reach a user's personal information, and this was created previously by the user. It also does not have any authority to save any personal information detail, and it is only able to read.

H4: The wizard is a tool that helps users to create different privacy policies in the data server through an internet mobile device and to provide users with the ability to hide or show the items in the created privacy policy. The user will be able to use it to create different privacy policies.

3.5 Theoretical Model of the Proposed Access Control System

The aim of this section is to explain the logic of how a user can have access to the Server 1 database (data server) and obtain some information from different websites (Server 2, 3 or 4). This section also provides the scope for this system to be applied on all social network websites. There are three main objectives in designing this access control system:

- protect the user’s data from unauthorised access;
- assist in controlling the distribution process for personal information; and
- establish an access control system that fosters and facilitates the management of the sharing process without affecting security resources.

As mentioned before, there are two types of connection: 1) direct connection between the user and Server 1 to create the profile, saving personal information and adding privacy policies by using the wizard; 2) the second type of connection is creating a connection tunnel for sharing users’ personal information between other internet sites (Server 2, 3 or 4) and Server 1 based on a created and defined privacy policy.

3.5.1 Access control system for a direct connection between the internet mobile device and the Server 1 (privacy system) database

In this case, when a user needs to retrieve information from the Server 1 database, some security policies must be applied. A Structured Query Language (SQL) database is located separately from the Server 1 application to provide more security options.

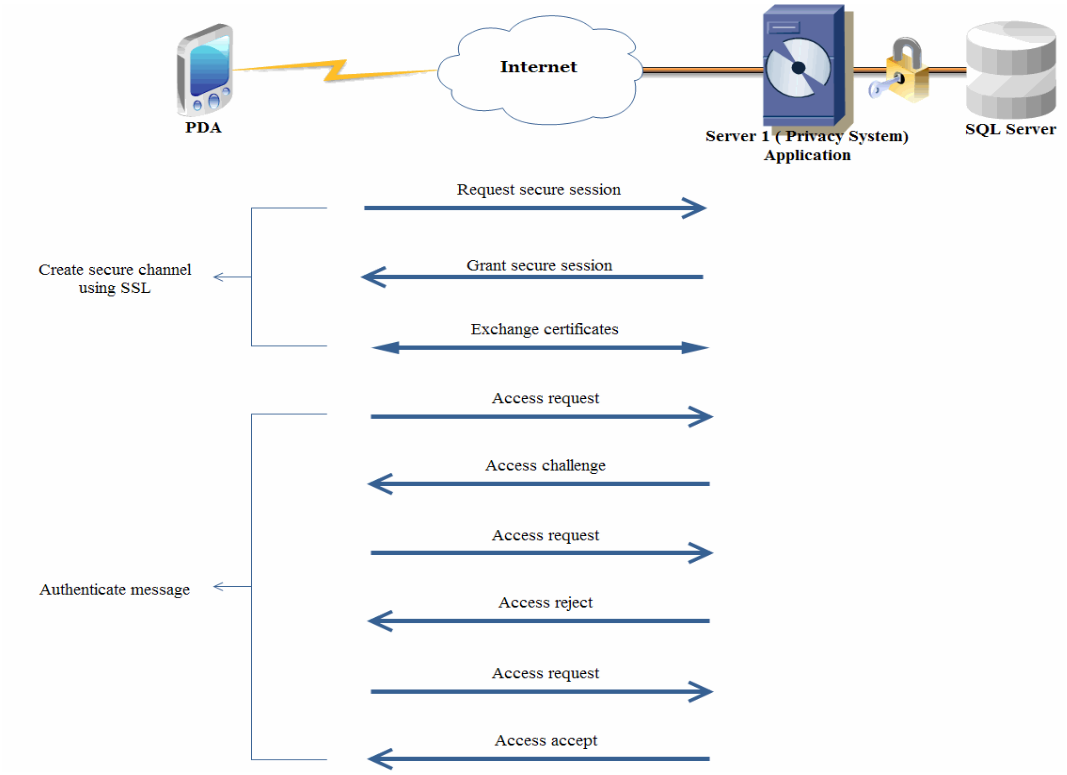


Figure 3.6. Secure connection between the PDA device and the Server 1 application

Different protocols are used to establish a secure connection between the client and the server. Secure Socket Layer (SSL) is a protocol used to secure the channel by using certificates that encrypt the communication. In this system, the author suggests using SSL to provide a secure channel between the user's device and the server application.

For secure communication between the PDA device (Personal Digital Assistant) and Server 1 in the suggested design, two steps are taken to reach the database server. First, the PDA will communicate with the server application to have access to the data. Second, the Server 1 application will communicate with the SQL server to set policies for limited access to data.

Step one includes two security processes: creating a secure channel and authentication with the Server 1 application. In the first process, the PDA will request a secure session to establish a secure channel with the Server 1 application. When the Server 1 application receives this request, it will send a certificate to the client; the client will verify the certificate, and then present their own certificate for the server. The verification process will be performed again to confirm the certificate's authority, after which the access will be protected and encrypted (Figure 3.6). In the second process, the client will send authentication information to request access after establishing a secure channel. This request will include some identifying details, such as the username and password. The Server 1 application then either rejects or accepts the request or sends a challenge request to acquire additional information such as a PIN, a secondary password or another piece of information.

In step two, a database separate from the application is characterised by a number of security aspects. The programmer can add new security rules and apply them for all users at the same time through stored procedures, triggers or the use of constraints. The programmer can also minimise costs by not installing the database in more than one place. Finally, when the database is separate and independent, the support team can easily focus on maintaining it. Furthermore, the SQL server offers a suitable environment for thousands of users at the same time. It provides a high level of protection when users update a value for an item at the same time. SQL server authentication requires setting all authorised users and defining their policies. In the suggested system, when the user wants to access data, the privacy system application will request permission to access the database from the SQL server (Figure 3.7). The SQL server will verify the login details, and, if they are correct, the server will define the policies for the user and limit access for the database based on the given policy; if there is an error, access will be denied. The SQL database cannot be contacted directly; an application must be written to allow access to it. This application may have some third-party applications or utilities that run on the SQL server.

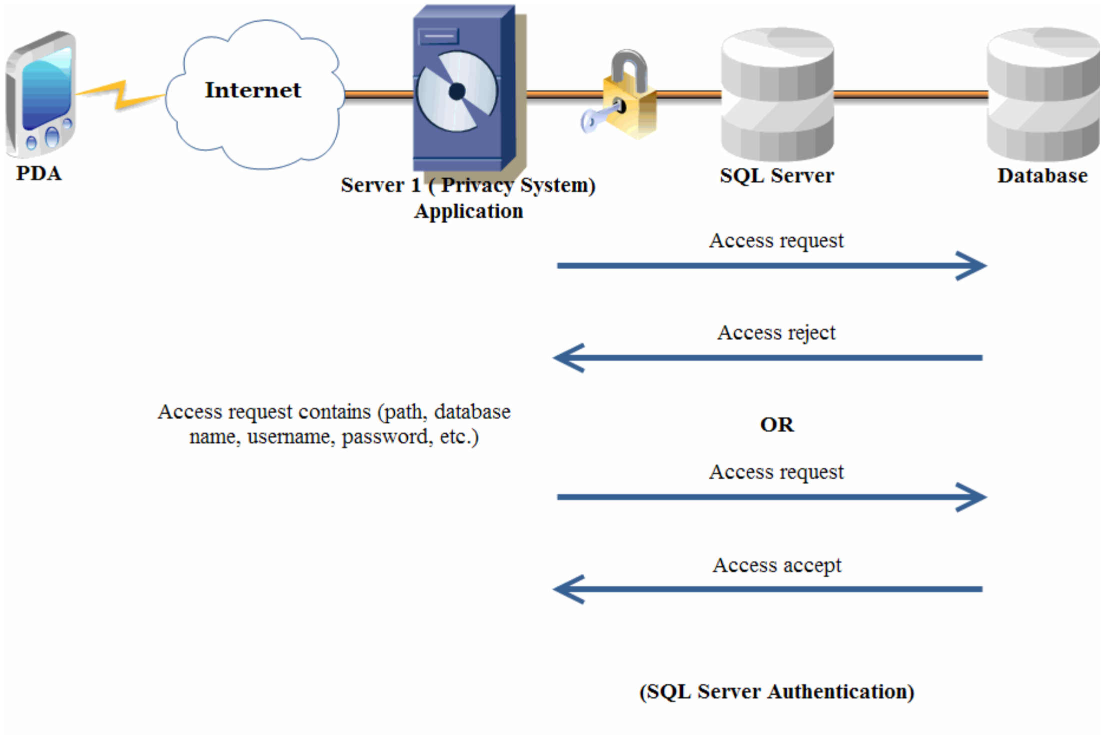

PDA
Internet
Server 1 (Privacy System)
Application
SQL Server
Database
Access request
Access reject
Access request contains (path, database name, username, password, etc.)
OR
Access request
Access accept
(SQL Server Authentication)

Figure 3.7. Secure connection between the Server 1 application and the SQL server

As mentioned before, accessing the SQL server requires a predesigned application that contains specific programming statements to access SQL data. Contacting the SQL server through the client application requires several steps and procedures. As shown in Figure 3.8, requesting data from the SQL server by using the Application Programming Interface (API) uses protocols (e.g. TCP/IP, NetBEUI) and Interprocess Communication (IPC) (e.g. named pipes or shared memory) to begin communication. Reversing these steps will enact the communication procedure from the SQL server to the client application.

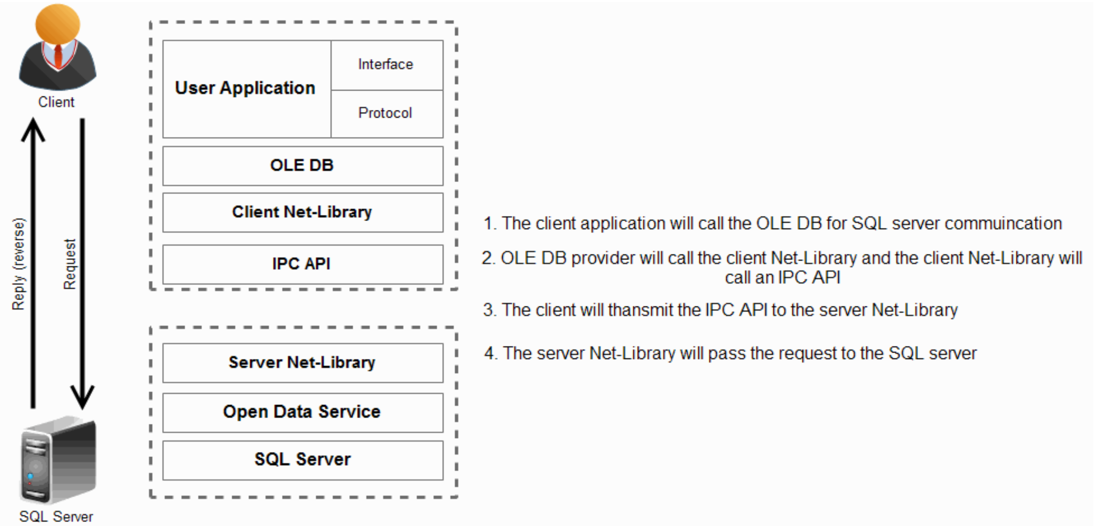
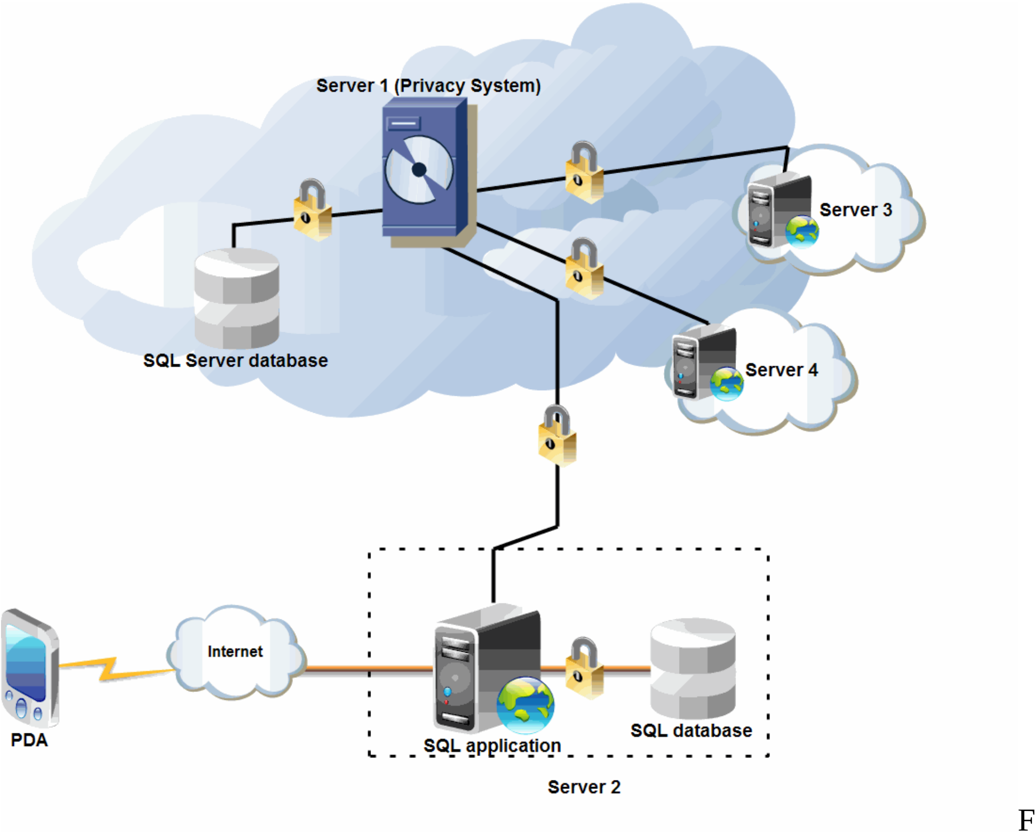

Client
Reply (reverse)
Request
SQL Server
User Application
Interface
Protocol
OLE DB
Client Net-Library
IPC API
Server Net-Library
Open Data Service
SQL Server
1. The client application will call the OLE DB for SQL server commuincation
2. OLE DB provider will call the client Net-Library and the client Net-Library will call an IPC API
3. The client will thansmit the IPC API to the server Net-Library
4. The server Net-Library will pass the request to the SQL server

Figure 3.8. Secure connection between the Server 1 application and the database

3.5.2 Access control system for multi-connections between the internet mobile device and other servers

The suggested access control system has been designed to offer more authenticity for users who use PDA devices for browsing. Figure 3.9 shows the suggested access control system for accessing personal information from the Server 1 database through other server applications. First, the authenticated access procedure between PDA devices and all other servers is similar to the access control system between PDA devices and Server 1 (privacy system), as shown in Figures 3.6 and 3.7. Two main steps must be performed before accessing the database: creating a secure SSL channel and authenticating messages. After successful authentication, the next step is to request access to data in the SQL database; the same steps will be repeated to authenticate access to the SQL database. Allowing other servers to access data from the Server 1 database through PDA devices requires several authentication steps. The system will assume that all connections between the PDA, Server 1 and the other servers have been encrypted using SSL certificates. Therefore, the next description does not include the steps for using SSL certificates between connections.



Figure

3.9. An overview of the suggested access control system architecture

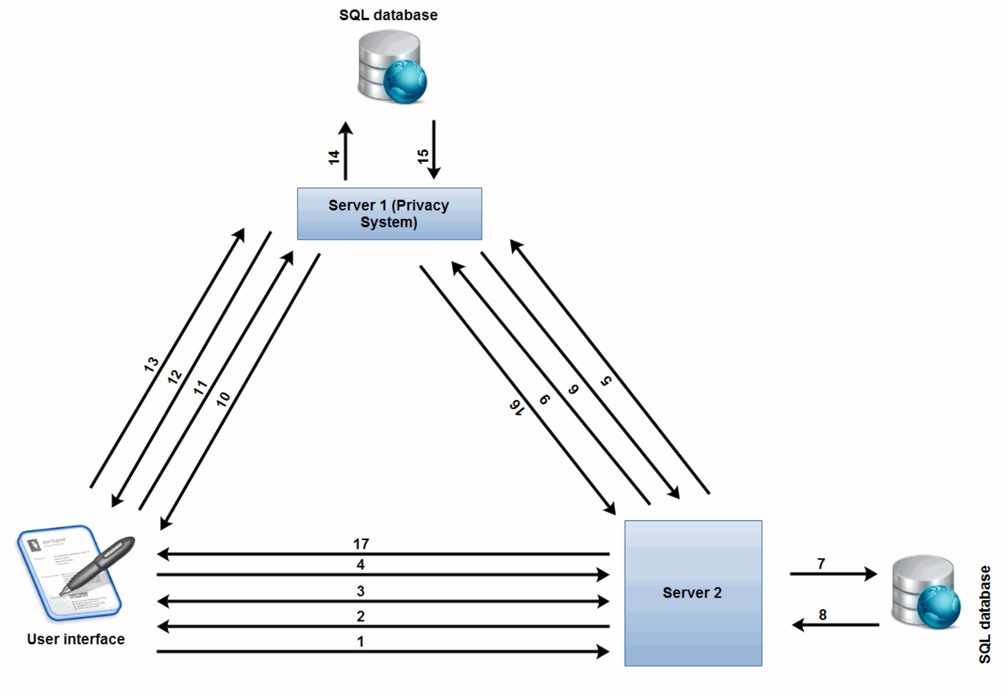


Figure 3.10. Authentication processes in the suggested access control system

The suggested access control system provides the Server 2 application with limited access to obtain data from the Server 1 database and to browse it through the user's interface. The following steps are part of this system, and are illustrated in Figure 3.10.

1. The user will send an access request to login to the Server 2 application from the user interface.
2. Server 2 will send one of three possible replies: accepted, send a challenge or rejected. If the request is rejected, the connection will be ended. If more information is needed, such as a PIN or a security code, Server 2 will reply with a challenge. If the access request is accepted, the system will perform the following steps.
3. The session will start.
4. The user will request access to data from the Server 1 database through the Server 2 application.
5. Server 2 will send an access request to the Server 1 application.
6. The Server 1 application will reply to the request with identification details for the Server 2 user.
7. The Server 2 application will request access to these details from the SQL database.
8. The SQL database will reply to the access request and authorise the Server 2 application to access these details.
9. Server 2 will send these encrypted details to the Server 1 application.
10. Before giving the Server 2 application authorisation to access data in the Server 1 database, the Server 1 application will send a request directly to the user to confirm access to the Server 1 database (username and password).
11. The user will reply to the request with login details.
12. After a successful login, Server 1 will request the user to define the access policy for Server 2.
13. The user will define the policy and reply to the Server 1 application.
14. Server 1 will save this policy in its SQL database and request the information that has been authorised to be shared with the Server 2 application.
15. The Server 1 database will accept the access request from the Server 2 application to access information.

16. Server 1 will transfer the encrypted access request to the Server 2 application.
17. The Server 2 application will send a reply to the user and display the authorised personal information.

3.5.3 Proposed architecture

This section presents the proposed access control architecture for the suggested system. The architecture is semi-automatically managed and requires specific actions from the user to ensure authorised access to data. As shown in Figure 3.11, the system has been built on three different layers: user interface, management and security. Each of these layers performs specific tasks.

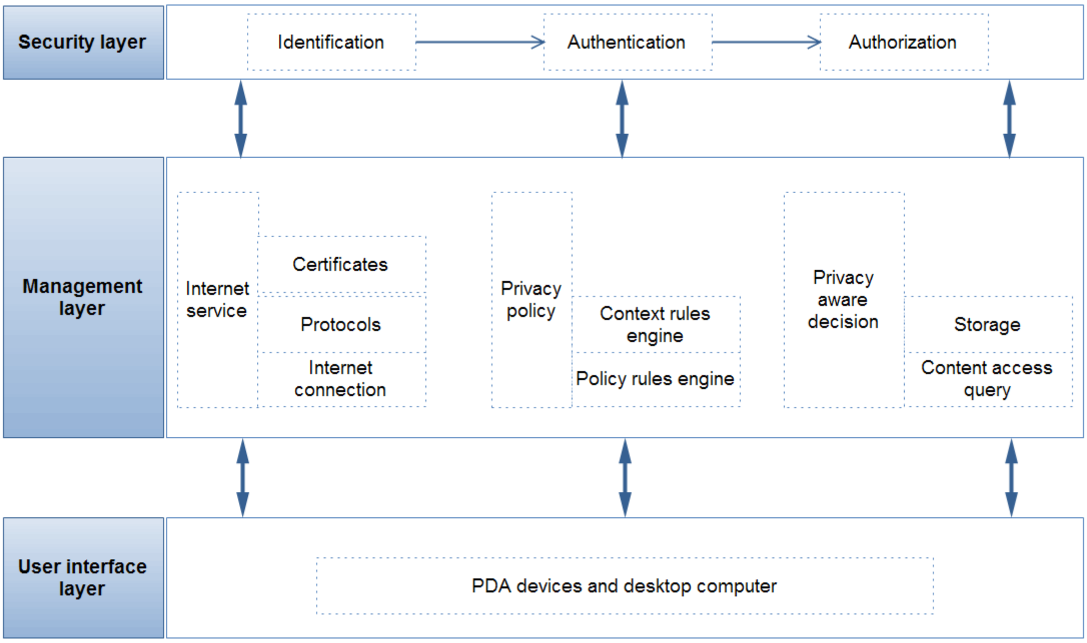


Figure 3.11. Proposed access control architecture

User interface layer. This layer captures all user actions and selections and passes them to the management layer. It provides users with a basic element of interaction with the system. The interface layer allows users to perform the following actions:

- Access the application using a mobile phone with internet access by obtaining permission from the service provider to browse its data and data from other servers.
- Browse results from requests to access data.
- Enter authentication information for servers.

- Control his or her profile and amend the privacy options by granting permission to others.
- Choose the security services available in the application, such as adding new privacy policies or editing current privacy policies.

Management layer. This layer represents all the architecture components and provides connectivity, storage and privacy processes.

a. Internet service consists of different web services and protocols offered by the internet provider and facilitates the connection between the user and other servers. In addition, it is responsible for creating secure channels between all connection parties by sharing certificates.
b. A privacy policy is a set of rules and procedures used to adjust a specific procedure, reach the database contents or add new content. It manages requests made by the user through the user interface and facilitates the process of adding new privacy policies or performing other actions.
c. A privacy-aware decision system controls all actions, such as reading, writing, updating and other processes. The control process is based on the results of the privacy policy and the information received from the security layer. It gives each server limited access to the data content based on the privacy policies created.

Security layer. This layer represents all the security procedures that have been suggested to provide more security for the system. It includes three stages to ensure adaptive security policies: security identification, authentication and the authorisation process.

a. Identification occurs after a secure channel between servers is established. It requires the user to identify him- or herself by providing public information such as the username or ID. The value of the identification variable should be unique to avoid duplication between users.
b. Authentication is the second stage of credentialing. It requires entering private information to complete the authentication. This information includes passwords, token devices, fingerprints or any other information that can confirm the identity of the user. Furthermore, applying more than one credential mechanism provides strong authentication.

c. Authorisation is the process of defining the authority of the user to access data based on predefined policies and to perform the allowed operations for the website.

Users can be authenticated with different credentialing methods; here, we will discuss some suitable methods that can be used with internet-accessible mobile devices.

1. Passwords: This method is one of the most common security authentication methods. It can be applied on all types of internet mobile devices. It is a string of numbers, characters and other symbols that constitute a secret key for the login process. There are several recommendations for users when selecting passwords including: using a combination of characters, numbers and symbols; creating a password that is not short or easily guessable; and changing passwords frequently.
2. Fingerprints: Some internet-accessible mobile devices, such as the iPhone 5s, use fingerprint technology as an authentication tool (Apple 2013). iPhone 5s users can log in to the Apple Store by using their fingerprints rather than using a username and password. Apple has not dispensed with using the classic authentication method (username and password), but this new method has been added as a supporting tool for the authentication process. This technology offers more flexibility and choices for authentication; it also reduces the time needed to access the database server.
3. Token devices or one-time passwords: These devices are used to generate a code or number to confirm the login process to the system. To use this service, a user must receive permission from the service provider by providing the user with his or her own authentication device or application (Billings 2009). A token device has an LCD screen that displays the generated number; the user is required to type that number into the login page. These numbers change from time to time based on the clocking mechanism. Recently, different banks around the world have offered token applications for internet-accessible mobile devices to authenticate users in the bank's database. Banks using these applications include the Abu Dhabi Commercial Bank in UAE and the National Commercial Bank in Saudi Arabia. (These applications are available in the Apple Store under the names ‘ADCB Mobile Token’ and

‘AlAhliToken’.) Verifying an internet-accessible mobile device as a token device by using an application increases the authentication strength.

3.5.4 Characteristics of the proposed access control system compared with other mechanisms

The proposed access control system has two different types of data access: direct access to the server's database and access to the Server 1 database through other servers. When the first part of the proposed access control system (direct access to the database) is compared with other access control models, some similarities and differences can been found.

First, the direct authentication scheme between the smartphone or the tablet device and the local server's database has some similarities with the RADIUS access control protocol. It needs to send an access request to obtain authorisation for accessing data, and this request may have one of three replies (accept, reject or request more identification details). In the proposed access control system, the server will be a RADIUS server, and the PDA device will be a RADIUS client. Additionally, some security components will be added to the authentication process for browsing the internet through internet-accessible wireless devices. Creating a secure session between the client and the server is an important step for increasing security levels. All authentication details and communications are encrypted by SSL certificates. Some connections between servers, as shown in the following paragraphs, need to deliver some important login details for other servers. Therefore, in the proposed access control system, SSL encryption is applied between all types of communication to provide more protection, especially for different types of wireless connection threats.

While RADIUS supports different types of devices as RADIUS clients, such as access points, remote access servers and virtual private networks, it is not an efficient method of authentication, especially with mobility (Szilagyi & Sood 2009). Users who use internet-accessible mobile devices may move between different access points and from one base transceiver station to other stations. Applying a RADIUS mechanism in a company that needs remote access permissions for their staff members or other branch offices is good choice, but it will not be sufficient for application on all internet access points around the world. Furthermore, all RADIUS clients must be configured for communicating with RADIUS servers.

The proposed access control mechanism is based on direct authentication between the internet-accessible mobile device and the server; however, with the RADIUS method, computers or wireless portable computers running a client operating system cannot be RADIUS clients (Microsoft 2013). As mentioned before, wireless access points, switches or routers can be used as RADIUS clients.

The access control list is another way to control data access. Comparing the proposed access control system with ACL, there are some similarities in the functional properties to note. ACL lets each user set access conditions for his or her objects; in the proposed access control system, the user is able to create different access policies for each object and define who can access these objects. In the proposed access control system, the user is an administrator for all other parties and can create the list and define all object access permissions for all websites that need to access the data. Moreover, the access control list is not recommended for external access due to some disadvantages, such as the possibility of breaking the security system, the difficulty of controlling a large list of users, the need to increase the code size to check each user interface in conjunction with the increasing number of users, and the possibility that the large size of the coding may cause loopholes in the system (Samarati & Vimercati 2001; Rizvi et al. 2004).

Second, accessing a server's database through other servers requires an access control model with certain specifications. Several techniques have been used to design the proposed access control system. Different access policies have been designed to control access and use the permission list to control permissions for each site. This can be clearly seen by comparing the proposed access control model with other models.

The RADIUS agent is an access control model that works as a proxy server to forward messages between the RADIUS server and the RADIUS clients. It is a linking point between the RADIUS server and the RADIUS clients for authenticating users, which will not allow direct authentication between the server and the client to track the RADIUS traffic (Droms & Schnizlein 2005). It works as a mediator between the clients and the server. When a RADIUS client sends an access request to the server via a specific port, the RADIUS agent receives this request and extracts the authentication information, such as ID or username. After extracting this information, the RADIUS agent transfers the request to the RADIUS server to check the authentication request and send acceptance or rejection to the agent. The agent evaluates the response and forwards it to the client. When the authentication is accepted, the RADIUS agent adds the corresponding entry to the user map (a list of user details such as usernames, passwords and IP addresses). When the user map is updated, the RADIUS agent sends the usernames and IP addresses to the filtering service. This service assigns policies for users to log in to the server (Websense 2013).

Several differences exist between the proposed access control model and the RADIUS agent technique with regard to accessing the database server through other servers. In the proposed access control system, there is no agent responsible for filtering the request services and saving them into a user map like there is in a RADIUS agent. As mentioned previously, when a user requests access to the Server 1 database through other servers, a direct connection will be established between the PDA device and Server 1 using the other server's window to authenticate that server for accessing the Server 1 database.

The other server does not save any authentication details from the Server 1 database, but it does send its own user identification details to Server 1 to let the user create an access policy for the server. Some identification details are saved in the other server’s database (that are provided from Server 1) to be used only to identify the policy given from Server 1. For example, Alice gives Server 2 permission to access data from Server 1 by selecting or creating a specific privacy policy (after a successful authentication process between Alice and Server 1 through Server 2’s window). Server 1 provides Server 2 with identification details, such as the name of the privacy policy and the identification number, to request this privacy policy in the future. When updating the status, Server 2 will only be able to update this information after contacting Server 1 and receiving permission for the update process from Alice.

The proposed access control system is a mix of ACLs and the RBAC model. The similarity with ACLs is in the use of lists to control all the objects' access policies. In the Server 1 database, a table saves different privacy policies that have been created, and each object included in the table has a different access policy status. It is easy to find the differences between them by comparing Table 3.1 (in section 3.2.1) and Table 3.2. In Table 3.1, each user is a row in the table, and one access permission is set for each object; in Table 3.2, each user has many rows and different access permissions can be set for each object. In addition, each row in Table 3.2 acts as a different privacy policy for the user.

Privacy policy	Object 1	Object 2	Object 3	Object 4
Policy no. 1	Read	Read	No Access	Read
Policy no. 2	No Access	Read	Read	No Access
Policy no. 3	Read	No Access	Read	Read

Table 3.2. An example of using a list to identify a privacy policy for the user

Furthermore, the similarity with RBAC is found in the creation of different access roles. In the proposed access control system, every user is an administrator. The user can create all access rights and permissions for his or her personal information and set an access value for objects. In addition, the user can authorise other servers for accessing data by applying a specific role for each server. This can be done after completing the authentication acceptance and verification processes. The system applies a specific access role for this server based on the values received from the user.

3.6 Conclusion

Different access control models are used to control data access permissions, and several privacy models have been applied for most internet websites. This chapter reviewed and discussed several common access control systems used for protecting users' privacy. As the research is related to protecting the privacy of users' personal information, this study presented a review of several types of access control models. These models were Discretionary Access Control (DAC); Mandatory Access Control (MAC); Role-Based Access Control (RBAC); Access Control List (ACL); Usage Control model (UCON) and Remote Authentication Dial-In User Service (RADIUS).

Building on the information that has been provided in the literature review in the previous chapter, the main research question was provided as well as the derived sub questions. This encouraged the study to establish a proposed model that works to solve the identified problems.

The proposed access control model consists of two types of connections that were based on four hypotheses in the design. These connections are 1) direct communication between the user interface and the server's database and 2) communicating with the Server 1 database through the other server's window. In addition, the architecture and all the connection steps between the system’s components are shown. Some current access control models and techniques that are used for authentication and authorisation processes were presented. These models and techniques were summarised to show the differences between them. The proposed model was compared with the current access control systems. Some differences exist between them, but some similarities are present in the methods for filtering access permissions. The main idea of the proposed access control system is somewhat similar to the ACL, RBAC and UCON models. The proposed access control system was developed to provide more flexibility for users in controlling objects through different internet websites. Therefore, there is no fixed standard for controlling privacy policies and accessing permissions; however, developing different access control models will allow users and administrators to control the process of accessing their data. The next chapter describes the methodology, algorithms, and all other operations used to test the hypotheses and to design the proposed access control model.

Chapter 4: Research Design and Methodology

4.1 Introduction

In research, there are several types of research design: quantitative, qualitative, applied, analytical, predictive, exploratory, deductive, inductive and basic research (Collis & Hussey 2009). All types of research have a unifying theme that require researchers to focus on two main questions (Kripanont 2007). These questions are what types of methodologies will be used in the research and how the researcher will justify the selected method to underpin the assumptions of the study (Crotty 1998).

In this study, the methodology was selected to achieve the essential research objectives. This chapter also presents in detail the justifications, uses and design of the selected research type. As this study contains four main steps to achieve the objectives, different stages were implemented. The first stage was collecting some necessary data through a survey to design the next step. The second stage was coding a wizard system based on the previous data. The third stage was another survey about implementation of the system, and to measure its success. The last stage was coding and testing the proposed privacy framework.

This chapter discusses all materials used to achieve the objectives. It re-states the research objective and specifies the research stages for designing the proposed framework. It also presents the survey populations, the sample procedures for the two surveys, the data collection and the data analysis. This study is guided by the following question: given the high participation in each online social networking site and personal information distribution processes, how can the user control the process of distribution of his or her personal information, taking into account the increasing number of social networking sites and the use of Internet mobile devices for browsing? Within this chapter, the development of a privacy framework that is relevant to addressing the fundamental research question is discussed.

4.2 Objective

The broad objective of this study is to design a privacy framework that facilitates the method of selecting privacy settings. The framework will be compatible with Internet mobile devices and offers a simple way to control the process of distributing personal information details through the Web. To achieve this goal in a meaningful way, the author has set the research questions as follows:

i. What framework of personal information privacy will increase the users' confidence in online systems?
ii. What type of privacy access control model is suitable for the mobile Web?
iii. What types of information need to be protected as private in online systems in the area of sharing personal information details with others?
iv. How are users able to manage and control their information privacy to be satisfied that their personal information is secure?

Therefore, the main research objectives for this study that underpin the research sub-questions are:

- To propose a privacy-aware framework supporting most Internet mobile devices to increase the confidence of mobile device users.
- To develop a privacy model that is suitable for controlling personal information settings through Internet mobile devices.
- To develop a privacy management model to support users' ability to manage their personal information.
- To design a prototype system to verify the framework and models.

4.3 Research Design

Research is a process of collecting and analysing data to arrive at solutions for a problem by taking a series of rational choices (Sekaran 2006). This study consists of five phases, which are identical to the research methodology phases used by Vaishnavi and Kuechler (2004), as shown in Figure 4.1.

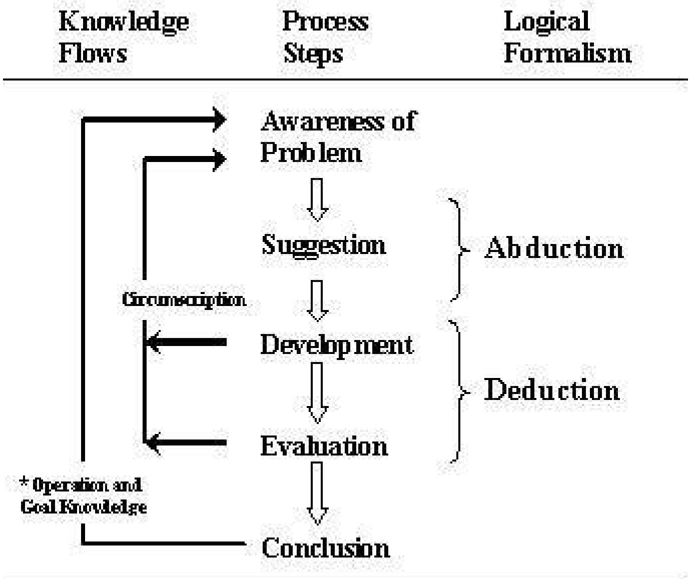


Figure 4.1. The General Methodology of Research Design (Vaishnavi & Kuechler 2004).

1) Awareness of the Problem

This phase focuses on awareness of the problem and identifies the research concepts. This can be accomplished by analysing scientific experience and expertise, by examining new developments in the industry and by reading research related to the field (literature reviews and other information). Therefore, the output for this stage is the proposal, which consists of identifying the research topic and stating the research problem, taking into account the research focus at all stages of development. This stage has been completed.

In this study, as awareness of the problem increases so does the need to survey some mobile and privacy concerns before the suggestion step. This can be done by applying a survey methodology that studies the sampling of smartphone and social networking site users. Some associated survey data collection techniques will be used such as a questionnaire construction method and improving the accuracy of respondents' answers. Moreover, understanding the research problem clearly required the researcher to focus on different types of topics such as the use of smartphones or tablets, the used of social networking sites, the properties of users and privacy concerns. The target population of the study was obtained from lists of university members from two countries (Australia and Saudi Arabia). However, making decisions is the most important methodological challenge facing the researcher

(Groves et al. 2011). So, the researcher selected a quantitative survey to model and analyse the data, using scientific methods.

2) Suggestions

This phase describes the initial proposals and solutions related to the initial design, which seeks to develop or solve the problem. This phase also helps identify and solve the weaknesses that occur during the first phase by providing feedback. It is an important part of the research proposal because it offers a new scenario for solving the research problem. Thus, the output of this stage is the development of a privacy-aware framework for the mobile Web to increase the confidence of users so they can use their mobile devices and control the privacy of their personal information.

In the previous step, all survey data was analysed using IBM SPSS 19. So, this step involves the review and synthesise of the survey's results and suggests some hypotheses to design a framework to enhance privacy awareness in mobile web system. It also involves the design of the smart wizard system and the connection procedure between different servers. The final findings relating to solving these suggestions were incorporated into this thesis.

3) Development

This phase focuses on the development of the model, which can be achieved by designing a prototype model. This model requires the design of a new algorithm. As a result, the output of this phase was a new privacy-aware mobile model.

In this phase there were some suggestions to develop two applications that assist the user in controlling the privacy settings via smartphones or tablets. Two interrelated applications emerged from the suggestion phase: (1) designing a smart wizard system tool for assisting the user in setting the privacy policy and (2) developing a whole privacy framework for protecting the privacy of users' information.

The initial design of the smart wizard system was derived from the design of recommendation systems as discussed earlier in chapter two. The recommended system analyses the user's selections and then shows him some options. Therefore, the mode of action of the recommended system could be used to design a tool that suggests a suitable privacy policy for the user to be applied on his social media profile. On the other hand, the initial design of controlling access processes for personal information located in different servers was derived from the method used in the PayPal site for payment processes. As discussed in the earlier literature review, the spread of users' information may set users at risk (EDM 2014). This encouraged the researcher to develop a system similar to the centralising of credit card information in the PayPal system. In the PayPal system, the user gives other sites that have payment requests permission to collect the money via accessing the PayPal server through these sites after a successful login to the PayPal server. In the initial design the user will give permissions to other sites to access some personal information based on the created policy from the previous tool, and successful login to the main server database via different sites.

4) Evaluation

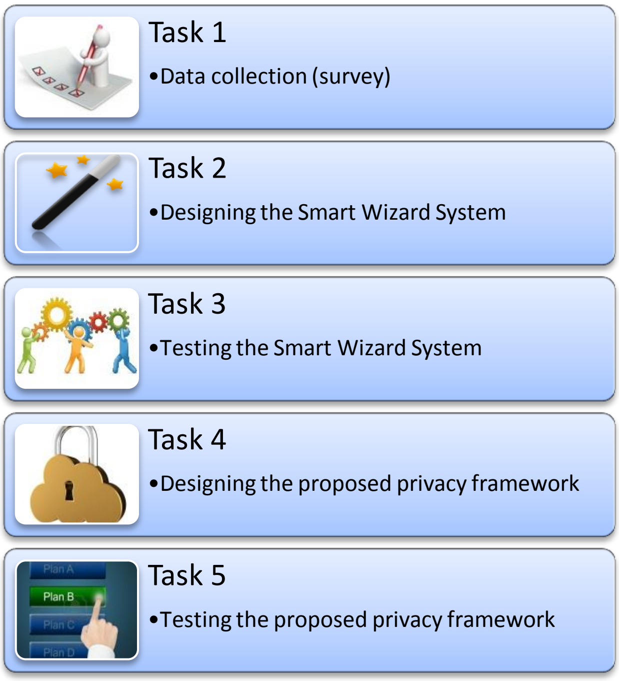
At this stage, the implementation of the model is evaluated and feedback is obtained. This stage is also known as the evaluation phase because it contains sub-evaluations that enable the researcher to assess the different parts of the model in order to track the model's processes to ensure that each part of the model accomplishes the specific role it is assigned within the framework. Furthermore, this phase contributed to proving or disproving the effectiveness of the design of both the privacy-aware framework and the model. Thus, the output of this stage contributed to the development or the redesign of the model or the framework to ensure the effectiveness of both.

Though not the focus of the development phase about the design of the framework, a brief description of the evaluation of the experimental design is necessary to understand the evaluation process and find the needed corrections of it in the future. Firstly, the evaluation of the proposed wizard tool in this study was undertaken by an implementation of it. Participants were asked to answer some questions asked by the system and evaluate the suggested privacy policy, and modify the appearance of personal information items (if needed) to suit the participant. Finally, the accuracy of the wizard tool will be calculated by using a formula. Secondly, the evaluation of the whole privacy system will be measured by implementing the system and testing access for user information via other sites, and defining which information could be accessed and which not. Several examples will be used to check the system.

5) Conclusion

The conclusion is the result of the research effort. It can be obtained after the assessment phase has been completed and after the model and the framework have been tested. Therefore, the conclusion contains excerpts and results from the four previous phases.

However, the specific methodology used to achieve the objectives proposed in the early phases include suggestion, development and evaluation. This depends upon an analysis of the framework and the model, and an explanation of whether or not the proposed suggestions for the development of the privacy model work. As shown in Figure 4.2, the methodology consists of five tasks, and each task is complementary to the others.



Task 1
- Data collection (survey)

Task 2
- Designing the Smart Wizard System

Task 3
- Testing the Smart Wizard System

Task 4
- Designing the proposed privacy framework

Task 5
- Testing the proposed privacy framework

Figure 4.2. Stages of designing the proposed privacy framework.

Task 1: the purpose of this task is to measure the importance of controlling personal information privacy settings for users, and the use of Internet mobile devices to control these settings and identify which personal information is more important for users. This step was carried out through the use of a quantitative survey.

Task 2: through the results of the previous survey, the “smart wizard” system was designed based on the answers of the participants. This system is designed to facilitate the method of selecting privacy settings through Internet mobile devices as well as other computers.

Task 3: the next task is testing the Smart Wizard System by uploading the wizard system online and asking participants to test it and set privacy settings. Participants were provided with the ability to modify the suggested privacy settings by changing the showing status for any personal information item. The system also will automatically calculate system accuracy for each participant based on the changed items.

Task 4: after evaluation and verification of the efficiency of the wizard system, the author designed a privacy framework that provides the user with more control tools for minimising the process of distributing personal information details on the Web. The Smart Wizard System was included as a main part of the privacy framework. It helps the user set up different privacy policies from different Internet devices, including Internet mobile devices.

Task 5: the last task of this research was implementing the privacy framework. In this phase, the author created different user accounts on the main server (server 1, which contains all users' personal information details and the created privacy policies), and then he created accounts on other websites and gave each site limited access to server 1 to read some personal information details by applying one privacy policy to it.

Applying all these tasks systematically assisted the author in achieving these goals:

1- The first goal of applying the first three tasks is to design a Smart Wizard System for controlling privacy settings that will increase users' confidence in using their mobile devices to adjust privacy settings.

Based on research findings from the existing literature review, which underscored the importance of privacy in the area of technology, especially regarding the protection of personal information when using mobile phones, the result of applying these tasks was the development of a Smart Wizard System that increased users' confidence in using their mobile phones for social communication and facilitated the selection method of privacy settings. Moreover, the system was designed using ASP.net as a programming languages and SQL Server 2008 to deal with databases. Databases were also used to simulate real communication between users to achieve the main goal of designing the privacy model.

2- The second goal of applying the fourth and fifth tasks is to design a privacy-aware framework.

The framework will include the Smart Wizard System. This goal works to increase the level of personal information protection and focuses on the design of a specific technique to develop an appropriate level of privacy for personal information. While the literature review notes that some techniques currently exist, those techniques need to be improved. Therefore, to build a prototype system, the following steps were needed:

- Specification of the system: This step is achieved through an analysis of the system to determine the target by conducting a case study of a sample of students before and after the design of the model. Doing so will measure the importance of privacy protection to users and identify their level of satisfaction with the prototype system. Moreover, at this stage, a case diagram is developed to provide an overview of the actors (the sample of users) and to chronicle the cases and the results.
- Implementation of the suggested model: At this stage, both the privacy model and the privacy management model are implemented, as shown in the following sections.
- Testing of the prototype system: At this point, the system is tested, and then an attempt is made to determine errors and weakness in the system. The next step is to correct the errors and to re-address what is needed to strengthen the system by moving through the previous stages once more.

4.4 Research Philosophy and Approach

In research, the concept of the "research paradigm" has become an essential requirement to simplify the idea of the research. It views the idea as a world-view to help researchers or others in understanding, exploring and facilitating the complexity of the research (Seale 1999). The logical scientific approach is another highly important factor that helps researchers to collect and analyse the research data (Creswell & Clark 2007). On social networking sites, users are the most important party to evaluate any system. Therefore, the research purposes were designed based on individuals' judgments, and this was the value of the success of the system. Wenger (2005) pointed out that communities and individuals are the target group for designing social networking sites, and these sites are basically directed to them so that they can benefit from the services.

In this case, examining the system in a statistical way was based on individual evaluations by using quantitative methods, and the findings were used for the development of the system. Therefore, the specific approach for this study is to build a framework, based on the participants' feedback, to enhance privacy awareness and facilitate the control process in Internet mobile systems. The design of the system is based on the survey results. Bryman and Bell (2007) stated that the deductive approach is based on previous findings, which are tested by using statistical methods. Therefore, designing the proposed framework was based on a statistical analysis for the results obtained from participants.

In this study, the collected data from the survey will be used to design the infrastructure of the proposed smart wizard tool. It also will be compared with data collected from other studies conducted more than five years earlier, and view and compare the awareness of users about privacy of personal information details. The study will provide valuable and unique insights into shifts in perceptions over these years. Moreover, the developed applications in this study will be tested to check the validity of the framework to achieve the study hypotheses. In addition, the final application in this study will be compared with other current applications in order to note the differences between them and check the relative success of the study.

4.5 Research Progress

Several research studies have discussed different types of privacy issues, such as location, data encryption and others. Some have presented problems related to privacy issues but have not provided any suggestions or solutions, only general recommendations. On the other hand, some researchers have designed privacy systems to protect the user’s location and for data encryption, but only Fang et al. (2010) have designed a system for selecting a privacy system. Their system, a privacy recommendation wizard for users of online social networking sites, has three levels of privacy options: low, medium and high. Furthermore, the system allows the user to classify the friend list by inputting privacy settings for chosen friends, which allows or denies them access at certain items.

This unique research has several advantages that make it different from other studies, such as using a Smart Wizard System and a centralised system for controlling the processes of sharing personal information with websites. The smart wizard tool differs from other privacy tools by the simplicity of the design that assists the user in setting the privacy settings for twenty three items of his social networking profile in two minutes or less. The current tools for setting privacy settings used the method of selecting the status of each item or a group of items. The other feature of the framework is the use of a main server that contains the smart wizard tool to create different privacy policies, and control the visibility of users' information by managing access of them without publishing more personal information over the internet. These will be discussed in detail in this chapter.

The simplified ideas for the proposed framework are as follows:

1- *The Smart Wizard System*: This term refers to asking the user some questions about hiding or showing some personal information items and predicting some privacy features related to user answers. As previously mentioned, the adopted design for the functionality in this research was based on the results of the first task. In this case, Figure 4.3 shows an example of the basic functionality of the tool.

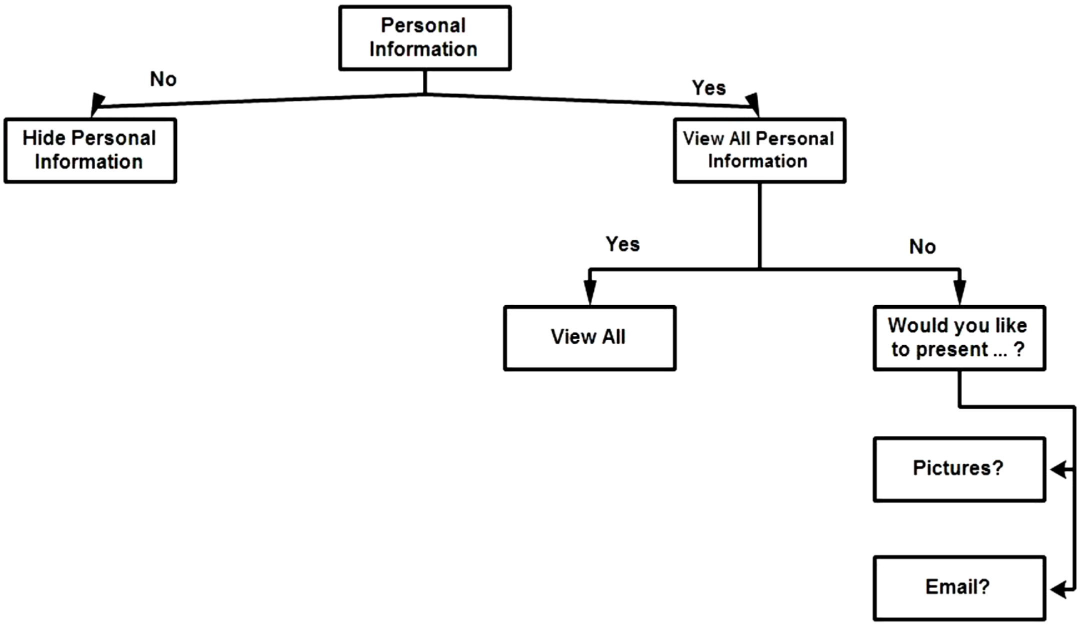

Personal Information
No
Yes
Hide Personal Information
View All Personal Information
Yes
No
View All
Would you like to present ... ?
Pictures?
Email?

Figure 4.3. The basic functionality of the smart wizard.

When the user wants to control the privacy setting properties, the model will ask the user some questions, and the design for the questions is tree-shaped, as shown in Figure 4.3. For example, the system will ask the user if he/she would like to share all his/her personal information with others or not. If the answer is yes, the system will automatically set the privacy setting; if the answer is no, the system will ask the user additional sub-questions. The system continues asking the sub-questions until the process is completed. Once the system completes the selection of automatic settings for the user, accuracy will be measured by comparing the privacy needs of the user and the results of the system.

2- *The centralised privacy system*: The term refers to creating one main account on the privacy server and establishing different privacy policies inside it. This account has all personal information details related to the user. It also gives the user the authority to classify the privacy policies into groups, and then the user can add a new or update a current website for a specific group. Thus, the applied privacy policy for the group will also be applied on the selected website, and it will allow the website to obtain only specific personal information from the privacy server.

4.6 Questionnaire Design

The first task of this study was designing a survey to determine several concepts needed to develop the suggested Smart Wizard System. The survey used was created by the researcher using a hard copy form that was designed to support anonymous participation to increase the confidentiality of participants and ensure that no one can be recognised by their names. In addition, the survey gave the participants full authority to complete or withdraw from participation without any consequences.

The method of designing the questionnaire was based on using close-ended questions. It limited participants to answering a list of choices questions, and the decision was made to rate the outcome on a scale continuum such as the Likert questions scale (Dillman 2011). The survey was quantitative research to generate numerical data by using SPSS software that can be transformed into usable statistics to help the researcher design the two applications.

The purpose of the survey was to measure the importance of privacy for Internet and mobile phone users and to define what personal information was more important to them. It also determined the difficulties of using the current style of choosing privacy settings for mobile phones, and clarifies whether a more suitable method needs to be developed. As a result, this information will be used to develop a Smart Wizard System that will help users to choose suitable privacy settings easily and quickly from any device, including mobile phones.

The survey was divided into five sections:

1. The first section of the survey asked some basic information about age, gender and other factors.
2. The second section asked some general questions about the participant's social networking accounts.
3. The third section asked some questions to rate the usage frequency of mobile services.
4. The fourth section was related to controlling the privacy settings and using a mobile phone to change them.

5. The last section of the survey asked the participants to evaluate each item of their personal information and determine the extent of its importance for them as it relates to their privacy.

According to Sekaran (2006), one of the main factors that contributes to the success of a survey is minimising bias in the research results. This can be done by concentrating mainly on these areas:

i. how the questions are formulated and the simplicity of the vocabulary;
ii. planning for categorising, sorting and coding the variables after the receipt of responses; and
iii. the overall design of the survey and the layout of the content.

The final design process for the survey took about two months (Aug. 2011 to Sep. 2011), and the survey was made available in two languages, English and Arabic, keeping in mind other surveys employed in other research. Thus, the researcher took into account the need to achieve research objectives that met the basic standards of designing the survey. Hence, a brief description will be given to describe each part of the survey and the scales used.

The first section of the survey focused on general knowledge about participants. It contained seven questions related to the participant's gender, age group and ownership of an Internet mobile device. It also focused on the use of browsing the Web through these devices. In this section, Nominal scales were used to develop the questions. These scales are used when the subject falls into a specific category and a rating of degree (such as high or low) is not needed (e.g., gender, age and eye colour) (Boone & Boone 2012).

The second section of the questionnaire consisted of five questions. All of them were related to general information about the online social networking accounts of the participants. The purpose of the first question was to measure the number of social networking accounts owned by the participants. The remaining questions were related to the use and time elapsed in browsing the account. In the design of this section, a nominal scale was used for the first question, and the other questions used cardinal scales. The cardinal scale is used to make quantitative comparisons between results based on the differences between the values (Azevedo 2012).

The main goal of the third section was to measure the usage frequency of Internet mobile services. These services included chatting, accessing email, browsing Facebook or any social network account, downloading applications, reading news or checking other services. There were five questions, and all of them were designed based on an ordinal scale. This scale allowed the participant to rank the variable by selecting one case (e.g. never, sometimes, often, usually or always), but it did not allow for relative degree of difference between them. For example, if there is a rank from 1 to 5 (1 meaning unhappy and 5 happy), it cannot be said that the participant who selected 5 is 5 times happier than one who selected 1 (Gigone & Hastie 2013).

The fourth section of the survey asked the participants some questions about controlling the privacy settings for their online social networking accounts, the use of Internet mobile devices to set privacy settings and the suitability of their mobiles to control the privacy settings. It consisted of seventeen questions, and there were three cases for each answer, yes, no and I don't know. The survey scale used for this section was a three-point Likert scale. This scale was developed to measure attitudes by asking participants some questions about the topic and defining whether they agree or disagree (Brown 2011).

The results from the fifth section of the questionnaire were important in designing the Smart Wizard System because they define the sensitivity of each personal information item. It consisted of 24 items to be rated by the participants. In this section, the author selected 23 items related to personal information details (e.g. name, age, email, date of birth and other information), and the last item asked them to rate their concern about online privacy. It used a five-point Likert scale that gave each item a rating from low importance to high importance (1 means low privacy sensitivity and 5 means high sensitivity) (Table 4.1). This type of scale has been used in other social networking surveys, such as Ellison, Steinfield and Lampe (2007), Lampe, Ellison and Steinfield (2006) and Steinfield, Ellison and Lampe (2008).

Name	Name	Name
Gender	Interest and activity	Comment and posts
Email	Favourite book	Tags
Date of birth	Favourite TV show	Friends' list

Phone number	Favourite music	Education and work
Physical address	Favourite movie	Religion
Current address	Relationship status	Website
School information	Pictures	
Hometown	Videos	

Table 4.1. The personal information items used in this study

4.6.1 Data collection and sample size

The sample of this study was selected based on the ownership of online social networking accounts and at least one account. The main idea of setting this condition was to evaluate the results and measure the privacy concerns of participants. The results were then used to design the Smart Wizard System. If this study had been based on the use of a probabilistic sampling method, it would have been necessary to build a procedure that gave all participants the same likelihood of being selected to participate in the study (Anderson, Sweeney and Williams 2011). Consequently, the study sample was selected from the University of Dammam in Saudi Arabia and the University of New England in Australia. The criteria for selecting respondents were that respondents have at least one social networking account and a mobile phone. In addition, the study population included both students and staff of the University of New England (UNE) and the University of Dammam who ranged in age from 18 and more than 45 years. Data were collected from some departments and colleges through hard copy forms included with the participation invitations. Most of the participants from the University of Dammam were men because there is no mix between the genders in colleges. The survey questionnaire was available in two languages: English and Arabic. A total of 185 respondents completed the survey (95 used the Arabic questionnaire and 90 used the English questionnaire), and all questions were multiple-choice questions. The two countries were selected to estimate population attributes especially in the selection of privacy policies of their social networking sites and the use of smartphones. The differences in the sample will assist the researcher to design a wizard privacy tool that would be suitable for different cultures and countries. Some privacy concerns in the two study countries are discussed in the next chapter.

When checking out the answers of respondents, there were eight papers containing a few missing answers for some questions. Participants between the ages of 18 and 25 represented the majority group, accounting for 75% of the respondents. Most of them had their own mobile phones, which were also used to browse the Internet.

4.6.2 Ethical considerations

In this study, ethical clearance is a mandatory step when the study involves humans. It also is an essential step based on the University of New England rules. It was presented to the Human Research Ethics Committee (HREC) and approval was given for the collection of data, with approval number HE11-210. This approval had some conditions and standards that should be applied throughout the data collection period.

Participants were clearly notified of their rights and told that their participation was voluntary. They also were notified about the confidentiality of the data and their right to withdraw from participation at any time. Furthermore, there was an information sheet attached to the survey containing information about the purpose of participation, the researchers, the rights of participants and contact details. The questionnaire did not include any room for providing any additional information that may identify the participant.

According to UNE regulations, the gathered data were kept secure and confidential and all these data were to be used only for research purposes. Participants were aware of the use of these data and notified that the results would be published and used in this study.

4.6.3 Data analysis

This section presents the data analysis procedure. In this study, SPSS v.19 was used as a statistical analysis application to analyse the data. Pallant (2010) stated that non-parametric techniques are an ideal tool for dealing with nominal and ordinal scales and are useful when the size of the sample is relatively small. Hence, to measure the validity and the reliability of the survey, Cronbach's alpha scale was used. When multiple Likert questions are used in a survey, the use of Cronbach's alpha scale is commonly preferred to determine the reliability of the survey (Lund & Lund 2013). Chapter five will discuss the data description and findings for this study and both surveys.

4.6.3.1 Reliability and validity

Testing the reliability and validity of the survey is a necessary step to measure the veracity of the data. Veal (2005) defined reliability as maintaining the research findings without bias toward any answer even when the researcher repeats or changes the survey sample at a later date. The most common scale used to measure it is Cronbach's alpha scale (Lund & Lund 2013; Sekaran 2006).

For this study’s survey, Cronbach’s alpha was used to calculate and check the reliability of the scales. Sekaran (2006) classified the reliability results into four categories: 1) poor when the reliability is 0.6 or less; 2) acceptable when it is about 0.7; 3) good when the reliability is at least 0.8; and finally 4) best when the reliability coefficient reaches 1.0.

Validity means calculating the accuracy of the measurement and determining which data were collected properly. Sekaran (2006) pointed out several types of validity measures, such as construct, content and criterion-related validity tests. In this study, Listwise deletion was used to test the validity of all variables in the procedure.

4.7 Developing the Smart Wizard System

This section provides a description of the design of the Smart Wizard System. The purpose of this wizard system is to facilitate the process of selecting privacy settings. The common way of selecting privacy settings for personal information items is the traditional pattern (Toch, Sadeh and Hong 2010) that allows the user to change the visibility status for each personal information item. With Internet mobile devices, this pattern can face some difficulties in the selection process. As seen in Chapter 2, there are some factors that can complicate the use of these devices for controlling privacy settings, such as mobile screen size and the method of selecting the item.

4.7.1 General code structure

This section describes the structure of the software code developed for the Smart Wizard System to determine privacy settings. The source code for the system is a combination of ASP.Net programming language and the SQL server database. Figure 4.4 describes the general structure of the functioning of the suggested system.

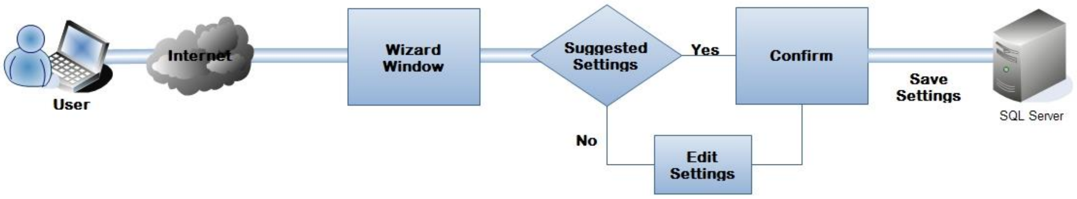


Figure 4.4. General code structure for the Smart Wizard System

As shown in Figure 4.4, the system comprises several stages:

1- The user has to log in to the Smart Wizard System Web page using the Internet connection of his/her mobile phone or computer.

2- The Smart Wizard System website asks the user some questions, from which the user can select various choices.

3- Based on the user's choices, various questions are asked relating to his/her choices.

4- At the end of the question stage, the system will run a specific inquiry based on the user's answers, and then the system will propose suggested settings to the user.

5- The user can modify any privacy item by hiding it or showing it; alternatively, he/she can confirm the proposed settings without making any modifications.

6- The last step requires the user to confirm and save the suggested privacy settings in the database.

In addition, there are several sub-stages in the stages listed above and various techniques to set the privacy settings. The technique shown in Figure 4.5 was used to program the Smart Wizard System.

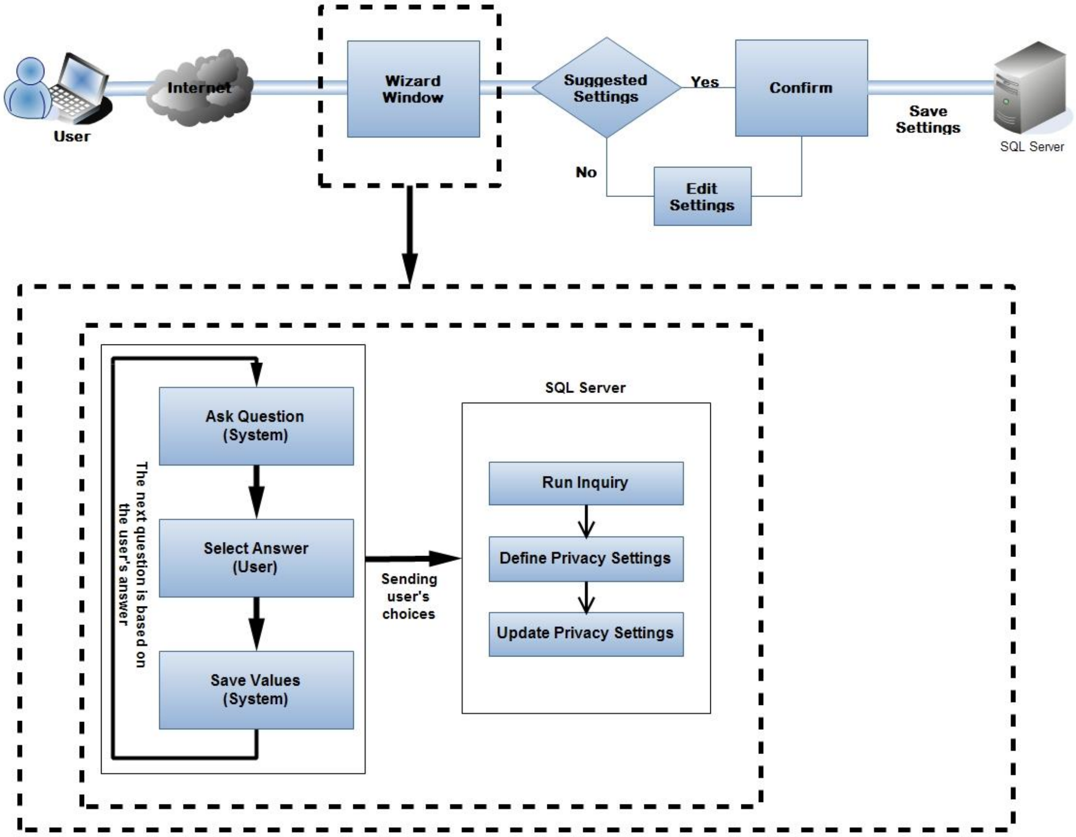


Figure 4.5. General code structure for the wizard's window stage

The main idea of the wizard's window is to give the user an easy way to set his/her privacy settings and save them on the server. This can be done by asking the user some questions related to whether he/she wishes to show or hide some personal information details. First, the system will ask the user to select his/her gender. When the user chooses the gender, the system will save the answer and move to the next question, which is based on the previous answer. Finally, upon completion of the questions and the selection of appropriate choices, the system will transfer the answers to the SQL server, and the SQL server will then run a specific inquiry depending on the answers. All values of the privacy items will then be updated.

In the next step, the system will present the proposed privacy settings based on the user's choices. As shown in Figure 4.6, several processes occur before confirming the suggested settings.

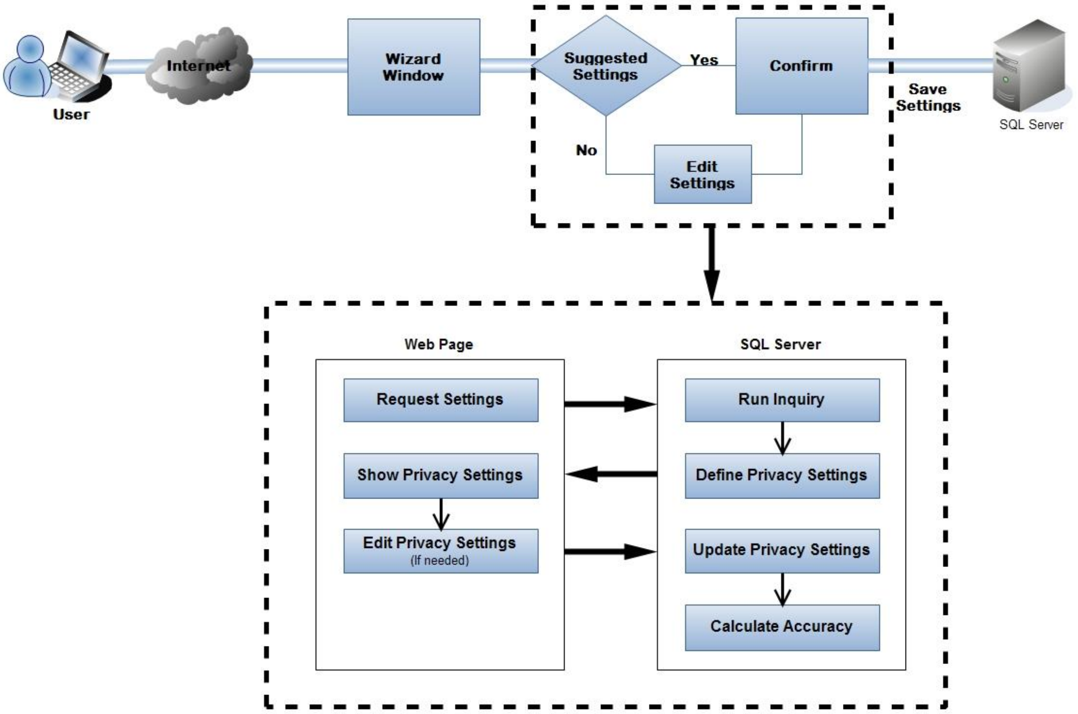


Figure 4.6. General code structure for the suggested settings stage

These steps are as follows:

- When the user has completed the selection of choices, the system will transfer the user to the suggested privacy settings page.
- The system will request the suggested settings from the SQL server by running a specific inquiry to return all values for all privacy and personal information items.
- All the settings will be available to the user to modify or confirm.
- If the user accepts all these settings, they will be saved in the database.
- The user can hide or display any personal information item by clicking on that item.
- A confirmation message will be presented to confirm the change.
- The SQL server will update all values regarding the changes.
- To make the selection of the privacy settings faster and easier, the success rate of the system will be calculated. This will be done by using the following formula to assess the system's accuracy:

(The number of items that are not changed ×100)/total number of items).

The main purpose of calculating the accuracy is to increase the system's credibility by modifying the current system if needed.

4.7.2 A scenario for selecting privacy settings using the Smart Wizard System

The Smart Wizard System scenario will simulate the actual use of the system. It will first ask the user some questions. Then, when the answers have been included, the system will set a value for one item or more. A value of 0 means that the personal information item will be hidden; a value of 1 means that the item will be visible. Furthermore, as shown in the scenario depicted from Figure 4.8 to Figure 4.15, the questions follow a particular sequence. The questions were designed based on the survey results. Moreover, the relationships between the personal information items were built based on the results of the survey.

As shown in the scenario below, depicted in Figure 4.8 to Figure 4.15, the system opens with a welcome screen, which provides a simple explanation about it or another explanation regarding the developers of the system. The next page has two choices to define the user's gender. Furthermore, pictures and symbols are used to provide a further explanation of the purpose of the question. For example, Figure 4.7 shows how pictures provide more information on the question. Hence, some pictures are included in some questions to emphasise the meaning of the question.

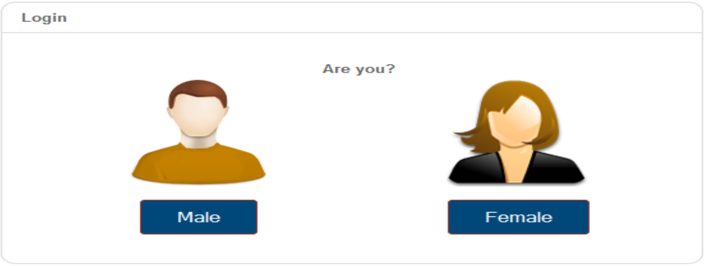


Figure 4.7. An example of using pictures in the Smart Wizard System

Other stages of the system ask questions related to the user's decision to show or hide personal information items. When he/she has answered all the questions, the system shows the suggested settings and allows the user to edit one or more of the items.

To give the user the opportunity to expand the range of choices, private personal information is classified into different categories based on the survey results. The survey classified the personal information items into three groups—high, medium and low—based on the sensitivity of the information. Within each privacy level, there are two different choices of settings: default or custom. The default settings are based on the results of the survey, which identified the settings best suited to the user's needs. Selecting a high privacy level as the default offers the user more privacy by hiding most of his/her personal information items. This level can be used to hide all items classified in the high and medium groups. Selecting a medium privacy level will hide all high-level privacy items and some personal information items that have low priority in the medium group. The last choice of default settings is the low level, and this level will hide only all high-level privacy items.

In contrast, selecting the custom settings offers more flexibility for users when choosing their privacy settings. Obviously, custom settings are designed to ask the user some questions about hiding or showing his/her personal information items, and all the questions are based on the survey results. These questions are shown in Appendix I. In addition, there are three levels of privacy in the custom settings: high, medium, and low. First, at the high level, various questions are asked. These questions are designed to be sequenced in such a way that the answer to one question dictates whether subsequent questions are asked. For example, the first question asks the user whether he/she wants to hide all his/her personal information items. If the answer is yes, then the system hides all the items, and there is no need to ask any more questions. However, if the user chooses no, other strategic questions are asked. Furthermore, the first questions are related to all items that have a high priority level according to the survey results. All personal information items that are located in the medium level are asked after the high-level questions. All items that are located in the low level are asked after the medium-level questions. Second, when the custom and medium privacy settings have been chosen, high and medium levels of privacy questions are asked. Another question asks the user whether he/she wishes to show or hide some personal information items that have a low level of privacy, such as the name and the website. Most personal information items with a low level of privacy will be shown. Finally, selecting low and custom privacy settings generates a question about all personal information classified as having a high or a medium level of privacy. All items with a low level of privacy will be shown.

4.7.3 Description of structures used in the Smart Wizard System

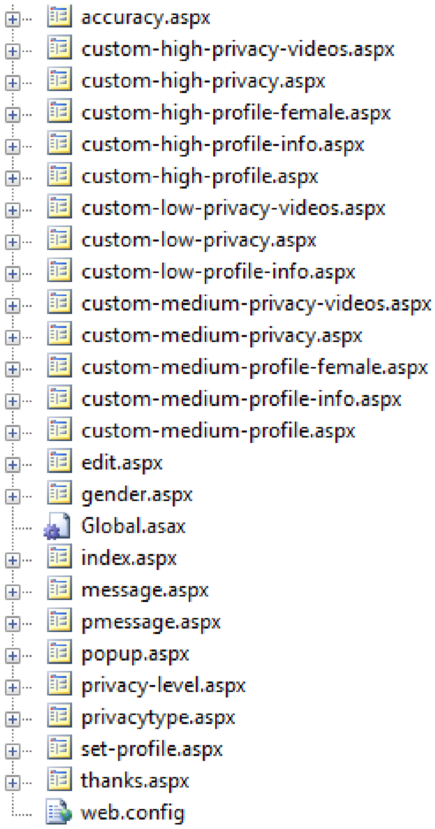
This section provides a description of the configuration structures for the Smart Wizard System. As mentioned before, the Smart Wizard System was designed using ASP.NET as a programming language (using C#) and SQL server structures. Table 4.2 shows all the fields used in the design of the Smart Wizard System's database and provides a short description of every field.

Database information:
Database type: SQL server database
Database name: users
Table name: permission

#	Column name	Field Description
1	ID	This field is used to give a unique number tor each user
2	Name	User's name
3	Gender	User's gender
4	Email	User's email
5	Date of Birth	User's date of birth
6	Phone No.	User's phone number
7	Physical Address	Physical address of the user
8	Current Address	Current address of the user
9	School Information	User's school information
10	Hometown	User's hometown
11	Interests and Activities	User's interests and activities
12	Favourite Books	User's favourite books
13	Favourite TV Shows	User's favourite TV shows
14	Favourite Music	User's favourite music
15	Favourite Movies	User's favourite movies
16	Relationship Status	User's relationship status
17	Pictures	User's pictures
18	Videos	User's videos
19	Comments and Posts	User's comments and posts
20	Tags	Users' tags
21	Friends' List	User's friends list
22	Education and Work	Education and work places of the user
23	Religion	User's religion
24	Website	Users' website
25	Accuracy	This field is used to calculate the accuracy of the system

Table4.2. Description of the Smart Wizard System's database

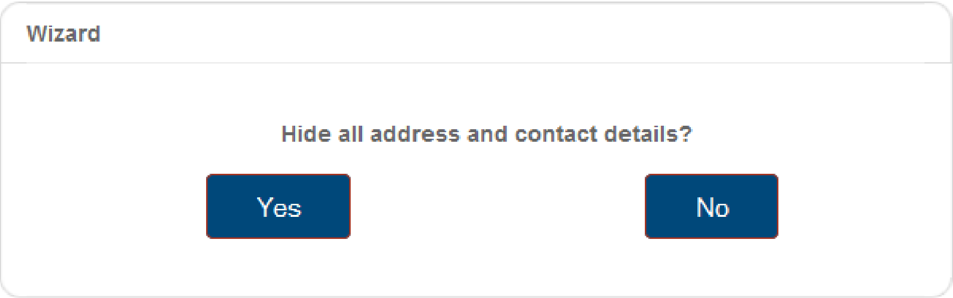
The Smart Wizard System is designed using various ASPX Web pages, and each page has one question that asks whether the user wishes to show or to hide items. All the pages and the other files are listed in Figure 4.8.



```
accuracy.aspx
custom-high-privacy-videos.aspx
custom-high-privacy.aspx
custom-high-profile-female.aspx
custom-high-profile-info.aspx
custom-high-profile.aspx
custom-low-privacy-videos.aspx
custom-low-privacy.aspx
custom-low-profile-info.aspx
custom-medium-privacy-videos.aspx
custom-medium-privacy.aspx
custom-medium-profile-female.aspx
custom-medium-profile-info.aspx
custom-medium-profile.aspx
edit.aspx
gender.aspx
Global.asax
index.aspx
message.aspx
pmessage.aspx
popup.aspx
privacy-level.aspx
privacytype.aspx
set-profile.aspx
thanks.aspx
web.config
```

Figure 4.8. Web pages of the Smart Wizard System

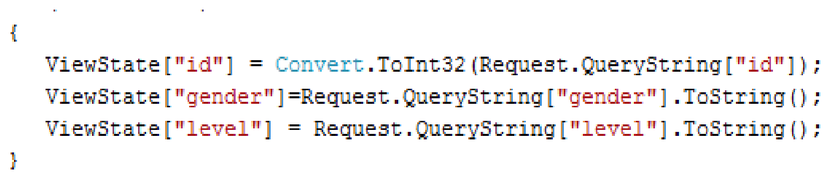
Furthermore, all the previous pages presented in Figure 4.8 are designed based on the smart wizard scenario. Figure 4.9 shows a sample question for the user to define his/her wishes to hide or show some personal information items.



Hide all address and contact details?

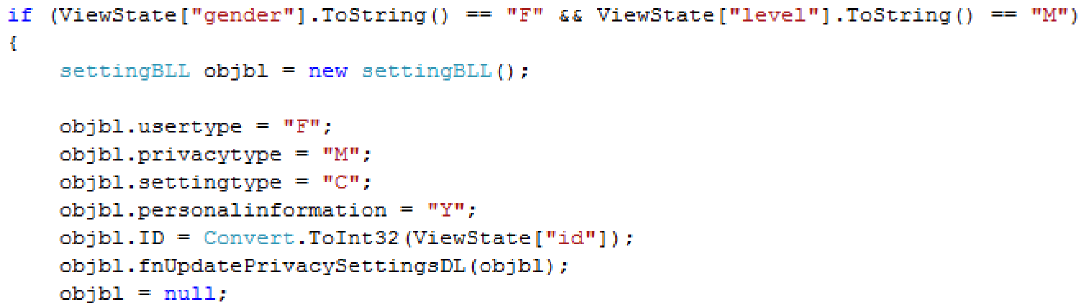
Figure 4.9. An example of a question in the Smart Wizard System

To access the Smart Wizard System, it is necessary to log in to the index page. The user then has to select his/her gender to move to another question. The command "*viewstate*," which is used in the ASP.net language using C#, as shown in Figure 4.10, is used to store the selected values from each question and deliver them to the next question until the user reaches the final stage. At the end of the selection stage, the system delivers all the selected values to the SQL server by adding them to a created object and then sets the suggested privacy values for all personal information items in accordance with the choices. Figure 4.11 presents an example of using the created object to transfer the values to the SQL server.



```
{
   ViewState["id"] = Convert.ToInt32(Request.QueryString["id"]);
   ViewState["gender"]=Request.QueryString["gender"].ToString();
   ViewState["level"] = Request.QueryString["level"].ToString();
}
```

Figure 4.10. An example of using the "viewstate" command



```
if (ViewState["gender"].ToString() == "F" && ViewState["level"].ToString() == "M")
{
    settingBLL objbl = new settingBLL();

    objbl.usertype = "F";
    objbl.privacytype = "M";
    objbl.settingtype = "C";
    objbl.personalinformation = "Y";
    objbl.ID = Convert.ToInt32(ViewState["id"]);
    objbl.fnUpdatePrivacySettingsDL(objbl);
    objbl = null;
```

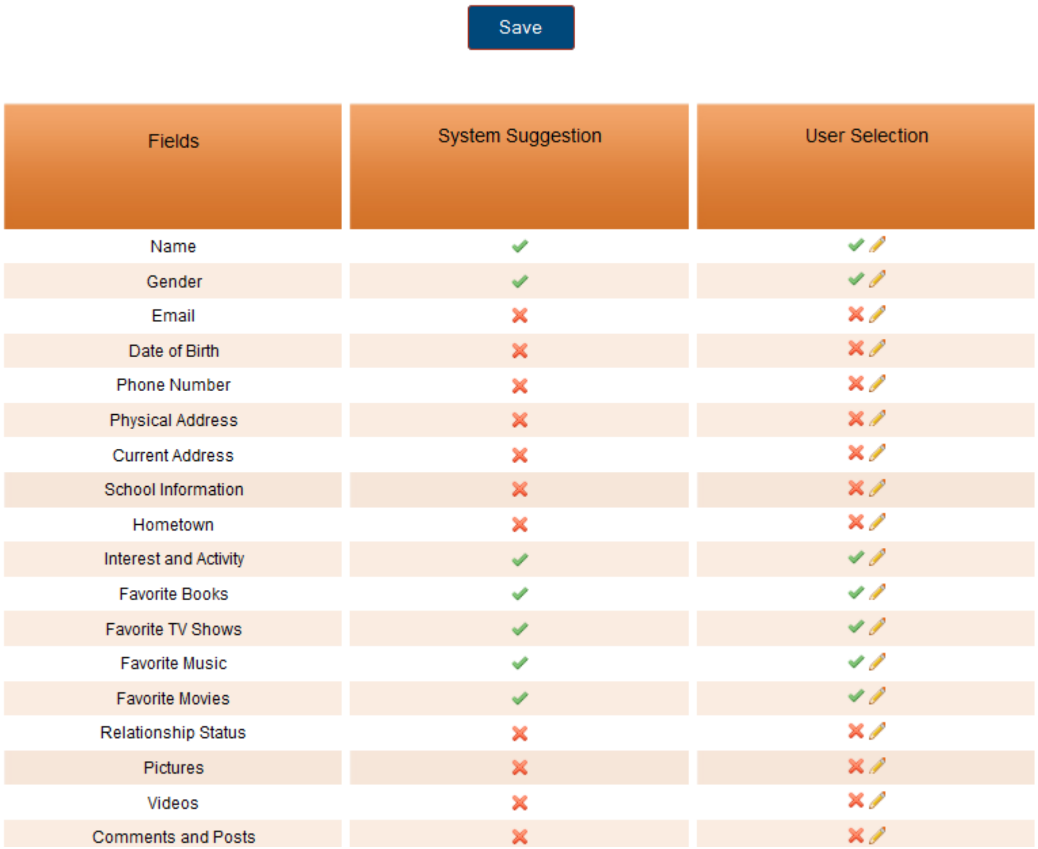
Figure 4.11. An example of using an object in the Smart Wizard System

When the system sends the object's values, the SQL server runs a specific inquiry based on these values. The values 1 or 0 are then assigned to each personal information item. For example, Figure 4.12 shows an example of how the SQL server sets different values in accordance with the user's selections. A value of 1 or 0 means that the item will be shown or hidden, respectively.

```
/*Female Low Custom*/
if( @User='F' and @PrivacyType='L' and @Settingtype='C')
begin
if(@PersonalInfo='Y')
begin
update permission
set
Gender=1,Name=1,FavoriteBook=1,FavoriteMovies=1,FavoriteTvShow=1,
FavoriteMusic=1,Email=1,DateOfBirth=1,PhoneNo=1,PhysicalAddress=1
,CurrentAddress=1,SchoolInformation=1,Hometown=1,InterestAndActiv
ity=1,RelationshipStatus=1,Pictures=1,Videos=1,CommentAndPosts=1,
Tags=1,FriendList=1,EducationAndWork=1,Religion=1,Website=1
,value=10
where ID=@ID
end
```

Figure 4.12. An example of how the SQL server sets privacy settings

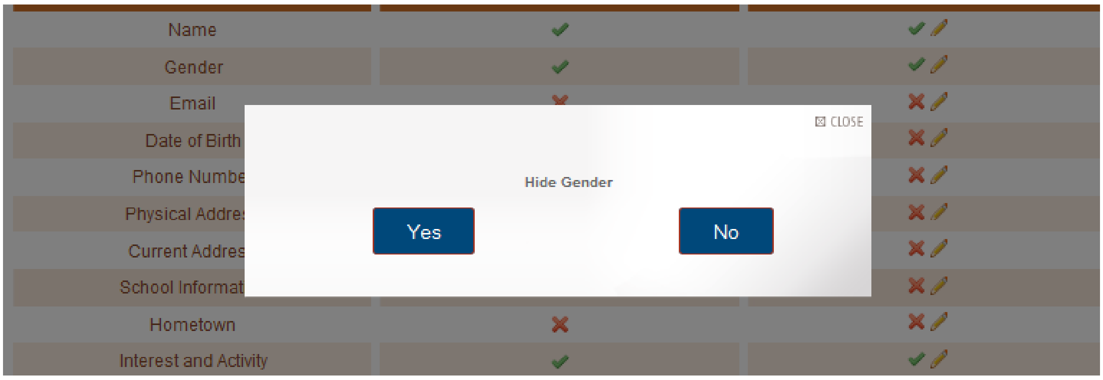
In the final stage, the system presents the suggested privacy settings to the user, showing which items will be displayed and which will not. Figure 4.13 provides an example of the system's suggested settings and the user's ability to edit one or more items. The ✗ symbol means that the item will be hidden, and the ✓ symbol means that the item will be visible to others.



Fields	System Suggestion	User Selection
Name	✓	✓ ✏
Gender	✓	✓ ✏
Email	✗	✗ ✏
Date of Birth	✗	✗ ✏
Phone Number	✗	✗ ✏
Physical Address	✗	✗ ✏
Current Address	✗	✗ ✏
School Information	✗	✗ ✏
Hometown	✗	✗ ✏
Interest and Activity	✓	✓ ✏
Favorite Books	✓	✓ ✏
Favorite TV Shows	✓	✓ ✏
Favorite Music	✓	✓ ✏
Favorite Movies	✓	✓ ✏
Relationship Status	✗	✗ ✏
Pictures	✗	✗ ✏
Videos	✗	✗ ✏
Comments and Posts	✗	✗ ✏

Figure 4.13. An example of the suggested privacy settings

Allowing users to edit some personal information items will increase the flexibility and the effectiveness of the Smart Wizard System. They will be able to modify the suggested settings for one or more items by clicking the edit symbol (✎), which is next to the item, and choosing the view state, as shown in Figure 4.14.



Name	✓	✓ ✎
Gender	✓	✓ ✎
Email	✗	✗ ✎
Date of Birth		✗ ✎
Phone Numbe		✗ ✎
Physical Addres		✗ ✎
Current Addres		✗ ✎
School Informat		✗ ✎
Hometown	✗	✗ ✎
Interest and Activity	✓	✓ ✎

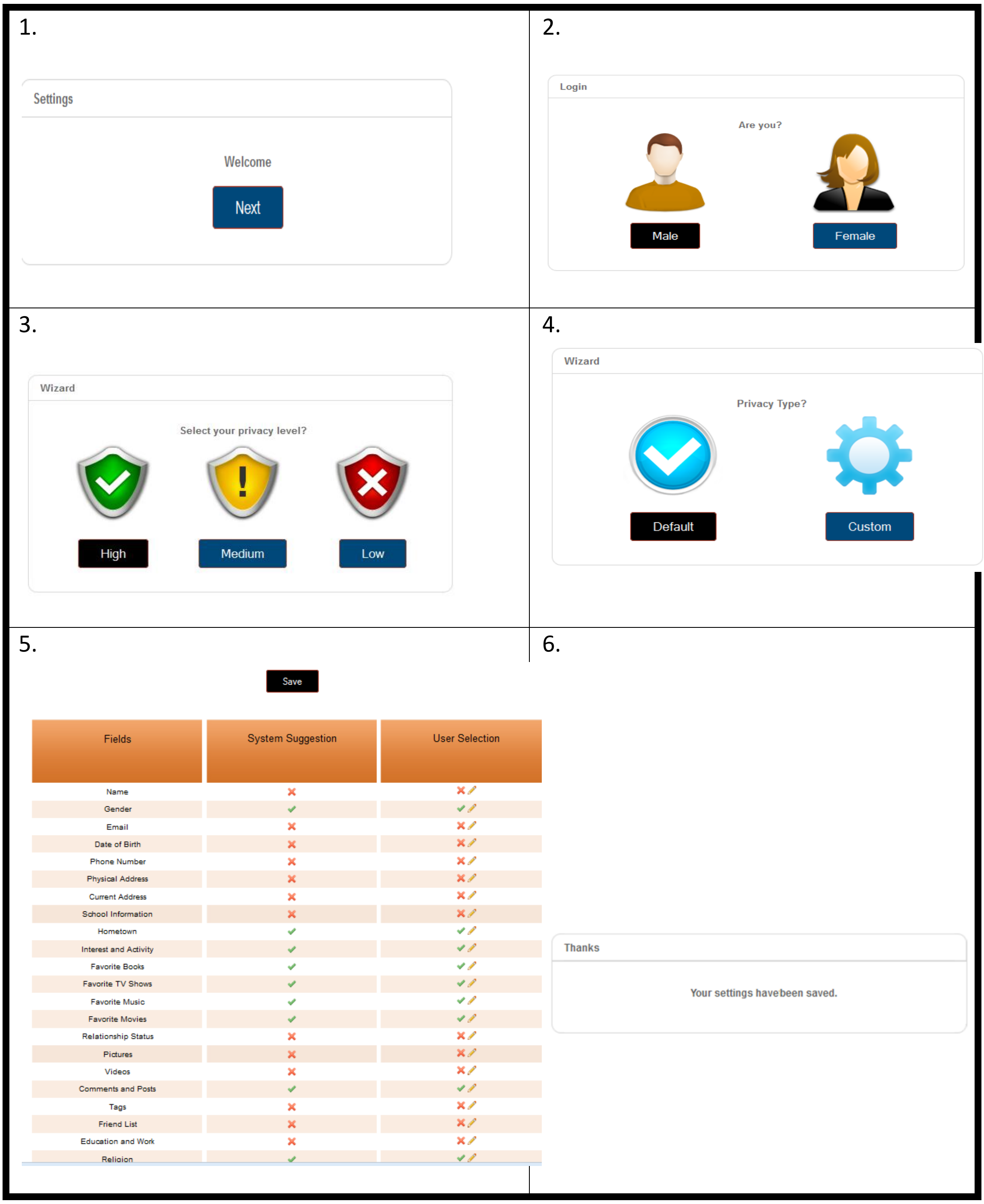
Hide Gender

Figure 4.14. An example of changing the suggested privacy settings

4.7.4 Smart Wizard System test code

This project has two main sections: a Smart Wizard System folder and an SQL server script. The Smart Wizard System folder contains the coding files, which are coded using the ASP.net (C#) programming language. This folder has subfolders, such as images and folders used for coding programming. The SQL server script is a file containing all the instructions used to set the privacy settings based on the user's selections. In addition, it is used to update the privacy settings and to calculate the system's accuracy. This step is explained below.

The way in which the privacy settings are selected in this system is not complicated. Only one option needs to be selected, and based on that option, another question will be asked. Figure 4.23 provides an example of testing the Smart Wizard System. The steps shown in Figure 4.15 to set the privacy settings are based on the user's gender, the desired privacy level, and the use of the default privacy setting for that level.



Fields	System Suggestion	User Selection
Name	✗	✗ ✎
Gender	✓	✓ ✎
Email	✗	✗ ✎
Date of Birth	✗	✗ ✎
Phone Number	✗	✗ ✎
Physical Address	✗	✗ ✎
Current Address	✗	✗ ✎
School Information	✗	✗ ✎
Hometown	✓	✓ ✎
Interest and Activity	✓	✓ ✎
Favorite Books	✓	✓ ✎
Favorite TV Shows	✓	✓ ✎
Favorite Music	✓	✓ ✎
Favorite Movies	✓	✓ ✎
Relationship Status	✗	✗ ✎
Pictures	✗	✗ ✎
Videos	✗	✗ ✎
Comments and Posts	✓	✓ ✎
Tags	✗	✗ ✎
Friend List	✗	✗ ✎
Education and Work	✗	✗ ✎
Religion	✓	✓ ✎

Your settings havebeen saved.

Figure 4.15. An example of the selection of privacy settings by using Smart Wizard System

In addition, Figure 4.16 is another example of using the wizard system when custom settings have been chosen. The main difference between the default and the custom settings is that the default settings have been designed for easy deployment when defining privacy settings. It helps to set privacy settings quickly and easily. However, the custom settings will result in greater security and in enhanced performance of these settings. The custom setting contains extra questions to increase the level of security and privacy. Figure 4.16 depicts how the custom settings help users to narrow their needs to achieve a high level of privacy settings. This option allows the users to select which items to show. For example, if the user wants to hide or show all his/her personal information with custom settings, he/she will be able to do that.

Calculating the accuracy of the system is also important for the programmer because this will help to measure the success rate of the Smart Wizard System and to determine whether modifications are needed. The system's accuracy will be calculated by defining the number of personal information items that have been changed from the edit window and comparing them to the values that the system suggested. Mathematically, this can be done using the following formula, where F is the total number of users, e is the user and $Accuracy_{F(E=e)}$ is the accuracy for the user e:

$$\text{Static score} = \frac{\sum_{e=0}^{|F|} Accuracy_{F(E=e)}}{|F|}$$

.

To calculate the accuracy for the user e, the following formula will be used:

$Accuracy_{F(E=e)}$ = (X ×100) / Y,

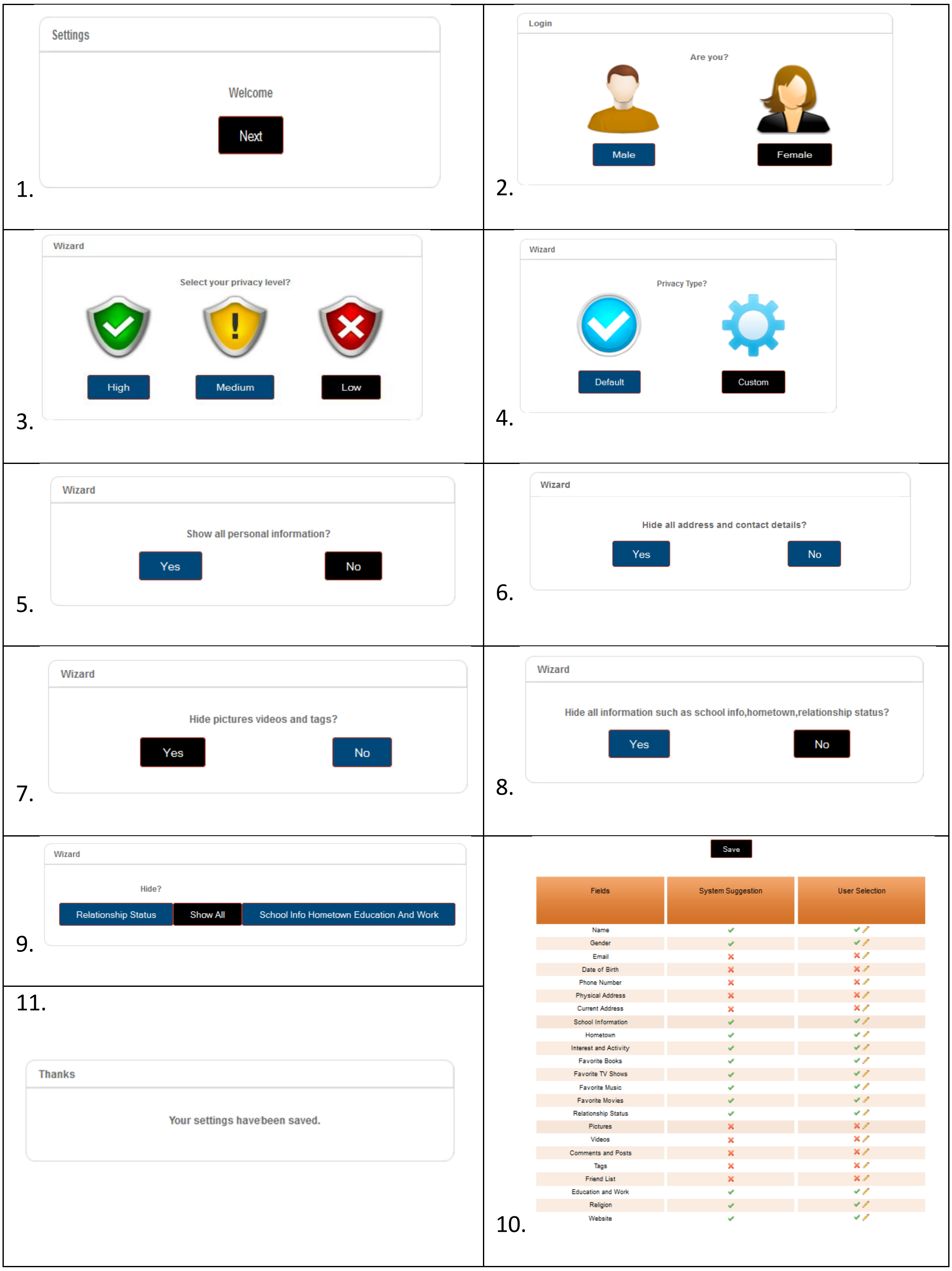
where

X = the total number of personal information items that were **not** changed by the user and

Y = the total number of all personal information items.

The importance of using this formula is to define the percentage of the changed items number that were modified by the participant. The accuracy percentage is important in the design of the tool for future modification and system maintenance. This formula was derived from the difference quotient standards (Reps and Rall 2003).

In addition, Figure 4.17 shows an example of using the previous formulas and presents the accuracy percentage. As mentioned already, the main purpose of calculating the accuracy is to develop the Smart Wizard System to set accurate settings for the user.



Welcome

Are you?

Select your privacy level?

Privacy Type?

Show all personal information?

Hide all address and contact details?

Hide pictures videos and tags?

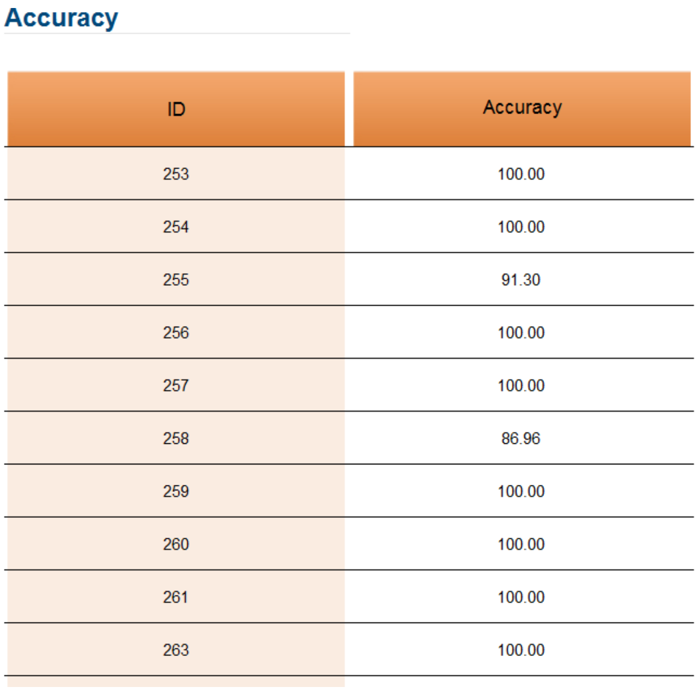
Hide all information such as school info,hometown,relationship status?

Hide?

Fields	System Suggestion	User Selection
Name	✓	✓ ✎
Gender	✓	✓ ✎
Email	✗	✗ ✎
Date of Birth	✗	✗ ✎
Phone Number	✗	✗ ✎
Physical Address	✗	✗ ✎
Current Address	✗	✗ ✎
School Information	✓	✓ ✎
Hometown	✓	✓ ✎
Interest and Activity	✓	✓ ✎
Favorite Books	✓	✓ ✎
Favorite TV Shows	✓	✓ ✎
Favorite Music	✓	✓ ✎
Favorite Movies	✓	✓ ✎
Relationship Status	✓	✓ ✎
Pictures	✗	✗ ✎
Videos	✗	✗ ✎
Comments and Posts	✗	✗ ✎
Tags	✗	✗ ✎
Friend List	✗	✗ ✎
Education and Work	✓	✓ ✎
Religion	✓	✓ ✎
Website	✓	✓ ✎

Your settings havebeen saved.

Figure 4.16. An example of selecting custom privacy settings using the Smart Wizard System



Accuracy

ID	Accuracy
253	100.00
254	100.00
255	91.30
256	100.00
257	100.00
258	86.96
259	100.00
260	100.00
261	100.00
263	100.00

Figure 4.17. Calculating the accuracy percentage of the Smart Wizard System

The Smart Wizard System offers a quick and accurate system to set privacy settings for the user's personal information. For mobile users, it is designed to be easy to use with mobile phones and to fit most mobile phone screens. It has been programmed based on the results of a survey. It has several advantages with regard to use, such as simplicity, flexibility, accuracy, speed and clarity. Clearly, the main factor of the design is asking the user particular questions and discovering users' expectations in relation to suitable personal information privacy settings. ASP.net and an SQL server were used to design the Smart Wizard System. In addition, the programming enquiries and instructions were created to set the desired privacy settings for users. The system has different levels of privacy and settings. Users have full authority to adjust the privacy settings, as shown in the scenario described for the method of selecting privacy settings for the Smart Wizard System. In addition, the system makes the users more aware of their personal information items and what items will be shown or hidden. Calculating accuracy for the Smart Wizard System is a measure of the success of the system or the need for further development. Given the high prevalence of the use of mobile devices, mobile phones will offer an easy way for users to set privacy settings for different websites in the years ahead.

4.8 Testing the Smart Wizard System

The third task of this study was testing the Smart Wizard System and measuring the concern of participants about the tested personal information items. There are several factors that distinguished this task from others. This survey is an implementation of a Smart Wizard System, and no similar wizard system is currently available to set personal information privacy settings. In addition, it can be used to support Internet mobile devices because of the simplicity of the design and the setting selection. The system was designed based on a previous survey done by the same author. This step was divided into two parts. The first part was the implementation of the Smart Wizard System and calculating the system's accuracy for each user. The second part was measuring concern about misusing personal information and the need to hide it. The two parts of this step gave the participant full authority to complete or withdraw from participation without any consequences.

The purpose of the first part was to implement the Smart Wizard System and calculate the accuracy percentage for it with respect to selecting personal information privacy settings and the participants’ satisfaction with the system’s suggested settings. On the other hand, the purpose of the second part was to measure the awareness of the participant about the issue of misusing one or several personal information details and whether he/she hides that item in his current social networking account or not.

The first part was designed as an Internet application that requires an interaction by the participant. First, when the participant completes the process of selecting privacy options, the application will transmit all the selected options to the SQL server. Second, the system will present recommended privacy settings based on the analysis of the data, and then it will define the suitable privacy option. Third, the recommended privacy settings will be presented to the participant, and he/she will have the authority to modify any item by changing the visibility status. Finally, without user intervention, the system will calculate the accuracy of the wizard based on the previous formula.

The second part of this task was an online survey, which was used to define the most sensitive personal information items for users. It also measured the behaviour of participants in hiding or showing sensitive items in their social networking accounts. This part consists of only one section that used a Likert scale to measure agreement.

This type of scale is helpful when the researcher wants to determine the attitude of the participants, and one of its forms asks "yes/no" questions (Kulshrestha & Kant 2013).

4.8.1 Data collection and sample size

For this task, data collection was based on an online application and a survey. It was necessary at this stage to give all participants the same likelihood of being selected to participate in this study (Anderson, Sweeney & Williams 2011). The survey was available in two languages, English and Arabic, and all pages were designed using the ASP.net language and SQL Server 2008 structures. The researcher used a private hosting service and domain to upload both the Internet application and the survey (http://www.smart-program.com/index.aspx). Moreover, the target group of participants were students and academic staff members at various universities. An email invitation was sent to different email lists for students and academic staff members. The email included the approval number from the University of New England and a letter of invitation to participate in the survey. In addition, an information sheet described the purpose of the survey and the Smart Wizard System.

To customise the target of the sample, the following procedures were undertaken:

1- Selecting two different cultures:

The first task was implemented using two different languages, and the author repeated the use of the same characteristics for the sample. This task was implemented using two different languages, English and Arabic, to diversify the sample. Data were collected from Australia and Saudi Arabia to facilitate the implementation of the proposed wizard system on a level asymptotic to that of the previous sample.

2- Customising the participation invitation

Participation for this task was customised for academic staff members and people who are interested in the technical field. Email invitations and blogs were used to encourage people to participate. First, email invitations were sent to staff members and students at several universities in Saudi Arabia and Australia. Each email contained information about the study and the participants' rights. Second, the author posted invitations on a number of Facebook pages that target the technical field. Each invitation contained information about the study and the participants' rights.

The results indicated that 439 participants implemented the Smart Wizard System (86 volunteers used English and 353 used Arabic), and 205 participants who completed the second part of the task.

The process of collecting data was previously planned and carefully organised. The survey link was posted on some Facebook pages targeting technical fields. The first reason for selecting Facebook pages is that Facebook is a community forum where people are able to discuss, chat, share links and engage in other social network services. Therefore, the author identified some active pages that address information technologies. The second reason for selecting Facebook pages is that the feedback received via Facebook participants will improve the study. This is because all the participants are already Facebook users and have an online social networking account.

4.8.2 Ethical considerations

As mentioned previously, ethical considerations are important in collecting data from humans. This task was approved by the Human Research Ethics Committee (HREC) at the University of New England in Australia with approval number HE12-219. This approval has some conditions and standards that should be applied throughout the data collection period.

Participants were clearly notified in both types of invitations (email and posted invitations) of their rights and informed that participation was intended for those aged 18 years and over. Participation was voluntary and clarified in the invitations. They also were notified about the confidentiality of the data and the right to withdraw from participation at any time. Furthermore, information was included about the purpose of participation, the researchers, the rights of participants and contact details. It was necessary for participants to read the information and accept the age condition for participation.

All data was kept securely and confidentially, based on UNE regulations. Furthermore, participants were aware of the purpose of the use of the data, and they were informed that all results would be published and used for the study.

4.8.3 Data analysis and reliability

Calculating the accuracy for the first part of the task was the main standard in evaluating the proposed Smart Wizard System and determining the need for more development of the system. In the first part, the author used the following formula to calculate the accuracy of the Smart Wizard System for each user by estimating the number of personal information items that had been changed.

$Accuracy\ e = (X \times 100) / Y,$

where:

X = the number of items that were not changed by the participant, and

Y = the total number of all personal information items.

After calculating the accuracy for each user, the average accuracy for all participants was also calculated using the following formula:

$$\text{Mean Accuracy} = \frac{\sum_{e=0}^{|F|} Accuracy_{F(e)}}{|F|}$$

where F is the total number of participants.

The second part of the task used a Likert scale (agreement) to assess the concern of the participant about personal information items and to determine whether they hid them on their current profiles or not. The next chapter will present a comparison of the findings and provide an analysis of the relationship between items with respect to several factors.

4.9 Developing the Proposed Privacy System

The fourth task of this study was developing the whole privacy system. It is an original idea compared with current privacy systems. This system, as mentioned in Chapter 3, consists of two parts. The first part includes the Smart Wizard System as a tool to set different privacy policies for a user's account. The second part is designing the infrastructure, linking servers together.

The purpose of this proposal is to build an integrated system that provides a high level of personal information privacy by controlling the process of data sharing with other websites (Figure 4.18). The proposed system is designed to deal with the exchange of users' personal information between websites with more confidence. In general, the main idea is to build a management privacy system that contains all of the user's personal information details, such as name, date of birth, email address, current address and other items, and to provide users with more authority to create different privacy policies for sharing this data. The users will be able to decide which personal information items they want to share with other websites. This system will also help to reduce the distribution times of personal information details when an individual signs up as a new user on a website. Further, it will give him or her permission to create different privacy policies for each website and determine which personal details may be shared.

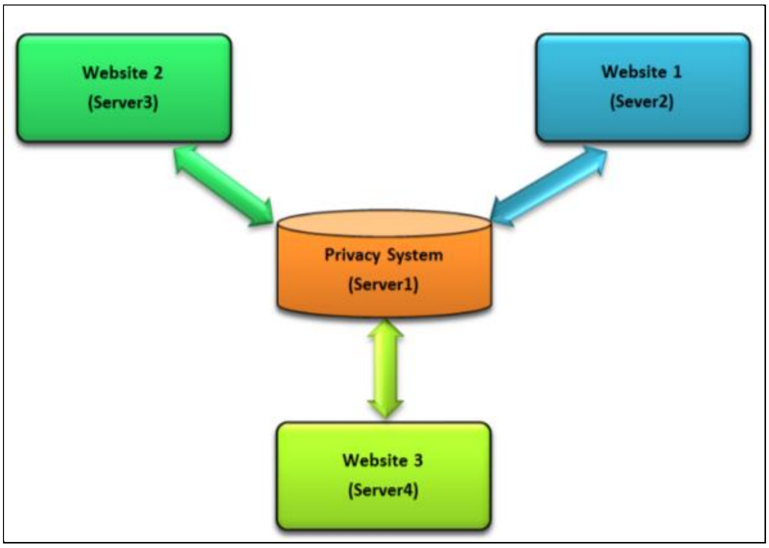


Figure 4.18. General infrastructure for the suggested privacy system.

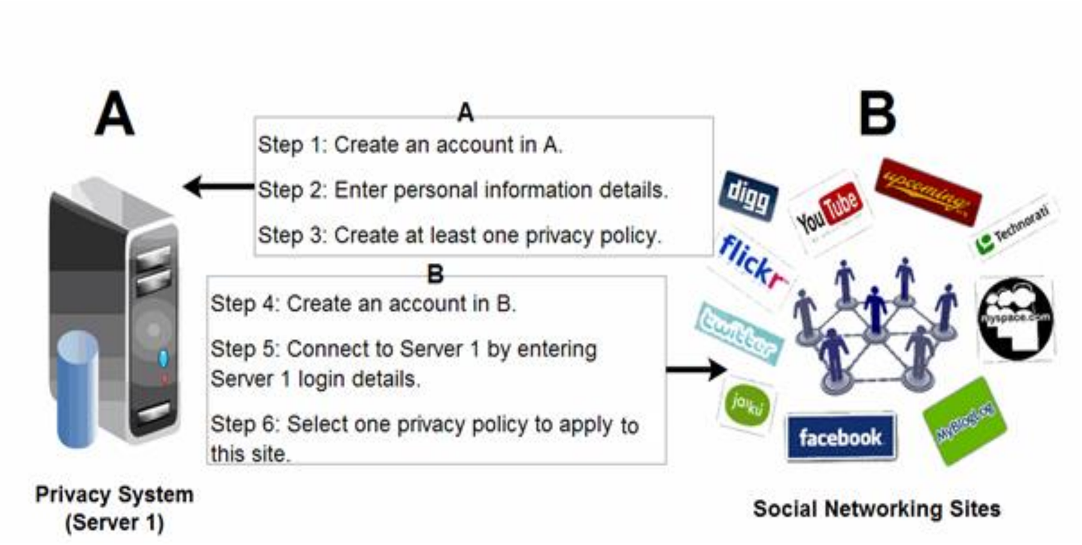

A
A
Step 1: Create an account in A.
Step 2: Enter personal information details.
Step 3: Create at least one privacy policy.
B
Step 4: Create an account in B.
Step 5: Connect to Server 1 by entering Server 1 login details.
Step 6: Select one privacy policy to apply to this site.
B
digg
YouTube
upcoming
Technorati
flickr
twitter
myspace.com
jaiku
facebook
MyBlogLog
Privacy System (Server 1)
Social Networking Sites

Figure 4.19. General infrastructure for the suggested privacy system.

As shown in Figure 4.19, different websites communicate with the privacy system (server 1) to request some data. Based on the created policies, server 1 will allow the other server to obtain some personal information.

The following explains the steps involved in this process.

Steps for server 1:

1. Alice creates an account in server 1 (using an email address and password).
2. After registering, she has to fill out personal data fields on server 1.
3. Next, Alice has to create various privacy policies using the wizard privacy system. She can create as many as she wants. In this example, Alice creates two different privacy policies. The first privacy policy allows for sharing only her name, age and gender, and we will name it “forums only”. The second privacy policy will allow for sharing her name, age, gender, photos, videos and address, and we will name it “social networking sites”.

The following steps are done for any other websites, such as those on server 2, 3 or 4:

Note: We assume that all other websites have used the compatibility tools and privacy requirements for swapping and sharing information with server 1.

4. If Alice likes one forum website, such as The Australian Internet and Technology Discussion Forums, and wants to register on it, she has to click on “sign up” or “create a new user account”.

5. She will need to fill out the login details for the page, such as an email address or a username and a password, to be used only when Alice wants to log in to this page later (note: a different email address from the one used on server 1 can be used).
6. Because we assume that there is a previous agreement between sites (this site and server 1), there is no need for Alice to enter any personal information details on this site.
7. After creating the new account, Alice has to select the suitable privacy policy to be used with this website and this will be done by clicking on “add privacy policy”.
8. When the link is clicked, the website will be redirected to the server 1 login page.
9. Alice then logs in using her email address and password for the server 1 site.
10. Once logged in, Alice will see the two privacy policies that she created earlier (i.e., “forums only” and “social networking sites”).
11. She will either choose a policy to apply to this site or click on the wizard symbol to create a new privacy policy.
12. After selecting the required privacy policy and saving it as the default privacy policy for the site, server 1 will allow the site to obtain only the information authorised by the chosen policy. For example, Alice selected “forums only”, The Australian Internet and Technology Discussion Forums will see only her name, age and gender.
13. By clicking on the “my profile” option in this site, Alice will see only her name, age and gender.
14. When Alice visits a social networking site, such as Facebook, and wants to register there as a new user, she will need to repeat steps 4 to 11, but in step 10, she will select “social networking sites” as the privacy policy.
15. In this site, Facebook will be allowed to see Alice’s name, age, gender, photos, videos and address.
16. Alice can apply one privacy policy to more than one website through registration procedures for other websites.

4.9.1 Algorithm description

This section will describe the basic algorithms for designing all servers and explain how each server works, including details on how to code the whole system. The next two subsections introduce the algorithm processing for all servers used in this thesis.

4.9.1.1 Algorithm processing for the privacy system (server 1)

- **Pseudocode**

The following pseudocode describes the steps used to design and code the privacy system (server 1). It will also show the registration steps for new users.

A = the user:

```
1      BEGIN
10     IF A has an account THEN
20         Login to the system
30     ELSE
40         A has to create a new account
50         A has to enter personal information details
60         A has to login to the system
70     ENDIF
80     SELECT CASE when A has already at least one privacy policy
90     CASE update the current privacy policy
100        Select the privacy policy
110        Update the selected privacy policy
120    CASE add a new privacy policy
130        Go to 150
140    END SELECT
150        Add other privacy setting.
170    IF A wants to add another privacy policy THEN
180        GO TO 150
190    END IF
200    End
```

- **Flowchart**

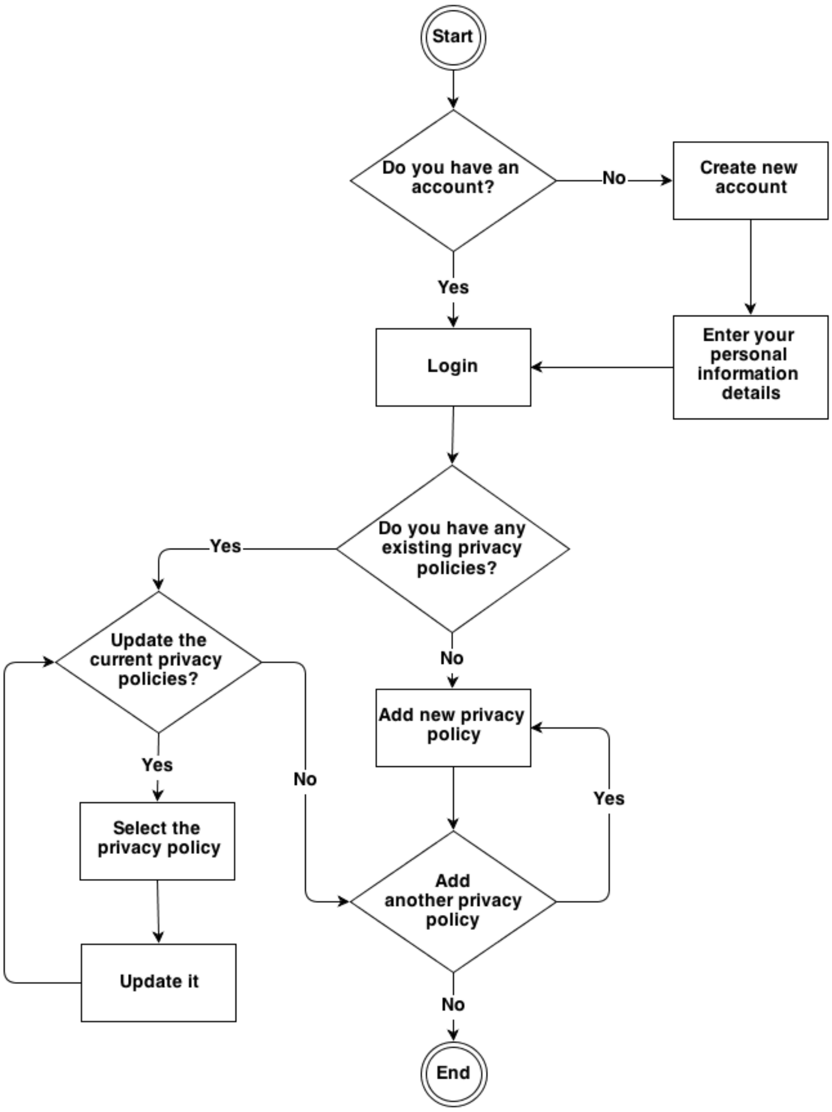

Start
Do you have an account?
No
Create new account
Yes
Login
Enter your personal information details
Do you have any existing privacy policies?
Yes
Update the current privacy policies?
No
Add new privacy policy
Yes
No
Yes
Select the privacy policy
Add another privacy policy
Update it
No
End

Figure 4.20. Algorithm processing for the privacy system (server 1).

- **Algorithm description**

This section will describe the steps used in the previous algorithm. First, the user will log in to the system using an existing username and password. If the user has no login details, then he or she would register as a new user and enter personal information details. Second, the user will be asked to create a new privacy policy or update a current existing privacy policy (if a privacy policy was created earlier). Third, if the user selected to update a privacy policy, he or she will need to choose and update it. Fourth, after the addition or updating of a privacy policy, the system will ask the user if he or she wants to add another privacy policy. If the answer is “yes”, the system will return the user to the previous step to create a new privacy policy. This will be repeated until the user chooses “no”. Finally, when the user is finished creating different privacy policies, he or she can log out of the system.

4.9.1.2 Algorithm processing for the privacy system (servers 2, 3 and 4)

- **Pseudocode**

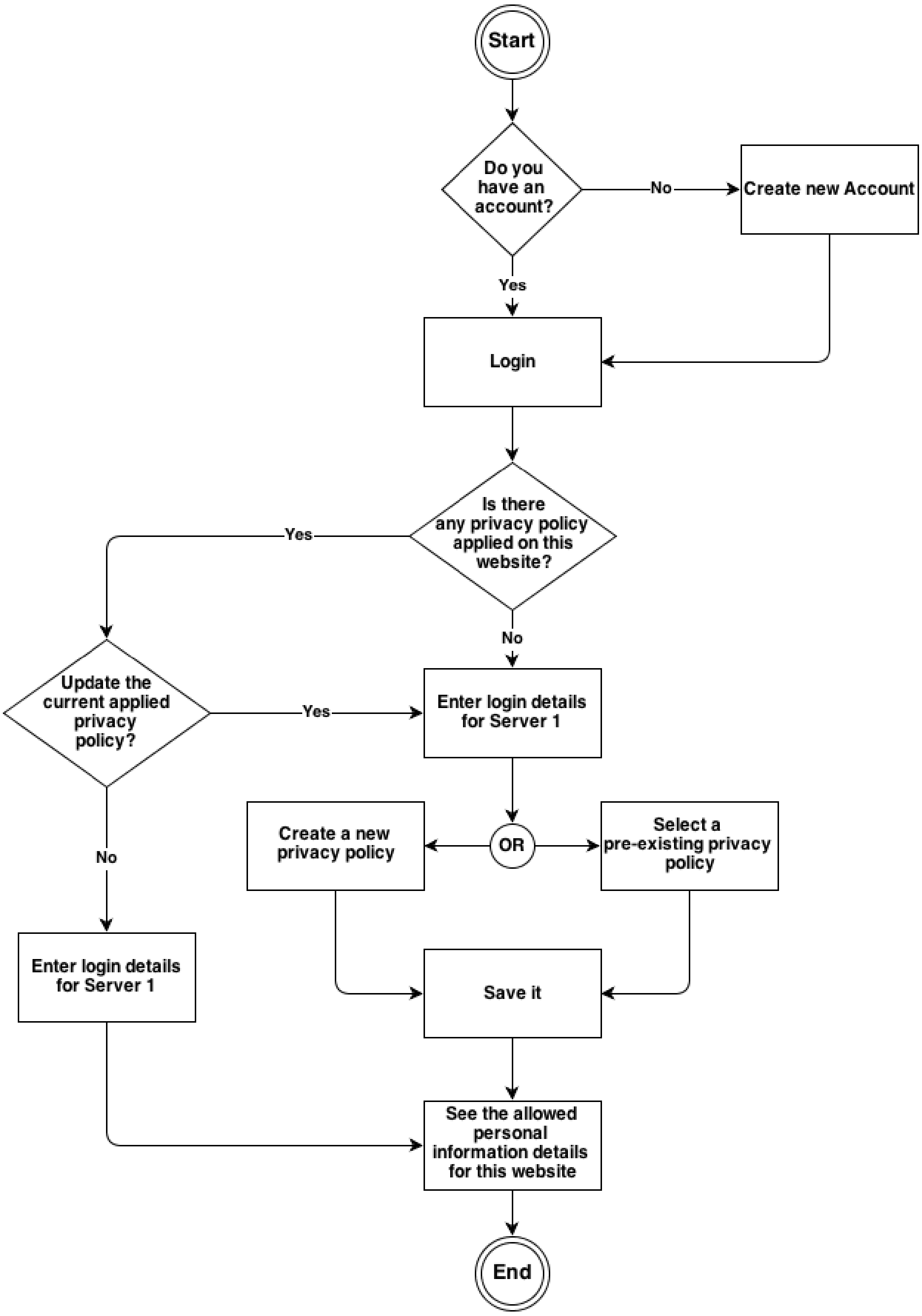
The following pseudocode describes the steps used to design and code the other servers used to communicate with the privacy system (server 1).

A = the user.

```
1   BEGIN
10  IF A has an account THEN
20          Login to the system
30  ELSE
40          A has to create a new account
60          A has to login to the system
70  ENDIF
80  IF A has an applied privacy policy on this website THEN
90          IF A wants to update the current privacy policy THEN
100                         Go To 160
110                 ELSE
120                         Enter login details for server 1
130                         Go To 250
140                 ENDIF
150         ENDIF
160         Enter login details for server 1
170         SELECT CASE when A wants to:
180                 CASE selecting a pre-existing privacy policy
190                 Select one from the pre-existing privacy policies
200                 Save it
210                 CASE creating a new privacy policy
220                 Create a new privacy policy
```

```
230                 Save it
240         END SELECT
250         See the allowed personal information details for this website
260         END
```

- **Flowchart**



Start
Do you have an account?
No
Create new Account
Yes
Login
Is there any privacy policy applied on this website?
Yes
No
Update the current applied privacy policy?
Yes
Enter login details for Server 1
No
Create a new privacy policy
OR
Select a pre-existing privacy policy
Enter login details for Server 1
Save it
See the allowed personal information details for this website
End

Figure 4.21. Algorithm processing for other websites (servers 2, 3 and 4).

- **Algorithm description**

The designs of the algorithms for servers 2, 3 and 4 are similar, with the exception of several codes for database connections. They all use the same strategy of coding and designing. This section will explain how the algorithm should work. First, the user will log in to the system using an existing username and password; it is not necessary for the login details to be the same as those used for server 1, and they will only be used for this website. If the user has no existing account, he or she must register as a new user. Setting a privacy policy will be the next step after the login process. If there is an existing privacy policy, the user can modify it or see what personal information will be shared with the site. To do this, he or she must log in to the system using the login details for server 1. If the site has no privacy policy selected to apply to it or the user wants to update the current privacy policy, he or she must log in to the system using the login details for server 1 to add a new privacy policy or update the current one. Finally, after making the modifications and saving the changes, the user will be able to see what personal information will be shared with the site based on the applied privacy policy.

The pseudocode and algorithms used in this study contribute to the understanding of the strategy of designing the framework and assist its future development. These algorithms retain the privacy properties for users by giving them the authority to control the process of sharing their personal information with other websites. In these algorithms the researcher provided the way to understand the applied procedures for creating accounts in the main privacy server and the other servers that required access to specific information. It also presented the differences between the ways of storing information in the current privacy systems that are located in some social networking sites, as mentioned earlier in chapter two, and storing the process of users' information in this framework.

4.9.2 Programming method

This part will explain the procedure for designing and programming the privacy system.

4.9.2.1 Databases and tables

Various databases were used to test the proposed privacy system on different servers. This was necessary to create some communication procedures to establish a channel of communication between servers.

- **Privacy system database (server 1)**

In this research study, SQL Server 2008 was used to design all the databases and create different internal procedures for different purposes, and ASP.NET was used as a programming language (using C#) to design all the Web pages. All procedures and other code structures will be explained later.

This section will give a detailed explanation of the database used in the privacy system (server 1).

- Database type: SQL Server 2008.
- Database name: server1.

Since the main objective of the suggested system is to facilitate the process of selecting privacy settings, some personal information items and files that are often uploaded, such as photos, videos, friend lists, comments and tags, will not be necessary. It will be sufficient to add a reference to the item’s status (i.e., allowed to share with others or not allowed).

Server1 is the name of the database, and SQL Server 2008 is the type. It has two tables (*wizard_user* and *permission*). The first table is used to save the user’s login details and personal information details, and the second table is used to save the privacy settings that are created or updated by the user. At least one column in each table has been set as a primary key for identification purposes and to create relationships between tables and various databases.

First, as shown in Table 4.3, the *wizard_user* table has two columns set as primary keys (*userID* and *email*). The *userID* column is set as a primary key for identification and linking purposes, and the *email* column is used to prevent duplication.

#	**Column Name**	**Variable Type** ("🔑" primary key)	**Field Description**

🔑

1	UserID	Bigint	Assigns a unique number to each user
2	Name	nvarchar(100)	Saves the entered value for the name
3	Gender	Int	Saves the entered value for the gender
4	Mobile	nvarchar(50) 🔑	Saves the entered value for the phone or mobile number
5	Email	nvarchar(50)	Saves the entered value for the email address
6	Password	nvarchar(50)	Saves the entered value for the login password
7	Dateofbirth	nvarchar(50)	Saves the entered value for the date of birth
8	Schoolinformation	nvarchar(200)	Saves the entered value for the school information
9	Hometown	nvarchar(100)	Saves the entered value for the home town
10	Interestandactivity	nvarchar(200)	Saves the entered value for the interest and activities
11	Favoritebook	nvarchar(200)	Saves the entered value for favourite books
12	Favoritetvshows	nvarchar(200)	Saves the entered value for favourite TV shows
13	Favoritemusic	nvarchar(200)	Saves the entered value for favourite music
14	Favoritemovies	nvarchar(200)	Saves the entered value for favourite movies
15	Educationandwork	nvarchar(200)	Saves the entered value for education and work
16	Currentaddress	nvarchar(200)	Saves the entered value for the current address
17	Religion	nvarchar(100)	Saves the entered value for religion
18	Physicaladdress	nvarchar(200)	Saves the entered value for the physical address
19	Website	nvarchar(50)	Saves the entered value for the website
20	Relationshipstatus	nvarchar(50)	Saves the entered value for relationship status

Table 4.3. The design of the wizard_user table.

Second, the *permission* table is used to save the sharing status of each personal information item. Values 1 or 0 are used, with 1 meaning “allowed” and 0 meaning “not allowed” to share with others. Two columns are set as primary keys for identification and linking purposes with other tables and databases. As shown in Table 4.4, 26 items are used in this table, and three of them are used for identification purposes (*ID*, *userdID* and *settingname*). First, the *userID* column is used to identify the created privacy policy by saving the user ID as a value for this variable. Second, each created privacy policy is given a unique ID to distinguish it from others. Finally, to facilitate the means of selecting the required privacy policy for users, each created privacy policy will be given a name to help, and this name will be saved in the *settingname* column. The main reason for not setting this variable as a primary key is because the value of the variable can be repeated by others.

#	**Column Name**	**Variable Type** ("🔑" primary key)	**Field Description**
1	ID	int 🔑	Assigns a unique number to each privacy policy created
2	Name	int	Saves the sharing status for the item name
3	Gender	int	Saves the sharing status for the item gender
4	Email	int	Saves the sharing status for the item email address
5	DateOfBirth	int	Saves the sharing status for the item date of birth
6	PhoneNo	int	Saves the sharing status for the item mobile or phone number
7	PhysicalAddress	int	Saves the sharing status for the item physical address
8	CurrentAddress	int	Saves the sharing status for the item current address

9	SchoolInformation	int	Saves the sharing status for the item school information
10	Hometown	int	Saves the sharing status for the item hometown
11	InterestAndActivity	int	Saves the sharing status for the item interest and activity
12	FavouriteBook	int	Saves the sharing status for the item favourite book
13	FavouriteTvShow	int	Saves the sharing status for the item favourite TV show
14	FavouriteMusic	int	Saves the sharing status for the item favourite music
15	FavouriteMovies	int	Saves the sharing status for the item favourite movie
16	RelationshipStatus	int	Saves the sharing status for the item relationship status
17	Pictures	int	Saves the sharing status for the item pictures
18	Videos	int	Saves the sharing status for the item videos
19	CommentAndPosts	int	Saves the sharing status for the item comments and posts
20	Tags	int	Saves the sharing status for the item tags
21	FriendList	int	Saves the sharing status for the item friend list
22	EducationAndWork	int	Saves the sharing status for the item education and work
23	Religion	int	Saves the sharing status for the item religion
24	Website	int	Saves the sharing status for the item website
25	Settingname	nvarchar(300)	Gives a name for the created privacy policy
26	userID	int 🔑	Gives a unique number to each user

Table 4.4. The design of the permission table.

The following example will explain the previous information further. Alice is a user of the system, and when she registers as a new user, she will be assigned a unique ID, and this value will be saved as the *userID* variable. When Alice wants to create a new privacy policy, she needs to enter a name for this policy, which will be saved in the *settingname* variable. This privacy policy will have another unique number because Alice can create more than one privacy policy. Thus, the saved value in the *ID* variable will be helpful in identifying the exact selected privacy policy among all the privacy policies created by Alice.

- **The databases for servers 2, 3 and 4**

The main purpose of designing websites for Servers 2, 3 and 4 is to communicate with server 1, select the suitable privacy policy to apply to it and see the personal information shared with this website. Hence, there will be similarities between the databases designed for these websites (servers 2, 3 and 4). Each database has two tables, *wizard_user* and *wizard_favorite_setting*. The first table is used to save the login details, and the second is for saving the privacy policy applied to this website.

First, there are only three columns in the *wizard_user* table, and one of them is set as the primary key *userID*, as shown in Table 4.5.

#	Column Name	Variable Type ("🔑" primary key)	Field Description
1	userID	bigint 🔑	Assigns a unique number to each user
2	email	nvarchar(50)	Saves the sharing status for the item name
3	password	nvarchar(50)	Saves the sharing status for the item gender

Table 4.5. The design of the wizard_user table.

As mentioned before, the *userID* variable is used to provide the user with a unique ID to facilitate the process of linking the user with the required privacy policy on server 1. The other two variables (email and password) are used to save the registration information for this website. However, there is a difference between the *userID* variable in each of the server databases, and each may have a different value compared to the others because each variable is used for internal database processes for identification purposes.

Second, the *wizard_favorite_setting* table is used to save the selected privacy policy from server 1 and apply it to the website. When a website user creates an account and adds a privacy policy for this site, the referencing details for it will be saved in this table. As shown in Table 4.6, four variables are used as references to the selected privacy policy, such as *settingID* and *settingname*. Each record will have the name and the identification number of the selected privacy policy from server 1. By getting these details, server 2, 3 or 4 will be able to communicate with server 1 and get access to specific information.

#	Column Name	Variable Type (" 🔑" primary key)	Field Description
1	favsettingID	bigint 🔑	Assigns a unique number to each selected privacy policy
2	settingID	bigint	Saves the selected privacy policy ID from server 1
3	userID	bigint	Saves the user ID for this Website to be used for linking purposes with server 1
4	settingname	nvarchar(100)	Saves the name of the selected privacy policy from server 1

Table 4.6. The design of the wizard_favorite_setting table.

However, there is an important issue related to the communication and sharing processes. Websites that need to communicate with server 1 are not allowed to save personal information details. They can only gain access to read some information for viewing purposes.

4.9.2.2 Internal and external processes of servers

This part will logically explain the relationships between internal processes for all servers and databases, such as creating a user, adding personal information details, creating a privacy policy, applying a privacy policy and other processes.

- **Internal processes for the privacy system (server 1)**

Several procedures can be performed in the server1 database, and each one has separate actions whether updating or adding records. As mentioned, server1 has two tables for saving personal information and privacy policy details, so the following points will present the logical relationship between the database tables and internal processes.

1- Create a new account

When a user creates a new account, he or she needs to enter all personal information details shown in Table 4.3 (*wizard_user*) except the variable *userID*, which will be assigned by the system.

2- Add new privacy policy

To create a new privacy policy, the user has to use the wizard system to transfer his or her selections to the system to find the appropriate privacy settings. Therefore, the first step is to give a name to this policy, and the value will be saved in the *settingname* variable in Table 4.4 (*permission*). The next step is to set value 1 or 0 (1 meaning visible and 0 not visible) for all other items except the *ID* and *userID* variables. Values for these variables will be added automatically by the system. *UserID* will have the same value as used in Table 4.3 to identify the person who created this privacy policy, and the *ID* variable will uniquely identify the created privacy policy. Thus, a user with a unique number in the *userID* variable can create many privacy policies with different identification numbers that are saved as *ID* variables.

3- Updating personal information details and a privacy policy

To update some personal information details or change their visibility status, the user is required to select the option for updating information and enter the new values. The next step is the updating process. This will be done through some procedures that ask the user to enter new values and exchange the previous values with them. Variables set as primary keys, such as *userID* and *ID*, will not be affected because they are used for identification purposes.

- **Internal processes for other servers (servers 2, 3 and 4)**

As in the case of server 1, the other servers have some internal procedures. This section will explain them as follows:

1- Create a new user.

Similar to the creation process on server 1, the new user needs to type the login details. The only difference here is that the user will need to enter the email address as a user ID and password. This information will be saved in the *wizard_user* table under the variable names *email* and *password*. The third variable, *userID*, will be assigned automatically by the system.

2- Select a privacy policy to apply to the site.

When the user logs into server 1 through one of these servers, he or she will be able to see a list of all privacy policies they created earlier. If the user selects a privacy policy to apply, all the identification details will be saved in the *wizard_favorite_setting* table. For example, Alice is a user who created three privacy policies, as shown in Table 4.7, which are saved in the server1 database.

#	Privacy policy Name	Alice ID (userID)	Privacy policy ID (ID)
1	Facebook and Twitter	233	60
2	Forums	233	61
3	Other social networks	233	62

Table 4.7. Alice's privacy policies.

The above details have been saved under Alice's account, and her identification number is "233". When she created three different privacy policies, each one was assigned a unique identification number, such as “60” for Facebook and Twitter and “61” for forums. The next step occurs when Alice signs up in server 2 and wants to apply a new privacy policy to it. At this point, Alice needs to log in to server 1 through server 2 by using the server 1 login details. The system will show her a list of all privacy policies created by user “233” (in this case, there are only three policies). After the selection process (e.g., Alice selects “forums”), these values will be saved in the *wizard_favorite_setting* table (settingID: “61”; settingname: “Forums”). The other two variables, *favesettingID* and *userID*, will be given automatically.

3- Changing the current privacy policy.

To change the current applied privacy policy on this site, the user needs to log in to the server and select “update the current privacy policy”. Indeed, Alice needs to log in to server 1 and repeat the same steps for selecting a privacy policy, but there is a difference between them. Changing the policy will allow the system to update the values *settingID* and *settingname* for the user based on the associated user ID in the *wizard_favorite_setting* table.

4.9.2.3 Communication processes between servers

The centralisation of personal information details on server 1 requires more procedures for communication and data sharing. Each procedure has limited access to some data, and the user in other servers will know exactly which information will be shared with these websites. This part will address some tasks that require information sharing between different servers.

1- View the current name of the applied privacy policy.

When the user requests that a system on server 2, 3 or 4 view the current name for the applied privacy policy, there is an internal process to contact the local database and return the value. In this case, the result will be obtained from the *settingname* column in the *wizard_favorite_setting* table based on the user ID.

2- Select a privacy policy from the server1 database.

Selecting a privacy policy to apply is the next step after creating an account. Therefore, it is important to log in to server 1 through the current server to import all privacy policies from it. As shown in Figure 4.22, there are several steps to apply to a privacy policy. First, the user logs into server 1 by entering the email address and password. Second, the authentication process verifies the user. Third, if the login details were correct, the system will return all privacy policies from the *permission* table in the server1 database that have been created by this user (*userID* will be used for this enquiry). Fourth, the names of these privacy policies will be added to the list on server 2 or other servers. Fifth, from the list, the user can select one policy to apply to the website. Sixth, the identification numbers (*ID* and *settingname*) will be saved in the *wizard_favorite_setting* table.

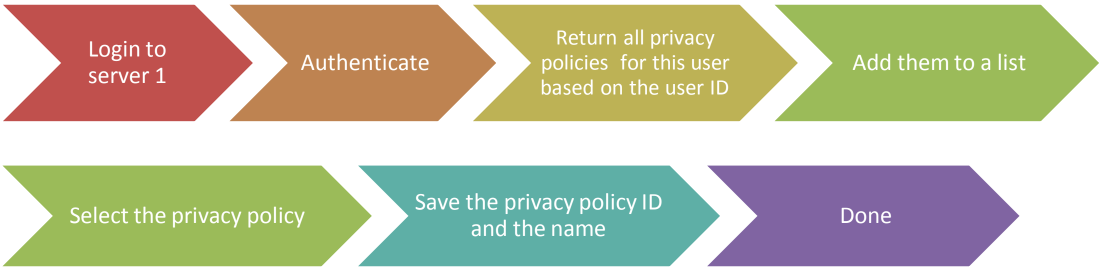

Login to server 1
Authenticate
Return all privacy policies for this user based on the user ID
Add them to a list
Select the privacy policy
Save the privacy policy ID and the name
Done

Figure 4.22. The process of importing and saving privacy policies from server 1.

3- Allow the browser to access personal information details.

The main aim of creating different privacy policies is to limit access to personal information details. This provides each website with controlled access based on the applied policy, with the user serving as the main manager for sharing this information. The procedure for gaining access to this data passes through several stages as follows:

- Calling the record that has all the variable values from the *wizard_favorite_setting* table based on the *userID* value.
- Running an enquiry to request a record that has similar values for both the *settingname* and *settingID* variables from the *permission* table in the server1 database. This record will have values to show or hide personal information items.
- Combining the *wizard_user* and *permission* tables in one enquiry to select all values for personal information items from the *wizard_user* table that have the authority to be shared with others based on the values in the *permission* table.

- Allow servers 2, 3 or 4 to read only these values and display them in the personal information page.

4- Adding a new privacy policy through server 2, 3 or 4.

One of the system's features is the ability to add a new privacy policy to the server1 database through other websites. Each website has internal files for the wizard system to transfer the user's selections to the server1 database. When the database receives these inputs, a specific procedure is applied based on them. Therefore, the system can offer more usability for users to add new privacy policies from any website, but as mentioned before, coordination and agreement between the companies and Internet application developers is necessary.

4.9.3 Code description

This section provides a description of the configuration structures for the suggested privacy system. As mentioned before, the Smart Wizard System was designed using ASP.NET as the programming language (using C#) and SQL Server structures.

4.9.3.1 Code description for server 1 (privacy system)

Registration page: On this page, the new user needs to register by filling in all required fields and using a unique email address (Figure 4.23). A duplicate email address is not allowed; therefore, the user must enter a unique email ID that has not been registered on the website. After successful registration, the user can log in to the website and set different privacy policies.

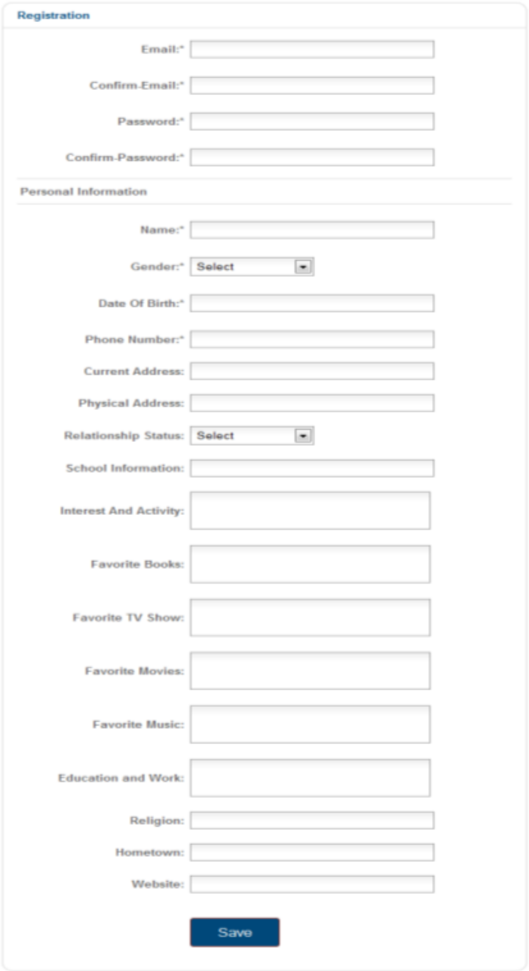


Figure *4.23. View of the registration page for server 1.*

When the user clicks on the “save” button, all entered values are saved into an object and then sent to the SQL server, where values are saved in the wizard_user table. Figure 4.24 presents the code and procedure used for this process.

Code:

```
    protected void btnregister_Click(object sender, EventArgs e)
    {
        permissionBLL objbl = new permissionBLL();
        objbl.ID = 0;
        objbl.name = txtname.Text;
        objbl.email = txtemail.Text;
        objbl.password = txtpassword.Text;
        objbl.hometown = txthometown.Text;
        objbl.gender = Convert.ToInt32(drpgender.SelectedValue);
        objbl.addressandcontact = txtaddress.Text;
        objbl.dateofbirth = txtdob.Text;
        objbl.phoneno = txtmob.Text;
        objbl.interestandactivity = txtinterest.Text;
        objbl.schoolinfo = txtschoolinfo.Text;
        objbl.favoritebooks = txtfavbook.Text;
        objbl.favoritemovies = txtfavmov.Text;
        objbl.favoritemusic = txtfavmusic.Text;
        objbl.favoritetvshows = txtfavtv.Text;
        objbl.religion = txtreligion.Text;
        objbl.educationandwork = txtedu.Text;
        objbl.physicaladdress = txtphysicaladdress.Text;
        objbl.website = txtwebsite.Text;
        objbl.relationshipstatus = drprlstatus.SelectedValue.ToString();
```

```
      Int32 dpcheck=Convert.ToInt32(objbl.fnAddUsersBL(objbl));
      if (dpcheck == -1)
      {  dupemail.Text = "Email Already Exists";}
      else
      {   dupemail.Text = string.Empty;
          Response.Redirect("login.aspx");}
        objbl = null;}
```

Store Procedure:

```
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE procedure [dbo].[wizard_add_user]
@name nvarchar(100),@ID int,@gender int,@mobile nvarchar(50),@email nvarchar(100),
@password nvarchar(100),@DOB nvarchar(50),@currentaddress nvarchar(200),
@schoolinfo nvarchar(200),@hometown nvarchar(100),@interestandactivity nvarchar(200),
 @favoritebooks nvarchar(200), @favoritetvshows nvarchar(200), @favoritemusic nvarchar(200),
 @favoritemovies nvarchar(200), @educationandwork nvarchar(200), @religion nvarchar(100),
 @website nvarchar(50), @relationshipstatus nvarchar(50), @physicaladdress nvarchar(200),
 @dpcheck int out
as
if (@ID=0)
begin
if exists(select * from Wizard_User where email=@email)
begin
set @dpcheck=-1
end
else
begin
insert into
Wizard_User(name,gender,mobile,email,password,dateofbirth,currentaddress,schoolinformation,hometow
n,interestandactivity,favoritebook,favoritetvshows,favoritemusic,favoritemovies,educationandwork,r
eligion,relationshipstatus,website,physicaladdress)
values(@name,@gender,@mobile,@email,@password,@DOB,@currentaddress,@schoolinfo,@hometown,@interest
andactivity,@favoritebooks,@favoritetvshows,@favoritemusic,@favoritemovies,@educationandwork,@reli
gion,@relationshipstatus,@website,@physicaladdress)
set @dpcheck=0
end
end
```

Figure 4.24. The code and store procedure for the registration page.

Login page: After successful registration, the user can log in to his or her account to gain access and create new privacy policies (Figure 4.25).

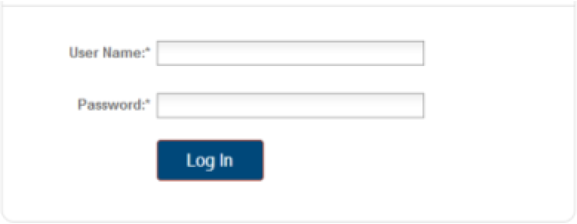


Figure 4.25. Login page.

When the "log in" button is clicked, the email address and password are sent to the SQL server for validation purposes. If they are valid, a unique user ID will be returned from the database to be saved into a session. It is also used to redirect the user to the dashboard, where he or she can control all privacy settings under his or her account (Figure 4.26).

Code:

```
    protected void LoginButton_Click(object sender, EventArgs e)
    {
        UserBLL objUserBll = new UserBLL();
        User objUser = objUserBll.ValidateUser(txtemail.Text.Trim(), txtpassword.Text.Trim());
        if (objUser.usr_id > 0)
        {
            Session["userID"] = objUser.usr_id;
            Session["user"] = txtemail.Text ;
            objUserBll = null;
            Response.Redirect("user-info.aspx");
        }
        else
        {   lblmessage.Text = "Invalid Username or Password."; }
    }
```

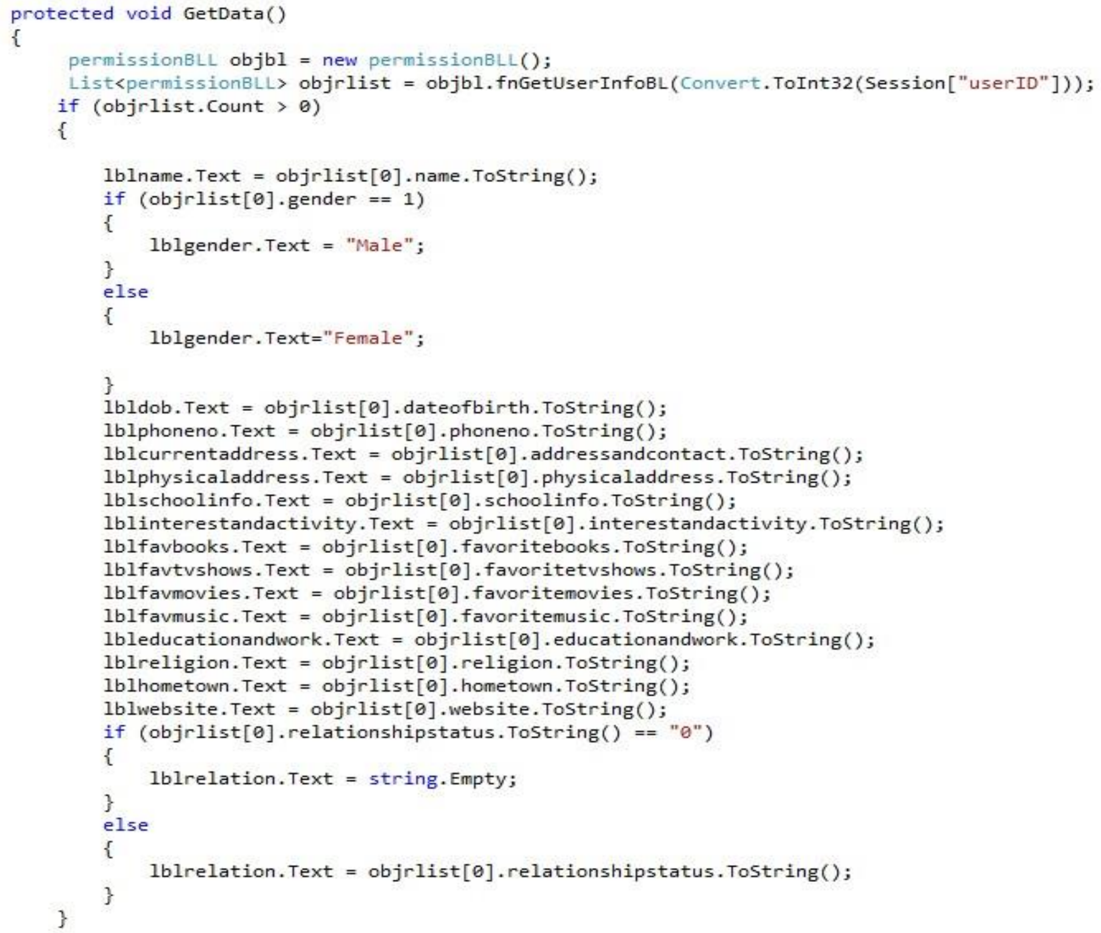
Store Procedure:

```
create procedure [dbo].[validate_user]
(
                 @login_name varchar(50),
                 @password varchar(50),
                 @usr_id int output
)
AS
set nocount on
declare @pwd varchar(50)
select @pwd=password
from Wizard_User  where email =@login_name

if @pwd=@password COLLATE SQL_LATIN1_General_CP1_CS_AS
        begin
                 select @usr_id=userID

                 from Wizard_User
where
                 email=@login_name and password=@password
        end
else
        begin
                 set @usr_id=-1
        end
```

Figure 4.26. The code and store procedure for the login page.

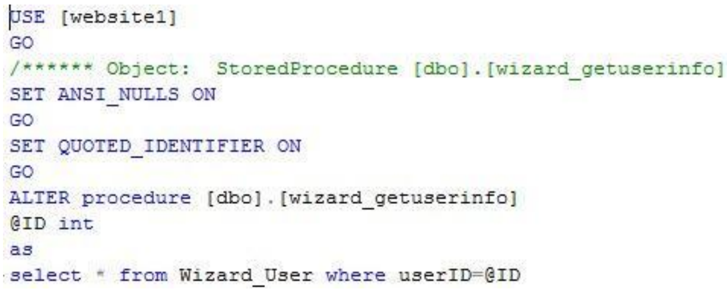
Personal information page: After the login process, the user is redirected to the user-info.aspx page, which has complete personal information details. In the loading process, the system checks whether or not the session is null. If it is not null, then the *GetData()* function will be called to obtain the user’s details based on his or her ID and display them in labels (Figure 4.27). Clicking on the “edit” button will redirect the user to the user-profile.aspx page, where this information can be edited.

Code:



```
protected void GetData()
{
     permissionBLL objbl = new permissionBLL();
     List<permissionBLL> objrlist = objbl.fnGetUserInfoBL(Convert.ToInt32(Session["userID"]));
    if (objrlist.Count > 0)
    {

        lblname.Text = objrlist[0].name.ToString();
        if (objrlist[0].gender == 1)
        {
            lblgender.Text = "Male";
        }
        else
        {
            lblgender.Text="Female";

        }
        lbldob.Text = objrlist[0].dateofbirth.ToString();
        lblphoneno.Text = objrlist[0].phoneno.ToString();
        lblcurrentaddress.Text = objrlist[0].addressandcontact.ToString();
        lblphysicaladdress.Text = objrlist[0].physicaladdress.ToString();
        lblschoolinfo.Text = objrlist[0].schoolinfo.ToString();
        lblinterestandactivity.Text = objrlist[0].interestandactivity.ToString();
        lblfavbooks.Text = objrlist[0].favoritebooks.ToString();
        lblfavtvshows.Text = objrlist[0].favoritetvshows.ToString();
        lblfavmovies.Text = objrlist[0].favoritemovies.ToString();
        lblfavmusic.Text = objrlist[0].favoritemusic.ToString();
        lbleducationandwork.Text = objrlist[0].educationandwork.ToString();
        lblreligion.Text = objrlist[0].religion.ToString();
        lblhometown.Text = objrlist[0].hometown.ToString();
        lblwebsite.Text = objrlist[0].website.ToString();
        if (objrlist[0].relationshipstatus.ToString() == "0")
        {
            lblrelation.Text = string.Empty;
        }
        else
        {
            lblrelation.Text = objrlist[0].relationshipstatus.ToString();
        }
    }
```

Store Procedure:



```
USE [website1]
GO
/****** Object:  StoredProcedure [dbo].[wizard_getuserinfo]
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
ALTER procedure [dbo].[wizard_getuserinfo]
@ID int
as
select * from Wizard_User where userID=@ID
```

Figure 4.27. The code and store procedure for the personal information page.

Adding new a privacy policy page: After successfully logging into the dashboard menu, the user is allowed to add a new privacy policy by clicking on “add new settings”. This will redirect him or her to the index page, where he or she can add a name for the new privacy policy (Figure 4.28). As mentioned before, this name will be used to distinguish processes between different privacy policies. After adding the privacy policy name, the user will be redirected to the wizard system pages, which were explained in the previous chapter (Figure 4.29). At this stage, the user can select from a list of options to create a specific privacy policy to secure personal information details against some issues that may pose privacy risks.

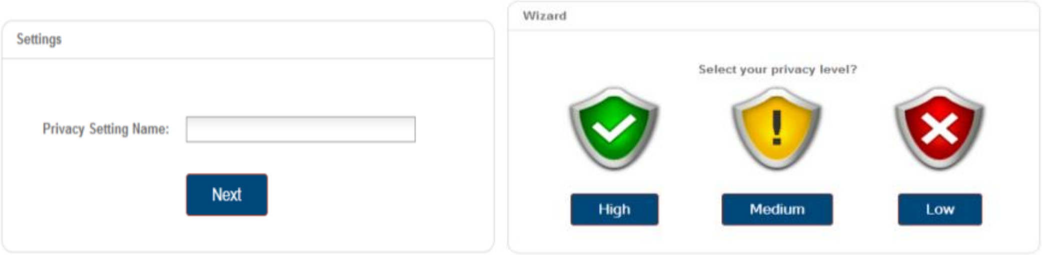


Figure 4.28. Adding a new privacy policy.

Code:

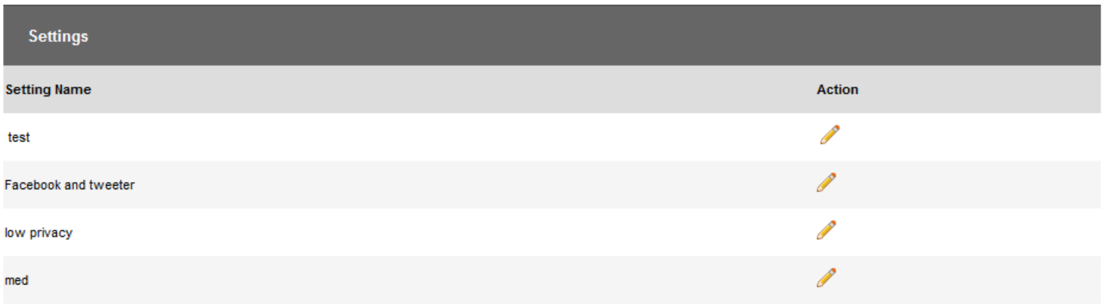
```
    protected void btnnext_Click(object sender, EventArgs e)
    {
        settingBLL objbl = new settingBLL();
        objbl.value = 1;
        objbl.settingname = txtsetting.Text;
        objbl.userID =Convert.ToInt32(ViewState["usr_ID"]);
        Int32 id = objbl.fnAddPrivacySettingsBL(objbl);
        objbl = null;
        Response.Redirect("gender.aspx?id=" + id);
    }
}
```

Store Procedure:

```
CREATE procedure [dbo].[permission_insert_settings]
(

@value int,
@ID int out,
@settingname nvarchar(300),
@userID int
)
as
begin

insert into permission(value,settingname,userID)values(@value,@settingname,@userID)
set @ID=scope_identity()
insert into user_accuracy(permissionID)values(@ID)
end
```

Figure 4.29. The code and store procedure for adding a new privacy policy.

Show all created privacy policy pages: Once the user has created a privacy policy for his or her account, the system offers an option to view all created privacy policies and provides the authority to modify any policy (Figure 4.30).



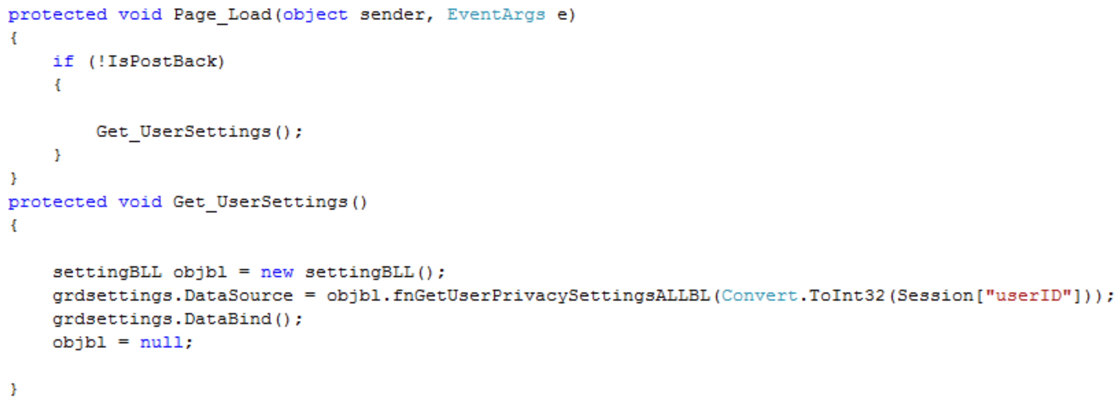
Settings

Setting Name	Action
test	✎
Facebook and tweeter	✎
low privacy	✎
med	✎

Figure 4.30. View all created privacy policies.

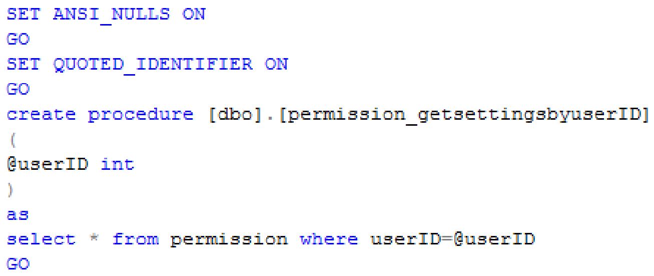
As shown in Figure 4.31, the system will request all names for the existing privacy policies from the *permission* table based on the user ID.

Code:



```
protected void Page_Load(object sender, EventArgs e)
{
    if (!IsPostBack)
    {

        Get_UserSettings();
    }
}
protected void Get_UserSettings()
{

    settingBLL objbl = new settingBLL();
    grdsettings.DataSource = objbl.fnGetUserPrivacySettingsALLBL(Convert.ToInt32(Session["userID"]));
    grdsettings.DataBind();
    objbl = null;

}
```

Store Procedure:



```
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
create procedure [dbo].[permission_getsettingsbyuserID]
(
@userID int
)
as
select * from permission where userID=@userID
GO
```

Figure 4.31. The code and store procedure for requesting the user's privacy policies.

4.9.3.2 Code description for other servers (servers 2, 3 and 4)

Registration page: This page represents an example of a social networking site. If this is the first visit to the website, the user must register as a new user. Only two fields need to be completed and confirmed by retyping the username and password (Figure 4.32). Once the user completes these fields and selects "save" to save these values in the internal database, he or she will be redirected to the login page. Duplicate usernames are not allowed in this system, so the user cannot register on this website twice using the same username.

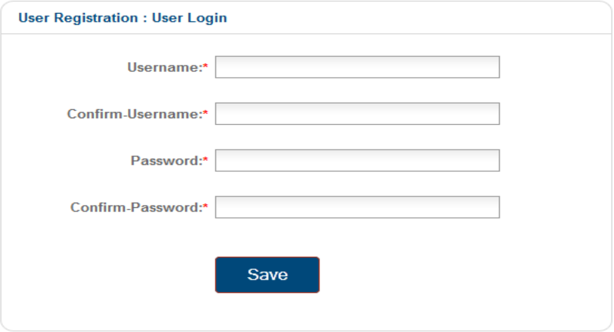
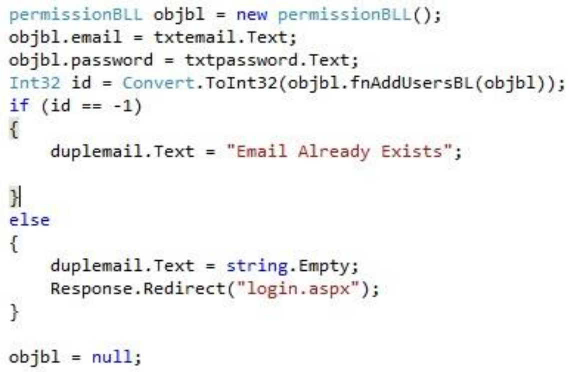


Figure 4.32. Screenshot of a new user creation window for servers 2, 3 or 4.

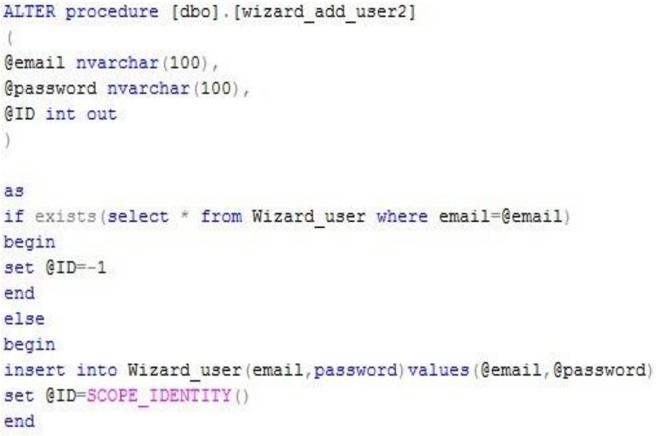
The code procedure sends the email address and password via an object (Figure 4.33). This object will pass these values to the SQL server to save them in its database. If the function *adduserBL* returns -1 as a value, the email address already exists and cannot be used for registration. If the value is not equal to -1, the user will be redirected to the login page.

Code:



```
permissionBLL objbl = new permissionBLL();
objbl.email = txtemail.Text;
objbl.password = txtpassword.Text;
Int32 id = Convert.ToInt32(objbl.fnAddUsersBL(objbl));
if (id == -1)
{
    duplemail.Text = "Email Already Exists";

}
else
{
    duplemail.Text = string.Empty;
    Response.Redirect("login.aspx");
}

objbl = null;
```

Store Procedure:

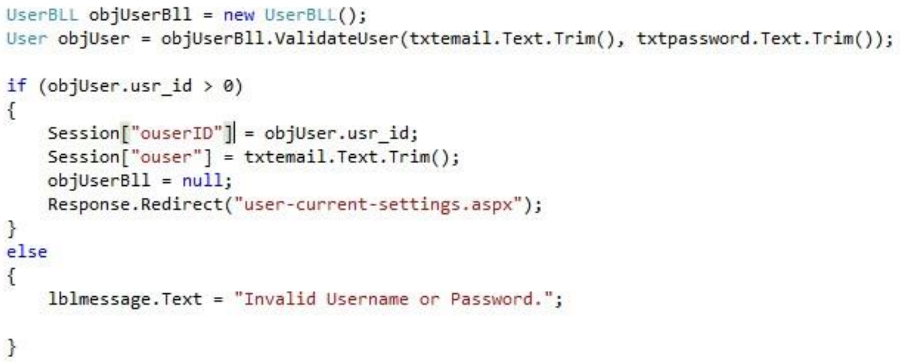


```
ALTER procedure [dbo].[wizard_add_user2]
(
@email nvarchar(100),
@password nvarchar(100),
@ID int out
)

as
if exists(select * from Wizard_user where email=@email)
begin
set @ID=-1
end
else
begin
insert into Wizard_user(email,password)values(@email,@password)
set @ID=SCOPE_IDENTITY()
end
```

Figure 4.33. The code and store procedure for the registration process for servers 2, 3 and 4.

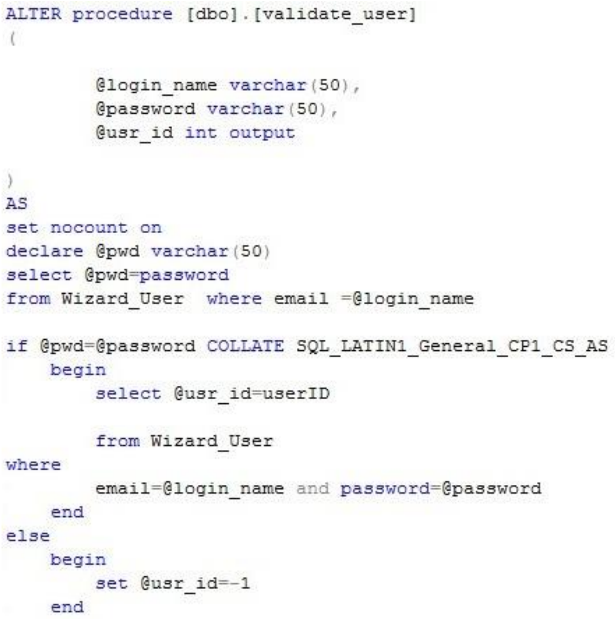
Login page: The login page is used to check the validity of the user account by entering his or her username and password. If these details are valid, the function will return an object that has a userID value to be used in the current session (Figure 4.34).

Code:



```
UserBLL objUserBll = new UserBLL();
User objUser = objUserBll.ValidateUser(txtemail.Text.Trim(), txtpassword.Text.Trim());

if (objUser.usr_id > 0)
{
    Session["ouserID"] = objUser.usr_id;
    Session["ouser"] = txtemail.Text.Trim();
    objUserBll = null;
    Response.Redirect("user-current-settings.aspx");
}
else
{
    lblmessage.Text = "Invalid Username or Password.";

}
```

Store Procedure:

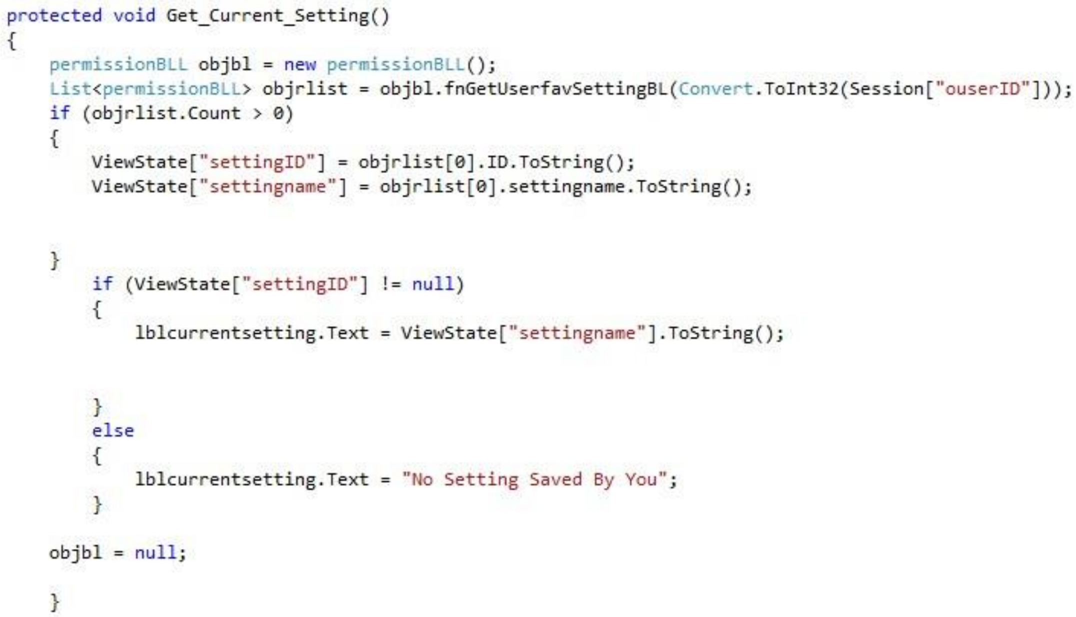


```
ALTER procedure [dbo].[validate_user]
(

        @login_name varchar(50),
        @password varchar(50),
        @usr_id int output

)
AS
set nocount on
declare @pwd varchar(50)
select @pwd=password
from Wizard_User  where email =@login_name

if @pwd=@password COLLATE SQL_LATIN1_General_CP1_CS_AS
    begin
        select @usr_id=userID

        from Wizard_User
where
        email=@login_name and password=@password
    end
else
    begin
        set @usr_id=-1
    end
```

Figure 4.34. The code and store procedure for the login page for servers 2, 3 and 4.

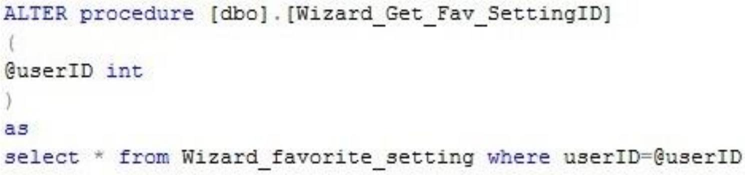
Current privacy settings page: This page shows the user the current selected privacy policy from server 1 and all the personal information details allowed to be seen on this website based on the selected privacy policy. When the page is loading, the function *get_current_setting* will be called to retrieve the current applied privacy policy. In this case, the *userID* value is necessary to return the values of both *settingID* and *settingname*, whether or not the values were null (if the value is null, the function will notify the user that there is no saved privacy policy for the website). These values will be transferred from this page to another by using the property *viewstate* (Figure 4.35).

Code:



```
protected void Get_Current_Setting()
{
    permissionBLL objbl = new permissionBLL();
    List<permissionBLL> objrlist = objbl.fnGetUserfavSettingBL(Convert.ToInt32(Session["ouserID"]));
    if (objrlist.Count > 0)
    {
        ViewState["settingID"] = objrlist[0].ID.ToString();
        ViewState["settingname"] = objrlist[0].settingname.ToString();


    }
        if (ViewState["settingID"] != null)
        {
            lblcurrentsetting.Text = ViewState["settingname"].ToString();


        }
        else
        {
            lblcurrentsetting.Text = "No Setting Saved By You";
        }

    objbl = null;

    }
```

Store Procedure:



```
ALTER procedure [dbo].[Wizard_Get_Fav_SettingID]
(
@userID int
)
as
select * from Wizard_favorite_setting where userID=@userID
```

Figure 4.35. The code and store procedure for importing the current applied privacy policy.

Selecting a privacy policy page: In this page, the user can import all created privacy policies from server 1 and add them to a list for selection purposes, as shown in Figure 4.36.

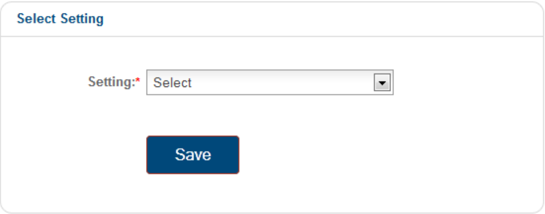
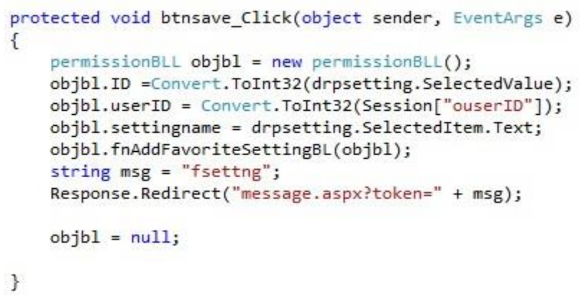


Figure 4.36. Selecting a privacy policy for the server 2 website.

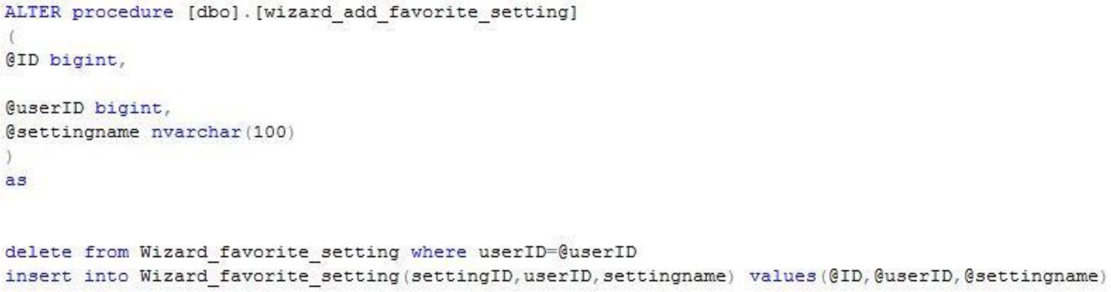
When the user selects a privacy policy from the list and clicks on the “save” button, the system will transfer the values for *user ID*, *setting name* and *setting ID* to the SQL Server database by using an object (Figure 4.37). This object is used to pass these values as parameters in a function (in this case, the function used is *fnAddFavoriteSettingBL*).

Code:



```
protected void btnsave_Click(object sender, EventArgs e)
{
    permissionBLL objbl = new permissionBLL();
    objbl.ID =Convert.ToInt32(drpsetting.SelectedValue);
    objbl.userID = Convert.ToInt32(Session["ouserID"]);
    objbl.settingname = drpsetting.SelectedItem.Text;
    objbl.fnAddFavoriteSettingBL(objbl);
    string msg = "fsettng";
    Response.Redirect("message.aspx?token=" + msg);

    objbl = null;

}
```

Store Procedure:



```
ALTER procedure [dbo].[wizard_add_favorite_setting]
(
@ID bigint,

@userID bigint,
@settingname nvarchar(100)
)
as


delete from Wizard_favorite_setting where userID=@userID
insert into Wizard_favorite_setting(settingID,userID,settingname) values(@ID,@userID,@settingname)
```

Figure 4.37. The code and store procedure for applying a privacy policy.

The allowed personal information page: This page presents all personal information details that the user has authorised to be shared with the website. This will be done by applying a specific privacy policy. When the user is redirected to this page, the system will request the personal information details from the server1 database in four steps. First, it will request the values for the applied privacy policy from the *permission* table. Second, the allowed items from this table with a value of 1 will be defined. Third, the values of these variables will be restored from the *wizard_user* table. Finally, these details will be viewed in labels, and the system will present a message, such as “not allowed for viewing”, for blocked items. As seen in Figure 4.38, the function *get_current_setting()* will be called when the page is loading to reach the current applied privacy policy, and after retrieving the current setting, the *get_user_info()* function will be called to get the personal information for the user according to the values of the applied privacy policy.

Code:

(both functions: *get_current_setting* and *get_user_info*)

```
    protected void Get_Current_Setting()
    {
        permissionBLL objbl = new permissionBLL();
        List<permissionBLL> objrlist = 
objbl.fnGetUserfavSettingBL(Convert.ToInt32(Session["ouserID"]));
        if (objrlist.Count > 0)
        {
            ViewState["settingID"] = objrlist[0].ID.ToString();
            ViewState["settingname"] = objrlist[0].settingname.ToString();
        }
            if (ViewState["settingID"] != null)
            { lblcurrentsetting.Text = ViewState["settingname"].ToString(); }
            else
            { lblcurrentsetting.Text = "No Setting Saved By You";}
            objbl = null;
        }
    protected void User_Info()
    {
       wizardBLL objbl = new wizardBLL();
        List<wizardBLL> objrlist = 
objbl.fnGetUserInfoBL(Convert.ToInt32(Session["userver1ID"]),Convert.ToInt32(
ViewState["settingID"]));
        if (objrlist.Count > 0)
        {

            lblname.Text = objrlist[0].pname.ToString();
            lblgender.Text = objrlist[0].pgender.ToString();
            lbldob.Text= objrlist[0].pdob.ToString();
            lblphoneno.Text= objrlist[0].pphoneno.ToString();
            lblcurrentaddress.Text = objrlist[0].pcurrentaddress.ToString();
            lblphysicaladdress.Text = objrlist[0].pphysicaladdress.ToString();
            lblschoolinfo.Text = objrlist[0].pschoolinfo.ToString();
            lblinterestandactivity.Text = objrlist[0].pinterestandactivty.ToString();
            lblfavbooks.Text = objrlist[0].pfbooks.ToString();
            lblfavtvshows.Text = objrlist[0].pfvtvshows.ToString();
            lblfavmovies.Text= objrlist[0].pfvmovies.ToString();
            lblfavmusic.Text = objrlist[0].pfvmusic.ToString();
            lbleducationandwork.Text = objrlist[0].peducationwork .ToString();
            lblreligion.Text = objrlist[0].preligion.ToString();
            lblhometown.Text = objrlist[0].phomtown .ToString();
            lblwebsite.Text = objrlist[0].pwebsite.ToString();
            lblrelation.Text = objrlist[0].prelationshipstatus.ToString();
            lblpictures.Text = objrlist[0].ppictures.ToString();
            lblvideos.Text = objrlist[0].pvideos.ToString();
            lblcomments.Text = objrlist[0].pcomments.ToString();
            lbltags.Text = objrlist[0].ptags.ToString();
            lblfrndlist.Text = objrlist[0].pfriendlist.ToString();
        }
        objbl = null;
    }
```

Store Procedure:

```
create procedure [dbo].[Wizard_Get_Fav_SettingID]
(
@userID int
)
as
select * from Wizard_favorite_setting where userID=@userID


CREATE procedure [dbo].[get_user_info_byprivacy]
(
@settingID int,
@ID int
)
as
select wu.*,p.* from Wizard_User wu
inner join
 permission p
 on p.userID=wu.userID
  where wu.userID=@ID and p.ID=@settingID
GO
```

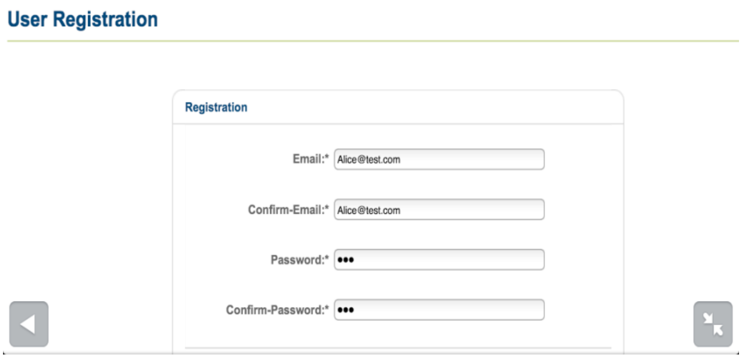
Figure 4.38. The code and store procedures for accessing personal information details.

4.10 Testing the whole privacy system

Testing the system is the next step after preparing and designing the system. In this case, Alice will be used as an example of a new user. First, she needs to create an account on server 1 (privacy system). This step can be done using different Internet devices, such as computers or mobile devices. It requires entering personal information details and creating different privacy policies; the data entry step will not be repeated, and the user has the ability to update her details later. As shown in the following scenario, Alice uses an iPhone to register in the system (all details used are fictitious and only for testing purposes).

Step 1: Create a new account

In this case, Alice uses Alice@test.com as the email address for the registration process (Figure 4.39).



User Registration

Registration

Email:* Alice@test.com

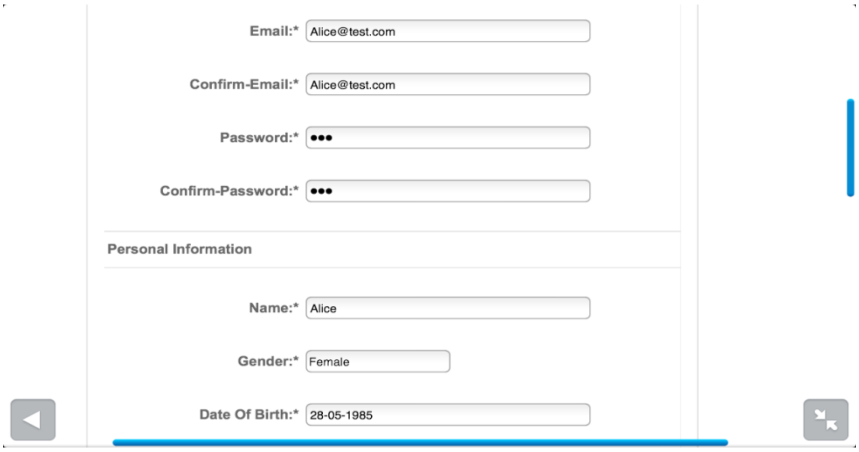
Confirm-Email:* Alice@test.com

Password:* •••

Confirm-Password:* •••

Figure 4.39. Registration page, part 1.

Step 2: By using the scrolling property, Alice will finish filling in her personal information details (Figure 4.40).



Email:* Alice@test.com

Confirm-Email:* Alice@test.com

Password:* ●●●

Confirm-Password:* ●●●

Personal Information

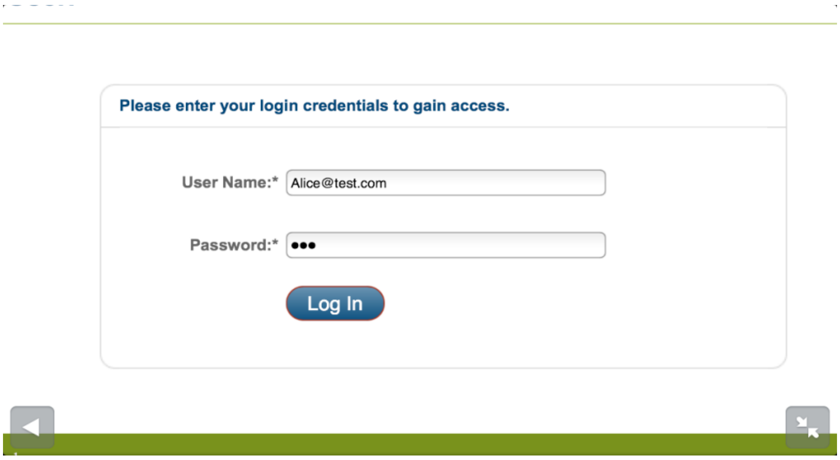
Name:* Alice

Gender:* Female

Date Of Birth:* 28-05-1985

Figure 4.40. Registration page, part 2.

Step 3: After completing the form, Alice is redirected to the login page, where she is required to enter her login details (Figure 4.41).



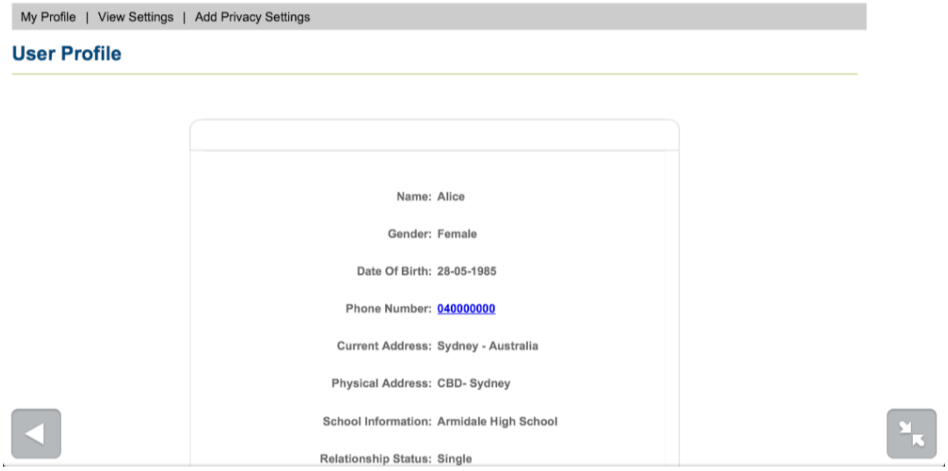
Please enter your login credentials to gain access.

User Name:* Alice@test.com

Password:* ●●●

Figure 4.41. Login page.

Step 4: After the login process, Alice can browse or update her profile and add new privacy policies (Figure 4.42). The “view settings” option allows her to see all the created privacy policies (Figure 4.43).



Name: Alice

Gender: Female

Date Of Birth: 28-05-1985

Phone Number: 040000000

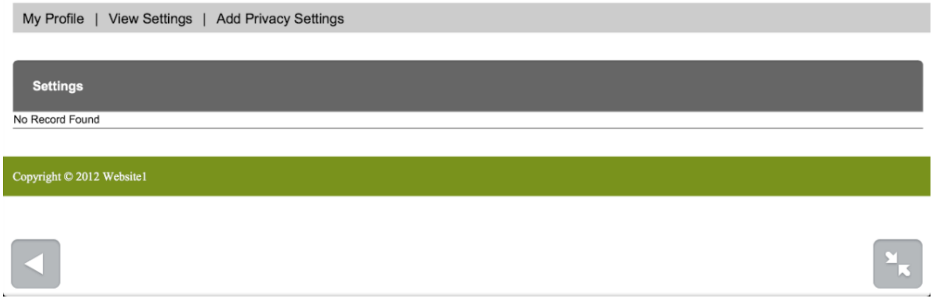
Current Address: Sydney - Australia

Physical Address: CBD- Sydney

School Information: Armidale High School

Relationship Status: Single

Figure 4.42. Main page.

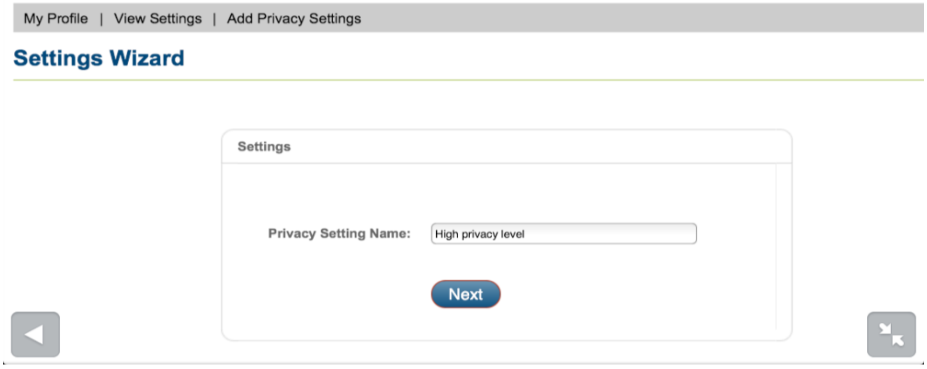


No Record Found

Copyright © 2012 Website1

Figure 4.43. View all created privacy policies.

Step 5: To add a new privacy policy, Alice clicks on "add privacy settings" in the command toolbar (Figure 4.44). After clicking on this link, she is asked to type a name for the policy for identification purposes. In this case, Alice types "high privacy level".



Privacy Setting Name: High privacy level

Figure 4.44. Creating a new privacy policy.

Step 6: The next steps use the Smart Wizard System to help Alice set her personal information privacy for the new policy (Figure 4.45).

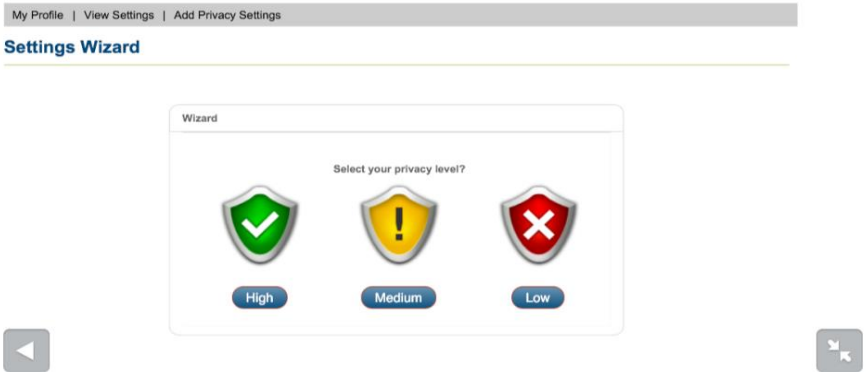
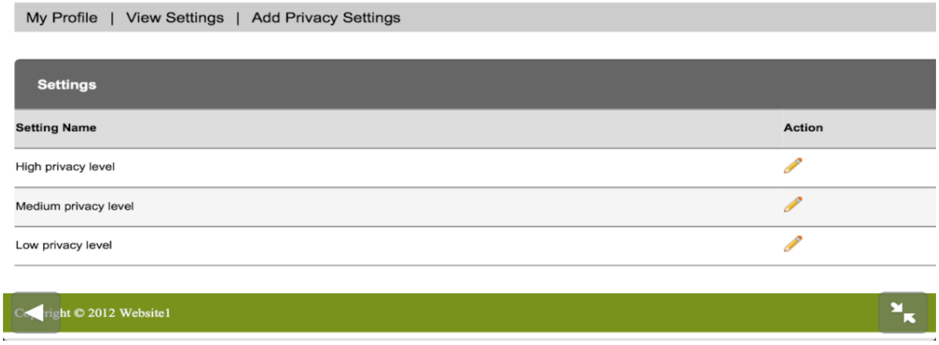

My Profile | View Settings | Add Privacy Settings
Settings Wizard
Wizard
Select your privacy level?
High
Medium
Low

Figure 4.45. Using the Smart Wizard System for adding and adjusting privacy policies.

Step 7: Alice repeats the previous two steps to add another privacy policy. In this example, she has three different levels of privacy policies (high, medium and low) and will apply each of them to a different website (Figure 4.46). These websites will act as real sites that request access to obtain personal information details from the server1 database.



Settings

Setting Name	Action
High privacy level	✎
Medium privacy level	✎
Low privacy level	✎

Figure 4.46. View all created privacy policies.

The following table shows all of the privacy settings for 23 personal information items set by three different privacy policies (✗ means that the item is not allowed to be shared and ✓ means that it can be shared).

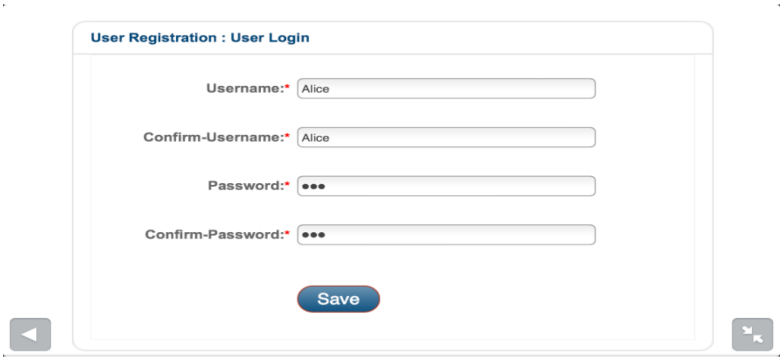
Privacy policy name	Name	Gender	Email	Date of birth	Phone number	Physical address	Current address	School information	Hometown	Interest and activity	Favourite books	Favourite TV shows	Favourite music	Favourite movies	Relationship status	Pictures	Videos	Comments and post	Tags	Friends list	Education and work	Religion	Website
High privacy level	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Medium privacy level	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓
Low privacy level	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓

Table 4.8. The status of sharing personal information items based on different privacy policies.

These are all the steps that need to be performed on the privacy system server. The next stage is linking the other websites with the privacy system server to obtain access to specific personal information details.

In this case, if Alice wants to subscribe to any other websites (server 2, 3 or 4), such as Facebook or Twitter, she needs to create a new user on these websites and import the desired privacy policy from server 1. The following steps illustrate how this is done.

Step 1: When Alice visits a website and clicks on “like” to subscribe to it through her Internet mobile device, she is required to register as a new user (Figure 4.47). It is not necessary for the username to be similar to the one in server 1, and she only needs to type a username and password.



User Registration : User Login

Username:* Alice

Confirm-Username:* Alice

Password:* ●●●

Confirm-Password:* ●●●

Figure 4.47. Creating a new user on server 2, 3 or 4.

In this step, Alice enters only two variables (username and password), and this shows the simplicity of using Internet mobile devices for registration.

Step 2: The next step is to log in by typing in the login details (Figure 4.48).

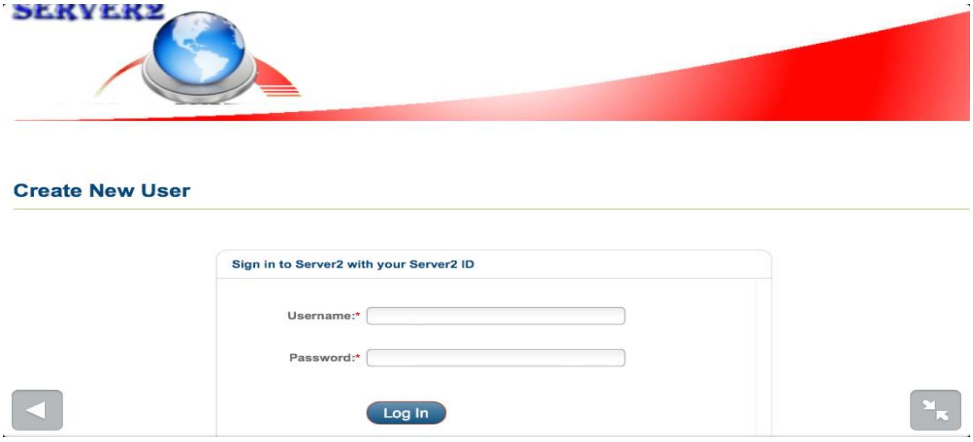
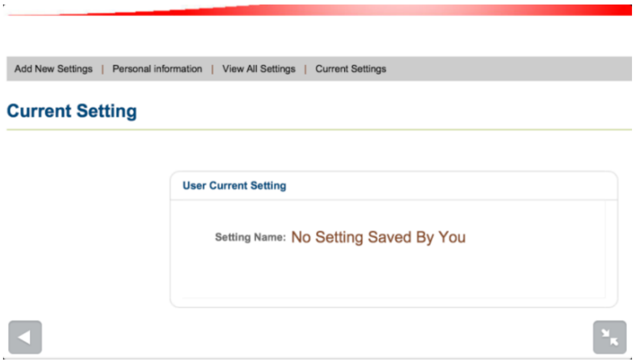


Figure 4.48. Login process on servers 2, 3 or 4.

Step 3: After the login process, Alice is redirected to her profile page, where she can import one privacy policy from server 1 to apply it to the website (Figure 4.49).



Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting

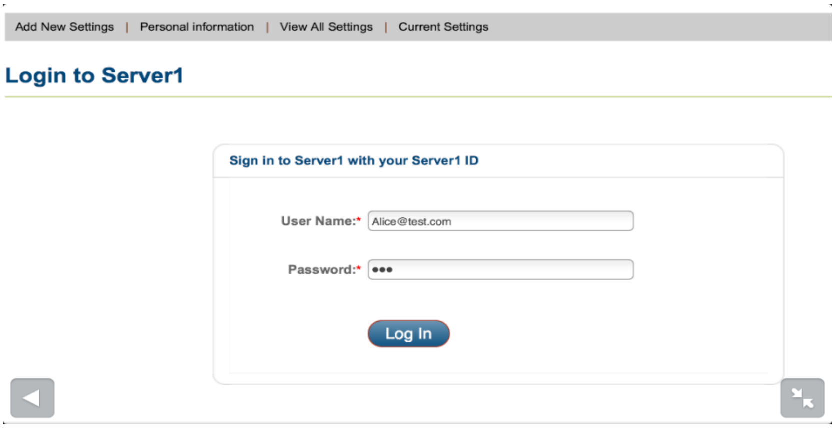
Setting Name: No Setting Saved By You

Figure 4.49. Alice's account main page.

On the main page, there are four options: add new settings, personal information, view all settings and current settings. These provide the user with the authority to communicate and import a privacy policy from server 1 and can be described as follows:

- Add new settings: This option allows the user to add a new privacy policy to server 1 directly through server 2, 3 or 4 without needing to browse the website for server 1.
- Personal information: This option lets the user know what personal information will be shared with the website and what is not allowed.
- View all settings: By clicking on this option, the user will be asked to log into server 1 to browse all the privacy policies that have been created thus far. All these settings will be displayed in a list, and the user will select one to apply to the website.
- Current settings: This selection tells the user about the privacy policy currently applied to this website.

Step 4: To apply an existing privacy policy to the website, Alice needs to click on "view all settings". She then uses the server 1 login details to import all the existing privacy policies on server 1 (Figure 4.50).


Add New Settings | Personal information | View All Settings | Current Settings
Log In

Login to Server1

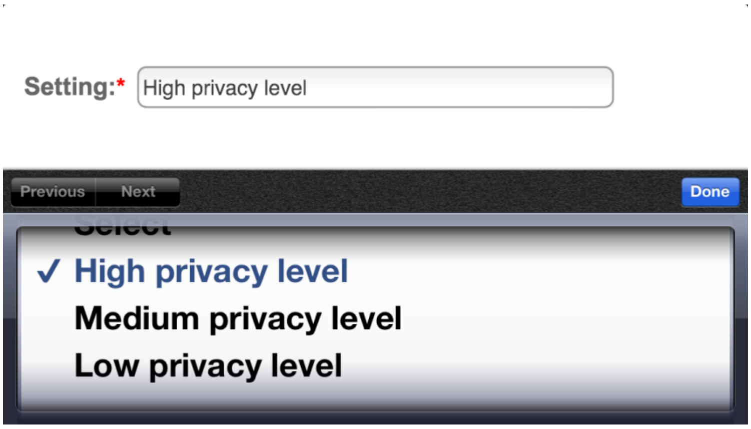
Sign in to Server1 with your Server1 ID

User Name:* Alice@test.com

Password:* •••

Figure 4.50. Log into the server 1 database through server 2, 3 or 4.

If the login is successful, then Alice will be able to select the suitable privacy policy from the list, as shown in Figure 4.51.



Setting:* High privacy level

Select

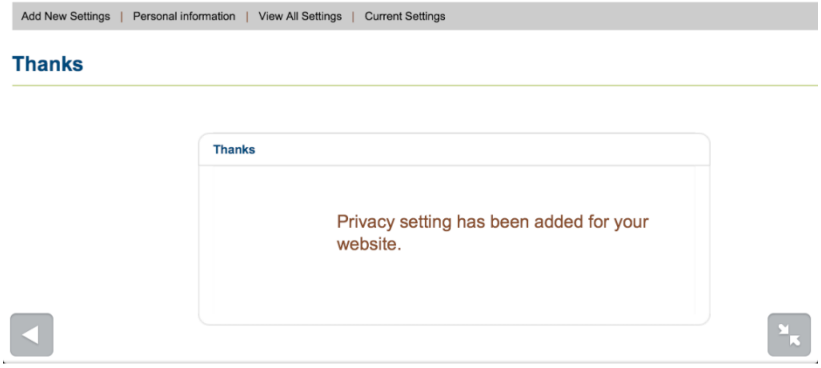
✓ High privacy level

Medium privacy level

Low privacy level

Figure 4.51. Selecting one privacy policy from the list.

Step 5: Saving the selected privacy policy is the next step (Figure 4.52). Clicking on the “save” button stores all identification variables for this policy in the database of server 2, 3 or 4. These variables all have identification details that need to communicate with the server 1 database and retrieve only the allowed personal information.



Add New Settings | Personal information | View All Settings | Current Settings

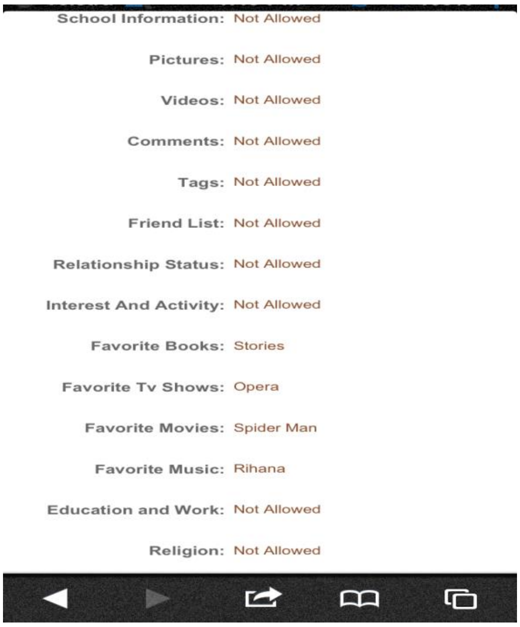
Thanks

Thanks

Privacy setting has been added for your website.

Figure 4.52. Saving a privacy policy.

Step 6: At this stage, Alice can see which personal information items are allowed to be shared with this website by clicking on “personal information” (Figure 4.53). The phrase “not allowed” will appear next to items that will not be shared.

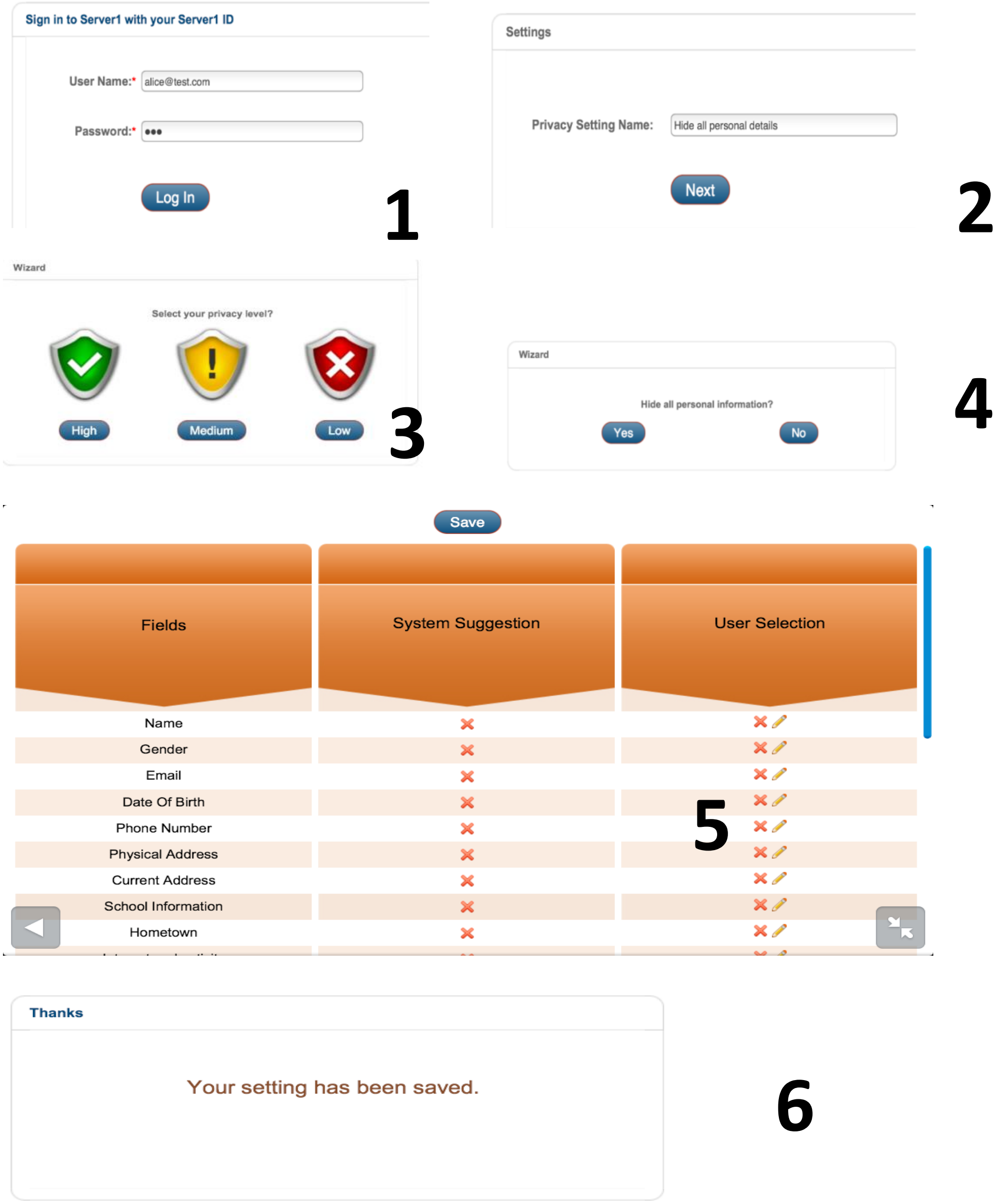


School Information:	Not Allowed
Pictures:	Not Allowed
Videos:	Not Allowed
Comments:	Not Allowed
Tags:	Not Allowed
Friend List:	Not Allowed
Relationship Status:	Not Allowed
Interest And Activity:	Not Allowed
Favorite Books:	Stories
Favorite Tv Shows:	Opera
Favorite Movies:	Spider Man
Favorite Music:	Rihana
Education and Work:	Not Allowed
Religion:	Not Allowed

Figure 4.53. An example of applying "high privacy level" to this website.

When the user wants to change the current applied privacy policy, he or she only needs to repeat steps 4 and 5.

Step 7: To add a new privacy policy to server 1 directly through server 2, 3 or 4, Alice must click on "add new settings". Clicking on this option shows the user a window with two fields for typing in the login details for server 1. After a successful login, Alice can use the Smart Wizard System to add the new privacy policy (Figure 4.54).



1

Sign in to Server1 with your Server1 ID

User Name:* alice@test.com

Password:* ●●●

2

Settings

Privacy Setting Name: Hide all personal details

3

Wizard

Select your privacy level?

4

Wizard

Hide all personal information?

5

Fields	System Suggestion	User Selection
Name	✗	✗ ✎
Gender	✗	✗ ✎
Email	✗	✗ ✎
Date Of Birth	✗	✗ ✎
Phone Number	✗	✗ ✎
Physical Address	✗	✗ ✎
Current Address	✗	✗ ✎
School Information	✗	✗ ✎
Hometown	✗	✗ ✎

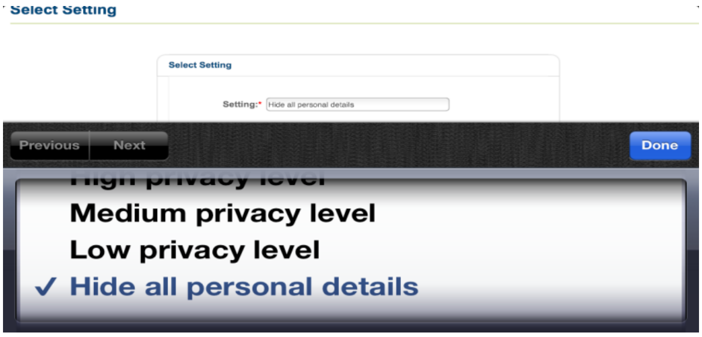
6

Thanks

Your setting has been saved.

Figure 4.54. Creating a new privacy policy through the websites of server 2, 3 or 4.

Step 8: The procedure to apply the new privacy policy is similar for step 4, and when the user browses the list, the new privacy policy will be added (Figure 4.55).



Select Setting

Select Setting

Setting:* Hide all personal details

Figure 4.55. The new privacy policy has been added to the list.

Repeating these steps for all other websites will result in setting a different privacy policy for each site. In the previous example, Alice selected “high privacy level” for the server 2 website. These steps were repeated for server 3 and server 4, but “medium privacy level” was selected for server 3 and “low privacy level” for server 4.

4.11 Conclusion

This chapter discussed the methodology used to design the proposed privacy framework. It outlined the stages of data collection within this study and explained the analysis procedure for each hypothesis. It also described all necessary steps for designing the Smart Wizard System and the whole privacy system. The author used standards to ensure and measure the validity and reliability of the used data.

However, the rapid increase in the use of Internet mobile devices, as discussed in Chapter 2, encouraged this study to develop a framework to enhance privacy awareness of mobile Internet systems and to protect users’ personal information privacy. Rather than discussing the privacy risks for personal information details and setting out to validate the measures in various studies, this study suggested and tested a privacy framework that provides Internet users with more control over the processes of distributing and sharing their personal information details via different online sites. As mentioned before, all data was analysed, and both systems were tested, so Chapter 5 will discuss the results of each task in this study.

Chapter 5: Results and Analysis

5.1 Introduction

This chapter presents the empirical findings of the study and discusses the results of implementing both the Smart Wizard System and the proposed privacy framework. As mentioned in the previous chapter, there were five tasks involved in designing the proposed privacy framework. This chapter will therefore discuss and analyse the findings by using statistical data analysis using SPSS for the selection of privacy settings in both systems.

The following research question was established for this study in order to design a framework that enhances privacy awareness in mobile systems:

> *How can online personal information privacy issues be addressed satisfactorily in an integrated services scenario involving different types of mobile devices, in order that the confidence of users in the effective protection of their personal details from misuse can be increased?*

5.2 Questionnaire Results

5.2.1 Data quality and characteristics of respondents

This section provides, through careful review and examination, a statistical analysis to ensure the data quality and its suitability for the first task of the study. The questionnaire contains several questions related to the attributes of respondents (such as gender and age). The survey was available in two languages: English and Arabic. A total of 185 respondents completed the survey (95 respondents used the Arabic form, and 90 used the English form); however, only 177 participants finished the survey.

The exclusion of cases followed Allison's (2000) approach by applying listwise deletion on all variables in the procedure for handling missing data by excluding data with missing values; thus, 8 cases were excluded. The data were carefully reviewed and all uncompleted responses excluded. The results show that the excluded cases represented only 4.3% of the total number of participants.

The 185 participants in the study comprised 157 males and 28 females. The age range 18–25 represented the majority group and accounted for 75% of all respondents. The reliability of a question type can be measured by using different scales (Litwin, M. S. 1995); the Alpha scale was chosen for this study. The results are shown in Table 5.1.

Case Processing Summary

		N	%
Cases	Valid	177	95.7
	Excluded[a]	8	4.3
	Total	185	100.0

a. Listwise deletion based on all variables in the procedure

Reliability Statistics

Cronbach's Alpha	N of Items
0.880	57

Table 5.1: Using the Alpha scale to calculate the reliability of the survey

Most respondents had their own mobile phones, which were also used to browse the Internet; hence, Table 5.2 presents the answers for the first section of the survey.

Field		No. of respondents	Percent %
Gender?			
	Male	157	84.9
	Female	28	15.1
Age?			
	18–25	141	76.2
	26–45	42	22.7
	46 or older	2	1.1
Having a mobile phone?			
	Yes	184	99.5
	No	1	0.5
Using mobile phone for browsing the Internet?			
	Always	70	37.8
	Sometimes	100	54.1
	Never	15	8.1
Normally, where do you use mobile phone to browse the Internet?			
	In the car	12	6.5
	At home	92	49.7
	At work	11	5.9
	Other	37	20.0
	More than 1 place	32	17.3
To browse the Internet do you use?			
	Mobile	5	2.7
	Computer	51	27.6
	Both mobile and computer	128	69.2

Table 5.2: Analysis of the survey data for 'Section one'

5.2.2 Usage of online social network accounts and Internet mobile devices

To discover and understand the online users who have social network accounts, participants were asked to answer some questions related to their usage, the number of friends on their friends' list and the time they spent browsing. Consequently, as shown in Figure 5.1, the survey shows that more than 45% of respondents had more than one social network account, and 32.4% of all respondents used Facebook accounts. Moreover, 48.1% visited their accounts from one to five times per day, and 40% spent about 30 minutes per day browsing their accounts (the others spent more than 30 minutes).

In addition, a rapid increase in the use of social networks was apparent. The survey showed that about 37% of respondents had social network accounts for more than three years and that the percentage had more than doubled in the last three years. This increase may be due to many factors: one factor is the widespread use of mobile phones, especially considering that the survey revealed that about 70% of respondents used both mobile phones and computers to browse the Internet.

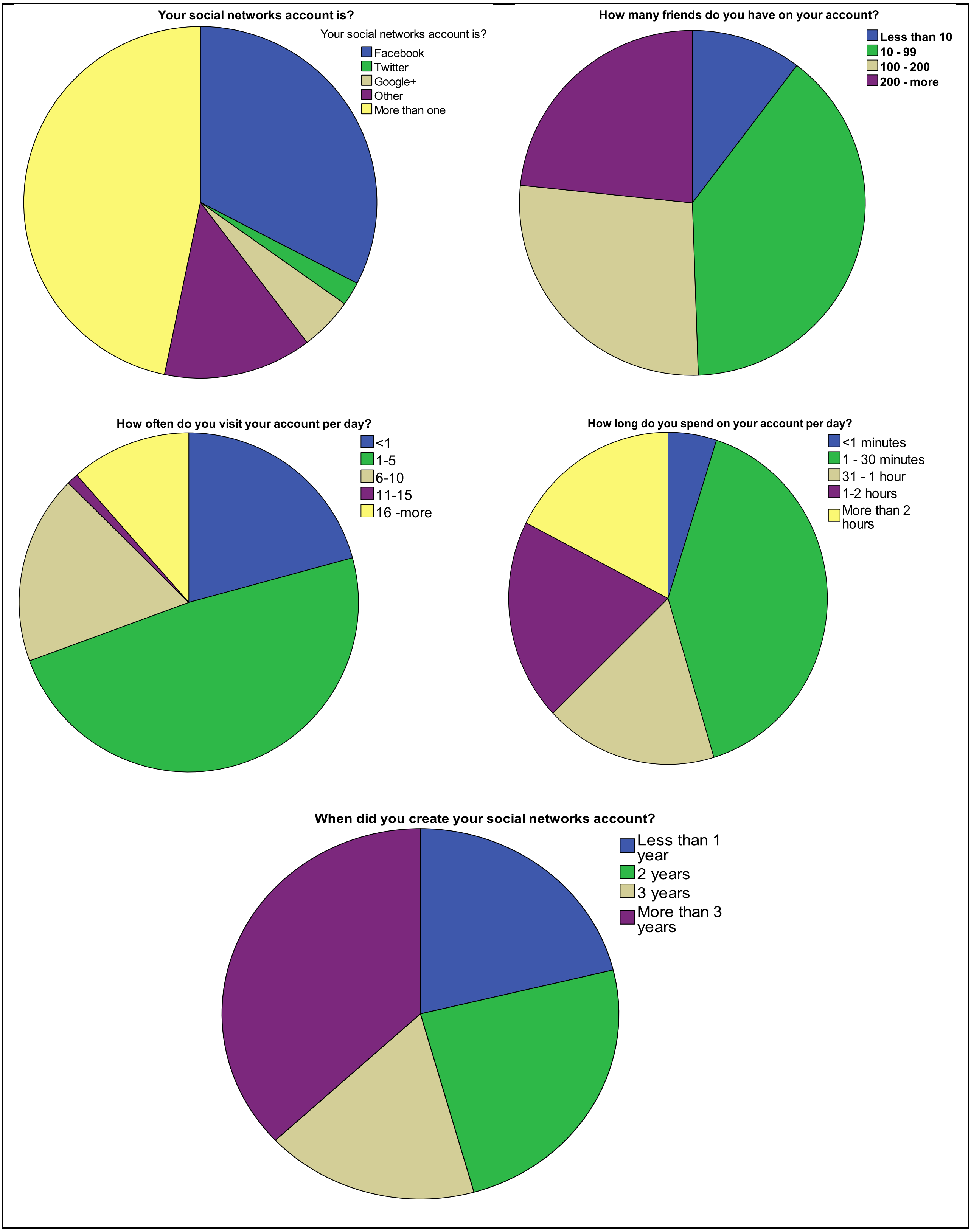


Figure 5.1: Analysis of survey data 'Section two'

The survey showed that participants used their mobile phones for a variety of uses. Most of the respondents used mobile services, such as accessing email, chatting and accessing social networks. As shown in Figure 5.2, the mean of respondent answers for using mobile services ranged from 52% to 65.4%. This confirmed that mobile phones were not only used for making phone calls but also to access other services. Because of the annual increase in the number of users of social networks and mobile phones to browse the Internet, mobile services need to improve to be more suitable for users.

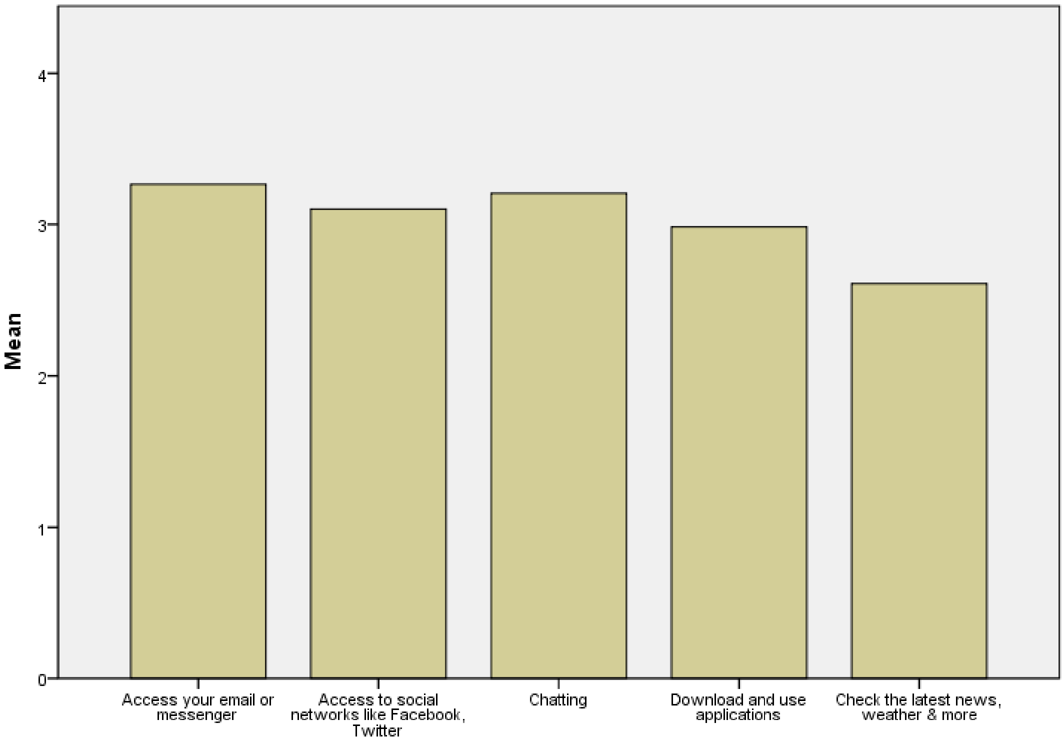


Figure 5.2: Analysis of use of mobile services

5.2.3 Awareness of privacy settings

The fourth section of the survey was divided into three categories where each category measures one concept. The three concepts measured were privacy settings, misuse of personal information and using mobiles to change privacy settings.

Firstly, the two aims of this subsection were to define whether users were aware of privacy settings (the first concept to be measured), and whether they were aware of the risks of private information leakage (the second concept to be measured). The results showed that most users *were* aware of privacy settings but most left them unchanged. For greater clarification, the survey asked the respondents if participants were interested in controlling the privacy settings for their accounts (Table 5.3). The results show that 67% of respondents were interested in controlling their privacy settings, and about 60% of respondents changed their privacy settings. Also, the percentage showing whether respondents were familiar with using privacy settings was close to the percentage of users who have changed their privacy settings for online social networks accounts: it showed that about 66% of users were familiar with the settings, and 73% said they could prevent others from seeing their personal information. Although about 71% of respondents were completely satisfied with their method of selecting privacy settings, about 57% did not regularly change their privacy settings.

Question	Yes	No	I don't Know
	%	%	%
Are you interested in controlling the privacy settings for your account?	67	23.8	9.2
Have you changed your privacy settings on your account?	59.5	35.1	4.9
Are you familiar with using your privacy settings?	65.9	25.9	3.2
Do you regularly change your privacy settings?	40	56.8	3.2
Are you completely satisfied with the method of selecting the privacy settings in your account?	71.4	18.4	10.2
Can you prevent other users from seeing your personal information?	73	19.5	7.5

Table 5.3: Analysis of survey data for 'Section four A'

Secondly, this subsection aims to measure if respondents were aware of the risks that could occur from the leakage of personal information. Moreover, as shown in Table 5.4, the results indicated a pattern. For further illustration, there is a question asking if the respondents used real information on their accounts. The results showed that about 64% of respondents used real information and about 34% did not. Also, there was another question asking if they were worried about the misuse of their personal information. The result was significantly close to the previous result. It showed that 66.5% of respondents were worried about misuse of their personal information, which is close to the percentage of respondents who used real personal information. In addition, the percentage of respondents who did not want strangers accessing their personal information is 68.6%, and this is close to the results for respondents who used real information and were worried about misuse of their personal information.

Likewise, the responses to two other survey questions indicated that a majority of users were concerned about privacy. One question asked if the respondents sometimes received an invitation to add a friend from an unknown person. The other question asked if they accepted those invitations. The results indicated that about 71% of respondents received such invitations, but about 68% answered that they did not accept such invitations for friends from an unknown person. Also, there is a convergence in the ratios between the users who did not use real personal information and the users who accepted invitations from unknown people. Finally, the respondents were asked if they knew if the account providers shared their profile information with other websites or not, and only about 44% selected 'No'. This leads to the necessity of developing a framework providing users with the authority to allow or disallow websites to use their personal information.

Question	Yes	No	I don't Know
	%	%	%
Are you worried about the misuse of your personal information?	66.5	26.5	7
Does your account provider share your profile information with other websites?	35.1	44.3	20.5
Do you sometimes receive an invitation to add a friend from an unknown person?	71.4	23.7	4.9
Do you sometimes accept an invitation to add a friend from an unknown person?	26.5	68.1	5.4
Do you use real personal information in your account?	64.3	33.5	2.2
Do you want strangers to see your profile?	23.8	68.6	7.6

Table 5.4: Analysis of survey data for 'section four B'

Finally, using a mobile phone to change privacy settings is one of the concepts that the survey sought to measure. Indeed, as shown in Table 5.5, there are three questions related to privacy settings. The first question asked if the respondents used their mobile phones to change their privacy settings. Only 34% of respondents used their mobile phones to change their privacy settings, and about 53% said they did not. Also, a question was asked whether the size of the mobile phone screen was suitable to control the privacy settings. About 42% of participants chose 'No' and about 17% were 'Not sure'. Similarly, when the participants were asked if it was easy to change the privacy settings through their mobile phones, about 42% chose 'Yes', 37% chose 'No' and about 21% chose 'Not sure'.

Question	Yes	No	I don't Know
	%	%	%
Do you use your mobile phone to change the privacy settings?	34	53	13
Is the size of your mobile screen suitable to control the privacy settings	41	42.2	16.8
Is it easy to change the privacy settings for your account through your mobile phone?	42.2	36.8	21.1

Table 5.5: Analysis of survey data for 'section four C'

On the other hand, providing information about the comparison between the answers of participants from the two different cultures can assist the researcher in the design of the system. It will be an important comparison that can be used to design the smart wizard tools. Table 5.6 showed some important facts that were founded from analysing the survey. It presented the differences between the use of social networking sites and mobile web systems.

Firstly, the results, related to the use of smartphones, showed that people who filled the English form used their smartphones to browse the internet more than Arabic people, and the common place of using them is at home more than the work place. This information assisted the researcher to take into account the need for simplicity in the design to suit the smartphones' screens in order to simplify the process of selecting privacy policies through smartphones or tablets. The use of smartphones did not ignore the use of desktop computers or laptops for browsing the internet. The evidence shows that both computers and smartphones were still working beside each other. About 75% of users who answered the English form used smartphones and personal computers to browse the internet, while about 63% of Arabic participants used both of them. Moreover, cultural development and the awareness about the content of the internet in these countries may affect diversity in the use of internet services via smartphones. For example, downloading mobile applications for Arabic participants had a higher percentage than English participants. About 28% of Arabic participants always downloaded applications via smartphones compared to about 7% of English language participants.

Secondly, the survey results about the use of social networking sites were fairly close and presented some similarities between the two sample groups. While the possession of the account, starting from the date of creation, was favoured by English language participants, the number owning more than one account in different social networking sites was close and showed that about half of both samples had more than one account. This shows that participants may have more accounts with the rapid increase in the number of social networking sites and this needs more control in profiles. In addition, the results showed about half of participants visited their accounts from one to five times daily and about 23% of Arabic participants spend more than two hours surfing their accounts. This is more evidence that shows the use of social networking sites is growing in the developing countries.

Thirdly, comparing privacy concerns in the two different cultures can provide the researcher with a clear picture about the classifications needed to design the smart wizard system. There were about 44% of Arabic participants and 33% of English participants who did not read the privacy terms and policies. The language used for writing the terms and policies, the complexity of the content or general lack of awareness could be reasons for neglecting to read this information. So, the proposed design should use simple methods to present user's privacy rights in a simple way. While a high percentage of both participants had concerns about misuse of personal information, more than half of them had some difficulties in changing the privacy settings via smartphones. About 82% of Arabic participants were satisfied with the current methods of selecting privacy settings, but only about 62% of English participants who were satisfied. The differences between the two cultures in the experience in dealing with social networking sites, the awareness of privacy concerns and the use of the technology could be reasons to account for differences in the percentage. Moreover, when asking participants if the service provider shares their personal information with other sites, the result showed about 35% of both samples answered ‘yes’ and about 20% ‘do not know’ if personal information was shared with other sites. The proposed privacy framework in this study is designed to alter this ratio in the users’ favour by giving the user the full authority to control and define which information can be shared with other sites. This will set up the user as an administrator of their information sharing processes.

Subject	Answer	Language	
		Arabic	English
Using smartphones for browsing the internet.	Always	28.7%	45.9%
The usual place where smartphones are used for browsing the internet.	At home	47.7%	52%
The device used to browse the Internet.	Computers and mobile devices	62.8%	75.5%
Owning an account in social networking sites.	More than one	47.7%	45.9%
Number of friends or followers for the participant's account.	200 or more	18.6%	27.6%
Visits to the social networking account per day.	From 1 to 5	46.5%	50.5%
Time spent on surfing the account.	More than two hours	23.3%	12.4%
The account creation.	More than three years	30.2%	42.9%
Accessing email address or messenger application.	Always	33.7%	22.4%
Accessing social networking sites.	Always	31%	18.4%
Using chatting applications	Always	32.6%	23.5%
Download applications	Always	27.6%	7.1%
Checking the latest news, weather and more	Always	13.8%	18.4%
Reading the privacy terms and policies for the social networking account.	No	44.8%	33.7%
Interest in controlling the privacy settings for the account.	Yes	71.3%	63.3%
Concerns about misuse of personal information	Yes	67.8%	65.3%
Has the participant changed the privacy settings for the account?	Yes	57.5%	61.9%
Is the participant familiar with using the privacy settings?	Yes	73.6%	59.2%
Does the participant regularly change the privacy settings?	No	51.7%	61.2%
The use of smartphones to change the privacy settings.	Yes	27.6%	39.8%
Suitability of mobile screen to change the privacy settings.	Yes	35.6%	45.9%
Satisfaction of the participant with the method of selecting the privacy settings.	Yes	81.6%	62.2%
Knowledge of the ability to prevent others from seeing the social networking profile.	Yes	75.9%	70.4%
Does the service provider share the participant’s information with other sites?	Yes	35.6%	34.7%
Receiving friend requests from anonymous users.	Yes	75.9%	67.3%
Accepting friend requests from anonymous uses.	Yes	75.9%	61.2%
Using real personal information in the account.	Yes	58.6%	69.4%
The desire to allow strangers to see the profile information.	No	75.9%	62.2%

Table 5.6: Comparison between Arabic and English language participants.

5.2.4 Rating the importance of personal information

The main purpose of the last part of the survey was to measure the importance of each element of a user's personal information and classify the elements according to their importance for both males and females. The survey showed that the percentage of concern about online privacy for all participants is about 66.5%; this means that a high percentage of users really cared about the privacy of personal information. The findings contributed to helping the researcher design the proposed research methodology. Furthermore, the level of privacy can be determined for each element by calculating the mean for each item. In general, according to Table 5.7, the maximum mean is 3.29 of 5, and the minimum mean is 2.24 of 5. There are some variables that need more privacy than others, such as physical addresses, favourite books and so on.

Descriptive Statistics

Item	N	Minimum	Maximum	Mean	Std. Deviation
Name	184	1	5	2.63	1.597
Gender	184	1	5	2.48	1.533
Email	184	1	5	3.15	1.432
Date of birth	184	1	5	2.83	1.494
Phone number	182	1	5	3.21	1.656
Physical address	182	1	5	3.21	1.633
Current address	182	1	5	3.29	1.586
School information	182	1	5	2.76	1.528
Hometown	182	1	5	2.52	1.448
Interests and activity	182	1	5	2.35	1.440
Favourite books	182	1	5	2.26	1.448
Favourite TV shows	182	1	5	2.24	1.420
Favourite music	182	1	5	2.42	1.513
Favourite movies	182	1	5	2.35	1.478
Relationship status	182	1	5	2.80	1.540
Pictures	182	1	5	3.07	1.556
Videos	182	1	5	3.02	1.573
Comments and posts	182	1	5	2.62	1.447
Tags	182	1	5	2.71	1.389
Friends list	182	1	5	3.09	1.485
Education and work	182	1	5	2.86	1.523
Religion	182	1	5	2.52	1.720
Website	181	1	5	2.78	1.533

Table 5.7: Analysis identifying the important elements in a user's personal information

The research suggestion is to classify these items into three groups based on the resultant mean. This can be done by calculating the difference between the maximum and the minimum values and then setting a range for these groups. For example, the maximum value in the previous table is 3.29, and the minimum value is 2.24; thus, the difference is 1.05. The difference can then be divided by three in order to classify the privacy of personal information into three levels: low, medium and high. As a result, the three levels of privacy were set at the following ranges:

- Low level: from 2.24 to 2.55
- Medium level: from 2.56 to 2.94
- High level: from 2.95 to 3.29

This research depends on the classification of both genders for determining the significance of each component of the personal information items. Moreover, the mean values for personal information variables have been measured. Indeed, the results show that males' answers for each element of personal information, as shown in Figure 5.3, range from 2.20 to 3.15 out of 5. Some items have more sensitivity than others; for example, email is more sensitive than favourite TV shows. On the contrary, mean values of female answers range from 2.39 to 4.04 out of 5, as shown in Figure 5.4. Some variables have higher sensitivity to privacy than the male results; but, in general, females desire more privacy for personal information than do males.

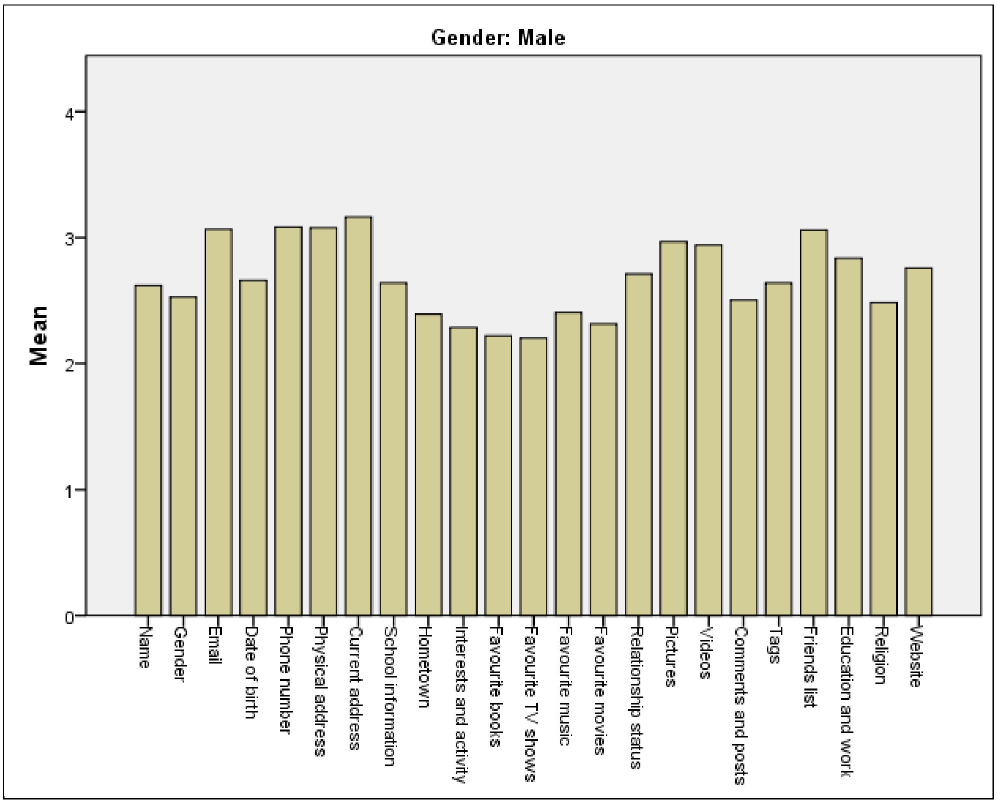


Figure 5.3: Mean values of the elements of personal information for males

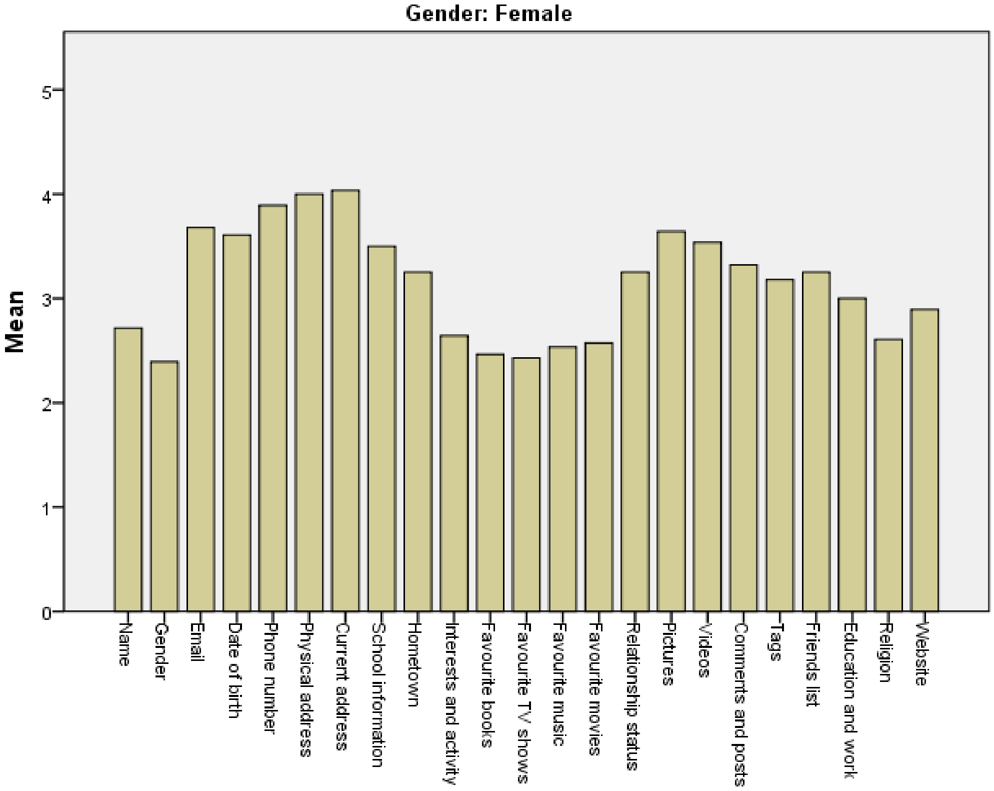


Figure 5.4: Mean values of the elements of personal information for females

In addition, when comparing the male and female results (Table 5.8), there are differences between the elements. Some items for females have higher concerns for privacy than for males; for example, date of birth for males rates 2.69 of 5, but for females the rating is 3.61 of 5. This suggests that date of birth is more sensitive for females than for males. It can be classified as a high-privacy item for females and a medium-privacy item for males. In addition, the findings show that females are more interested in the privacy of personal information. As a result, the issue of privacy should be framed in the research design in a way to accurately reflect the gender differences.

Thus, when using the previous equation to divide the current results for males and females to get the classifications for the privacy of personal information, both males and females will have separate classifications to distribute the privacy items for high, medium or low sensitivity for the user.

Item	Mean	
	Male	Female
Name	2.62	2.71
Gender	2.5	2.39
Email	3.05	3.68
Date of birth	2.69	3.61
Phone number	3.09	3.89
Physical address	3.07	4
Current address	3.15	4.04
School information	2.63	3.5
Hometown	2.39	3.25
Interests and activity	2.29	2.64
Favourite books	2.23	2.46
Favourite TV shows	2.2	2.43
Favourite music	2.4	2.54
Favourite movies	2.31	2.57
Relationship status	2.71	3.25
Pictures	2.97	3.64
Videos	2.93	3.54
Comments and posts	2.49	3.32
Tags	2.63	3.18
Friends list	3.06	3.25
Education and work	2.84	3
Religion	2.5	2.61
Website	2.76	2.89

Table 5.8: Comparison between males and females for each element of personal information

Hence, personal information items can be classified as low, medium or high level using the previously defined classification strategy. Because of the desire to work in separate classifications for both genders, some values which are less than 2.24 and more than 3.29 will be distributed for low and high levels; so, Table 5.9 shows the classifications for all items for both males and females.

Item	Mean	
	Male	Female
Name	Medium	Medium
Gender	Low	Low
Email	High	High
Date of birth	Medium	High
Phone number	High	High
Physical address	High	High
Current address	High	High
School information	Medium	High
Hometown	Low	High
Interests and activity	Low	Medium
Favourite books	Low	Low
Favourite TV shows	Low	Low
Favourite music	Low	Low
Favourite movies	Low	Low
Relationship status	Medium	High
Pictures	High	High
Videos	Medium	High
Comments and posts	Low	High
Tags	Medium	High
Friends list	High	High
Education and work	Medium	High
Religion	Low	Medium
Website	Medium	Medium

Table 5.9: Distribution of privacy levels for both genders

In conclusion, the main purpose of the survey is to measure the suitability of using mobile phones to select or control privacy options and to determine the percentage of users who use mobile phones to browse the Internet and other web services. The second purpose is to define which items of personal information demand more privacy than others.

The survey results show that mobile phones and privacy are two fields that need more research to find ways to satisfy the needs of users. Mobile phones are used to browse the Internet and most respondents use their mobile phone for other web services. The method of selecting variables through mobile phones should be developed to be more suitable for different mobile screens and to save the user time. In addition, personal information items have been studied in this survey, and the more important items have been classified into three groups; low, medium and high level. The results show that females desire a higher level of privacy than males for certain personal information items. Therefore, the next research step will be to develop a framework that achieves high levels of privacy and convenience for devices such as mobile phones and computers to control privacy settings.

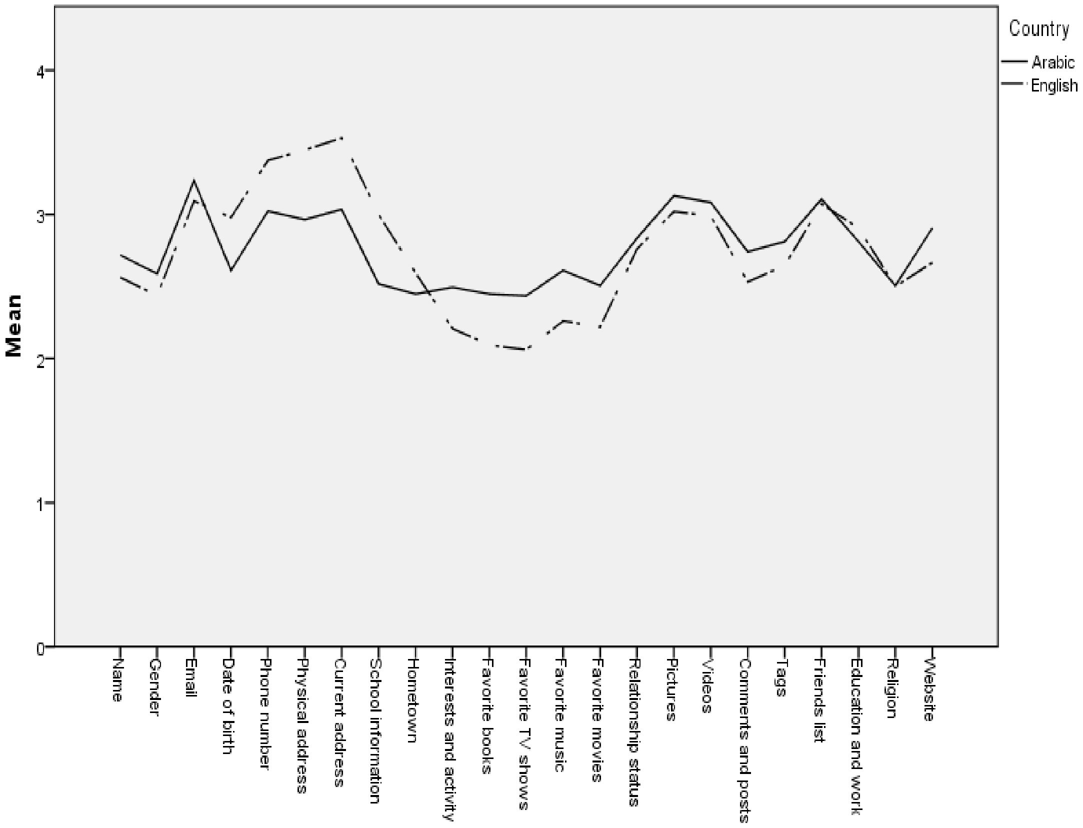


Figure 5.5: A comparison between Arabic and English cultures.

However, the comparison between the two samples collected by using Arabic and English languages presented some important results. These results showed the range of concerns about privacy of personal information for participants and the use of mobile and social networking sites. As shown in Figure 5.5, the chart lines for both of them were broadly similar, but concerns about sharing some personal information items with others differ between cultures. In detail, the average number of participants hiding email addresses who used the Arabic form was higher than for participants who used the English form. It was about 3.25 of 5 for the Arabic form while it was about 3.0 of 5 for the English form. In contrast, date of birth is very important for users who participated in the English form rather than the Arabic form. It got about 3 of 5, an importance that might relate to the use of date of birth in daily life as a security question to protect payment or credential processes. Address details were also more important for participants of the English form (about 3.5 of 5 versus

2.8). Hiding photos and videos were nearly similar in percentage between the two cultures, and hiding the religion as well. As a result, the convergent similarity between the two cultures showed that applying one privacy policy on users' profiles could be a weakness for privacy systems, especially if the users are from different cultures. In this study, it is important for the design to takes into account the differences and provide several options for users.

5.2.5 Comparing the findings with other research

The purpose of this section is to compare the findings of the present survey with those of other studies, and to define the differences between them. As mentioned in the literature review, several studies have discussed the issue of privacy, and have set different levels for evaluating the sensitivity of material, the extent to which personal information details are revealed, and the amount of trust placed in the service provider. Therefore, this section will compare the findings of this study with the results of the studies done by Gross and Acquisti (2005), Madden (2012), Christofides, Desmarais and Muise's (2010), and Acquisti and Gross (2006).

The standards on which this comparison is based considered several aspects, such as a comparison of the results of previous research with those of the current research from the perspective of items of personal information provided through social network accounts; a comparison of the percentage of trust different users have towards the service providers; and finally an examination of growth in the use of online social networking sites.

- ***Types of information disclosed***

In 2005, Gross and Acquisti conducted a study to evaluate the percentage of users who disclose personal information on their Facebook accounts. The sample was recruited from the Carnegie Mellon University, and the majority of respondents were undergraduate students in the 18-24 years age bracket. Thirteen elements were used in the measurement of the disclosure of personal information. These same thirteen elements have been utilised in the current research. A comparison between the findings of the 2005 study and the current study can assist in highlighting the changes among users over this period in the way they manage the privacy policies that control their personal information details. As seen from table 5.10, a big change happened between 2005 and 2013 in terms of the disclosure of personal information. Various items are now regarded as more sensitive by users than before.

Gross and Acquisti's (2005) study showed that 90.8% of participants made their images available to others, while in the present study the results show that only 44.39% of participants showed their images in their profiles. The 2005 study also showed that the percentage of those disclosing both their name and date of birth had decreased from 78% and 87.7% to 58.54% and 63.9%, respectively.

Item	Year	
	2005	2013
Name	78.00%	58.54%
Date of birth	87.80%	63.90%
Phone number	39.90%	27.32%
Current address	50.80%	39.51%
School information	87.00%	75.60%
Hometown	73.00%	77.07%
Interest and activity	65.00%	84.39%
Favourite book	61.00%	85.37%
Favourite TV show	62.90%	86.34%
Favourite music	67.00%	86.83%
Favourite movie	67.00%	84.39%
Relationship status	68.00%	66.83%
Pictures	90.80%	44.39%

Table 5.10: Percentages of disclosure of personal information items in years 2005 and 2013.

Similarly, 50.80% of participants listed their current residential addresses on their profiles in 2005, but in 2013 this percentage had dropped to 39.51%. This shows that people’s greater awareness of privacy risks has encouraged them to hide some items from others.

While there were several items that participants in 2013 preferred to have hidden, as compared with the previous study, there were other items that were not affected by the changes over these years. For example, disclosing interests and favourite things had increased by about 20% in 2013. This can be interpreted to indicate that this type of information does not contain personal information identification details. Therefore, the disclosing of personal information details via the internet has changed, and this is related to the sensitivity of the item. Some items are seen as more sensitive than others, and the majority of users prefer to hide them. So, when designing any privacy tool, designers should take into account that each item of personal information will have a different sensitivity level, and this can also differ between males and females.

In 2006, Acquisti and Gross (2006) evaluated the disclosure of certain personal information items in another study. A comparison of findings across the three studies will assist in revealing the extent to which privacy has changed across time. Figure 5.6 presents a comparison of three different items (birthday, phone number and current address) in the different years (2005, 2006 and 2013)

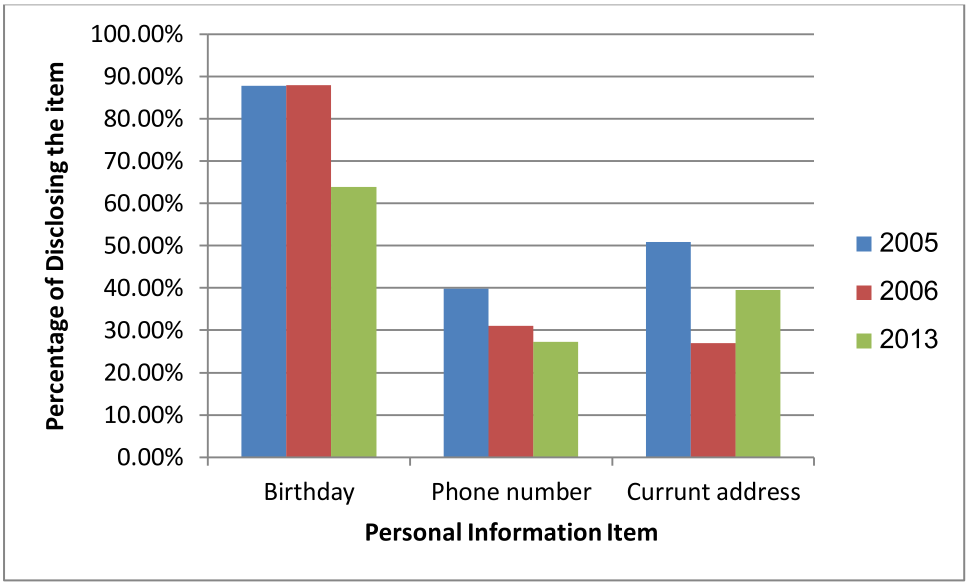


Figure 5.6: A comparison, showing the disclosure of information in three different years

From the previous figure, it can be seen that sensitivity over distributing information about birthdays, phone numbers and addresses has increased, presumably with the increased awareness of users regarding privacy risks. The decline in the percentage of those providing information about their birthday and phone numbers between 2005 and 2013, could be related to the frequent use of this information in certain financial transactions.

- ***The use of social networking accounts***

This point will compare the results of the current study with other studies relating to different aspects of the use of social networking sites and the related privacy issues. These aspects will be analysed as follows:

Age group: In most of the studies in this area, the age distribution of online social network users has indicated that they are favoured by young people. Gross and Acquisti's (2005) study showed that about 73% of the participants who had social network accounts were undergraduate students. Another study by the same authors in 2006 showed that about 79% of participants were undergraduate students (Acquisti & Gross, 2006). Madden's (2012) study about privacy management on social sites showed that 57% of social users were between the ages of 18 and 29 years old. The current study found that 76.2% of users were between 18 and 25 years old. Another study done by Hu (2011) showed that the highest percentages of participants using online social networks were between 18 and 34 years old. This study showed that 42% of users have Facebook accounts, 44% have Myspace accounts and 56% of them have QQ accounts. Hence, when designing any privacy tool, the target group of users should be taken into account. These results showed that most users of online social network accounts are young adults, and the current study showed that about 92% of users use their web mobile devices to browse the internet.

Usage of social network accounts: In Madden's study (2012) it was shown that roughly 42% of participants had more than one account, and in the present study, when this question was examined, the results were similar. Approximately 45% of the participants had more than one account. Taken together, these two pieces of evidence indicate that, with the rapid increase in social networking sites, about 43% of current users have more than one account. So, bearing in mind that a high percentage of users have more than one social network account, the developers of applications for these sites should take this factor into account, especially when they design privacy tools to minimise the distribution of information.

Frequency of login to the profile per day: Madden's study (2012) indicated that about 47% of participants visited their profiles at least once a day. However, this study found that about 78% of participants visit it daily with approximately 50% of them visiting it more than once, and up to five times per day. Therefore, the difference between these percentages shows that the use of social networks has become an essential task for internet users, and is seen as a daily task.

Privacy issues: In Christofides, Desmarais and Muise's study (2010) about 40% of the users added people that they didn't know personally, and about 35% accepted their invitations. The purpose of this was to increase their number of friends. However, in the current study, only 26.5% of participants accepted invitations from anonymous people. In Christofides, Desmarais and Muise's study (2010) the participants were asked whether they change the privacy settings on their accounts. Approximately 63% of the participants said they regularly changed their default settings, but in the current study 59.5% of them changed them, with about 40% of them changing them regularly (Figure 5.7).

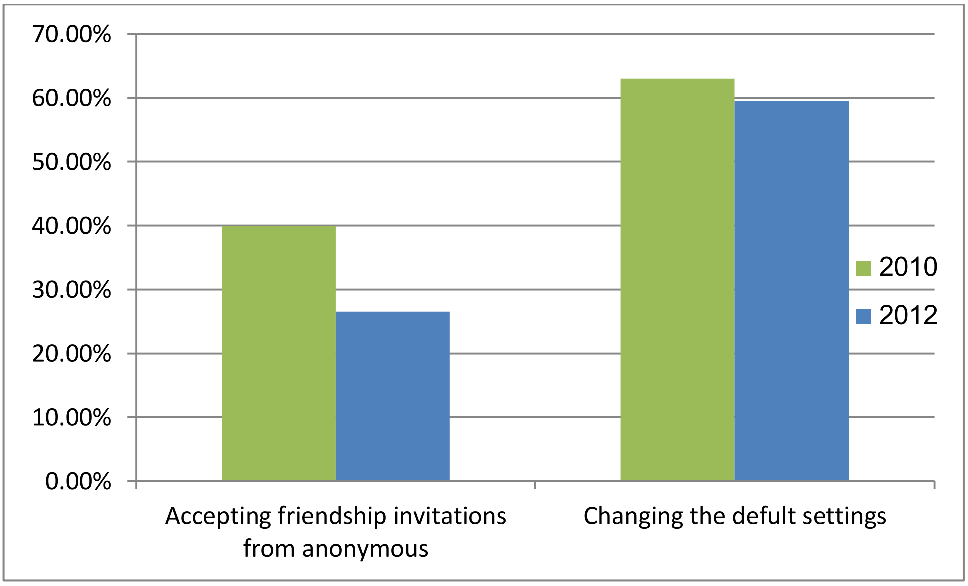


Figure 5.7: A comparison between the years 2010 and 2012

Moreover, in the Christofides, Desmarais and Muise's study, about 38% of participants did not know how to limit the access to their information for other users, but in this study only about 7.5% of participants were not familiar with the process for specifying the access for other users. Control of privacy settings was also measured in Madden's study (2012) and the results compared with the current study. Madden's study showed that 48% of participants encountered difficulties in managing the privacy controls, but in this study only 18.4% of them were not satisfied with the way they managed their privacy controls.

- ***Mobile web devices and the control of privacy settings***

This point describes the differences between the current study and earlier studies in measuring different concepts to do with the control of privacy settings in mobile web devices. In order to gauge the success of the suggested framework, the researcher studied much of the previous research related to this area. All of this work was designed to measure different aspects of privacy, but none measured the suitability of using mobile web devices to manage the privacy settings of users' online social network accounts. For example, Gross and Acquisti (2005) studied the sharing of relevant common information with strangers, and the privacy implications for online social networks. In 2006, the same authors did another study to examine the behaviour of online social network users and their awareness of privacy concerns (Acquisti & Gross, 2006). In addition, Madden (2012) investigated the concept of privacy management on social media, and studied different aspects related to this area. However, the current study was different from these other studies in that it measured the suitability of using internet mobile devices to manage privacy settings, and evaluated the commonly used information that users included in their profiles, based on privacy sensitivity.

5.3 The Smart Wizard System

5.3.1 Implementation results

This section discusses the results of implementing the Smart Wizard System and calculating its accuracy percentage**.** This was based on calculating the number of items where the visibility status of personal information items for each participant was changed.

Indeed, there are several reasons distinguishing this task from others; it is an implementation for a Smart Wizard System, and the research for this study found no similar wizard system that was available to set personal information privacy settings (chapter two). Also, it can be used to support internet mobile devices because of the simplicity of design and the selection process. As mentioned in the previous chapter, this system was based on a previous survey done by the same researcher.

- **Data quality and characteristics of respondents**

This section presents a statistical analysis of the results of implementing the Smart Wizard System, which was available in two languages (English and Arabic), to simplify the process of understanding the questions. All invitations to participate were sent via email and posted on selected social networking sites that were interested in information technology. All invitations contained information about the purpose of the Smart Wizard System, and a description of what was required from the participants. These details encouraged the participants to be careful with the selection process. In this part there were no uncompleted cases, because the system was designed to save all selections whenever the participant clicked on the 'Save' button to confirm their choice.

A total of 439 respondents implemented the wizard and completed the participation process (352 males and 87 females). Both languages were used (86 volunteers used English and 353 used Arabic).

- **The accuracy of the wizard**

The main purpose of calculating the accuracy of the Smart Wizard System was to determine the effectiveness of the system by measuring how the recommended settings suited the participants. So, in this research, the author decided to calculate the effectiveness of the system by measuring the accuracy for each participant. The formula that was used to calculate this accuracy percentage is based on the number of items that had been changed by the user. The system automatically counted the number of items where the visibility statuses were changed. Applying this criterion, the findings were as follows:

- Mean accuracy for both genders: 98.4%
- Mean accuracy for males: 98.13%
- Mean accuracy for females: 99.05%

- **Personal privacy**

Another purpose for implementing the Smart Wizard System is to define which personal information items have more sensitivity than others. Thus, this section will discuss the sensitivity of personal information items based on the selections of participants, whether they accepted an item's status or modified it to be hidden.

As can be seen from Table 5.11, there are some personal information items that had more sensitivity for participants, who considered them very private and wished them to be hidden in the implementation (for example, photographs, personal videos and addresses).

Item	The percentage of people who want to show the item		
	Total	Male	Female
Name	78.80%	95.50%	11.50%
Gender	92.90%	98.60%	70.90%
Email	4.10%	4.50%	2.30%
Date of birth	77.90%	95.70%	5.70%
Phone number	2.30%	2.60%	1.10%
Physical address	3.20%	3.70%	1.10%
Current address	3.20%	3.70%	1.10%
School information	81.80%	96.30%	23%
Hometown	90.90%	97.40%	64.30%
Interest and activity	92.70%	99.40%	65.50%
Favourite book	93.60%	99.40%	70.10%
Favourite TV show	93.60%	99.40%	70.10%
Favourite music	93.60%	99.40%	70.10%
Favourite movie	93.60%	99.40%	70.10%
Relationship status	77.40%	95.20%	5.70%
Pictures	0%	0%	0%
Videos	0%	0%	0%
Comment and posts	99.10%	100%	95.40%
Tags	0.70%	0%	3.45%
Friends' list	2.50%	2.80%	1.10%
Education and work	76.80%	94.60%	4.60%
Religion	92.70%	99.40%	65.50%
Website	82.70%	95.60%	26.40%

Table 5.11: The relative importance of privacy

The previous table presented some important relationships between personal information items; some items have high sensitivity for participants and vice versa. For example, videos, pictures and tags have a high priority for participants to hide , and that they not be shown or shared with others. In contrast, there are some items that participants have no objection to show and share with others, such as favourite books, TV shows and music. Therefore, this section will provide more detail about the different relationships between personal information items and compare the results for both genders.

The first part will study the relations between personal information privacy items for males, the second part will study the relations for females. According to Table 5.11, 15 out of 23 personal information items show a high percentage for sharing with others, and these have a low sensitivity to misusing these details. On the other hand, the other 8 personal information items which have specific personal information details, such as email, phone number and physical address show a low percentage for sharing with others. In addition, pictures, videos and tags have the lowest percentage in the survey because these items have picture identification that could be misused by others.

Based on the results shown in Table 5.11, females have more sensitive personal information items than males. The general percentage for sharing these items with others was lower than for males and the number of items that have a high percentage to be shared with others was less. Moreover, 11 items showed a high percentage (about 90% or more) of items to be suppressed from others, such as email, phone number and address. Also, three items were in contradiction with the male findings (which showed a high rather than a low percentage for sharing); these were name, relationship status, and education and work. In contrast, 8 items have percentages ranging from 60% to 71% for sharing with others and these percentages were lower than for the males. The only item showing approximately 95% to be shared with others was comments and posts. This may be due to the freedom of expression to write comments and share them with others. In conclusion, females have more interest in the privacy of personal information than males especially with identification items.

5.3.2 Concerns about hidden personal information items

The second part of this task was to study user concerns about misuse and hidden items. This survey was based on evaluating 23 items of personal information. The participant was asked to give their opinion about what items they felt might be misused by others, and to indicate if they had hidden these items in their profile or not.

This survey can be distinguished from other surveys by identifying two aspects of privacy: concerns and the procedures to address them. Statistical analysis will be used to classify the findings and to make comparisons between the genders.

This part was also available in two languages (English and Arabic) and the characteristics of participants were the same as for the first part of this task. A total of 205 respondents completed this area of the survey (131 males and 74 females).

- **The results of measuring the level of concern about misusing personal information items**

The findings of this part reveal a close relationship between user concern about misuse and the items hidden in his/her own current social network accounts. As shown in Table 5.12, about 61% of all respondents were concerned about misuse of their email addresses and about 51% of all participants hid their email addresses. Moreover, users' favourite items, such as movies or music, exhibited a low percentage of concern and hiding from others because they did not contain any personal identification and contact details.

Item	**Both genders**		**Male**		**Female**	
	Concerned	Hide	Concerned	Hide	Concerned	Hide
Name	51.22%	41.46%	44.27%	35.88%	63.51%	51.35%
Gender	20.49%	19.02%	16.8%	14.5%	27.02%	27.02%
Email	61.46%	52.2%	49.62%	45.8%	82.43%	63.51%
Date of birth	37.07%	36.1%	27.48%	29.01%	54.05%	48.65%
Phone number	74.63%	72.68%	65.65%	65.65%	90.54%	85.14%
Physical address	63.41%	62.44%	54.2%	54.96%	79.73%	75.66%
Current address	63.9%	60.49%	56.49%	55.73%	77.03%	68.92%
School information	22.44%	24.4%	17.5%	22.14%	31.08%	28.38%
Hometown	24.4%	22.93%	19.85%	19.08%	32.43%	29.73%
Interest and activity	17.7%	15.61%	12.98%	10.69%	24.32%	24.32%
Favourite book	14.14%	14.63%	9.92%	10.69%	21.62%	21.62%
Favourite TV show	12.68%	13.66%	9.16%	9.92%	18.92%	20.27%
Favourite music	14.15%	13.17%	10.69%	9.92%	20.27%	18.92%
Favourite movie	15.12%	15.61%	12.21%	12.21%	20.27%	21.62%
Relationship status	32.68%	33.17%	25.95%	27.48%	44.59%	43.24%
Pictures	61.95%	55.61%	52.67%	52.67%	78.38%	60.81%
Videos	62.93%	56.59%	54.96%	53.44%	77.03%	62.16%
Comment and posts	32.2%	28.78%	23.66%	22.9%	47.3%	39.19%
Tags	33.66%	31.22%	29.24%	29.01%	43.24%	35.14%
Friends' list	53.66%	44.88%	45.8%	41.22%	67.57%	51.35%
Education and work	26.34%	25.37%	19.08%	19.85%	39.19%	35.14%
Religion	20%	19.51%	16.03%	16.03%	27.03%	25.68%

Website	40.49%	35.61%	32.82%	32.06%	54.05%	41.89%

Table 5.12: Personal information items that concerned both genders and that were hidden

To analyse the attitudes of both genders for hiding items, Figure 5.8 presents the percentages for hiding each personal information item. The obvious conclusion from the graph is that all variables are largely homogeneous between hiding items and anxiety of misuse. Most users who are concerned about privacy and misuse of personal information hide information such as phone number, address and personal photographs. On the other hand, more general items, such as favourite music and movies, are not regarded as sensitive.

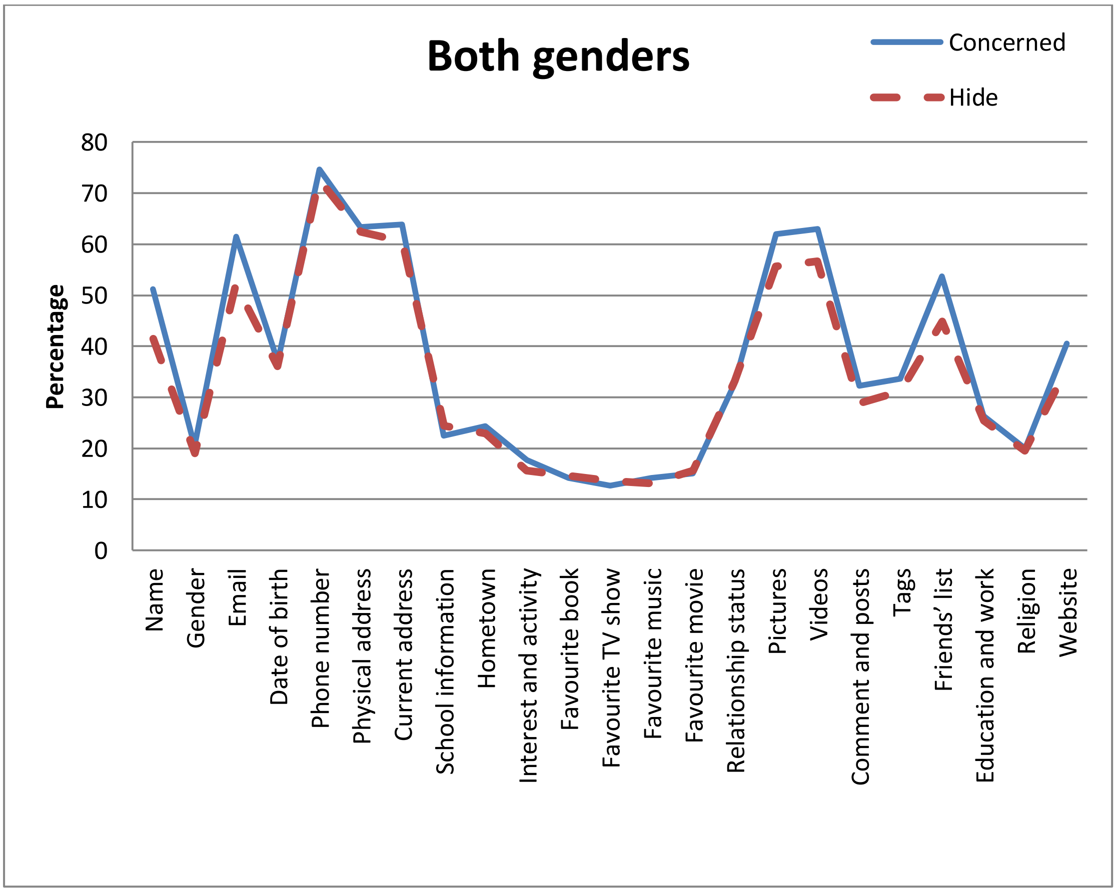


Figure 5.8: Combined male and female views of personal information that should or must be hidden

To identify the behavioural differences between genders to hide items, Figure 5.9 presents the findings of males and shows that user concern was reflected in the hiding of items. Items that have greater sensitivity and that can identify the respondent are more sensitive, and most respondents hid them. Males were sensitive to personal photographs and videos, phone numbers and address details. However, general topics that do not affect the identity of the user were not restricted (for example, favourite music and movies).

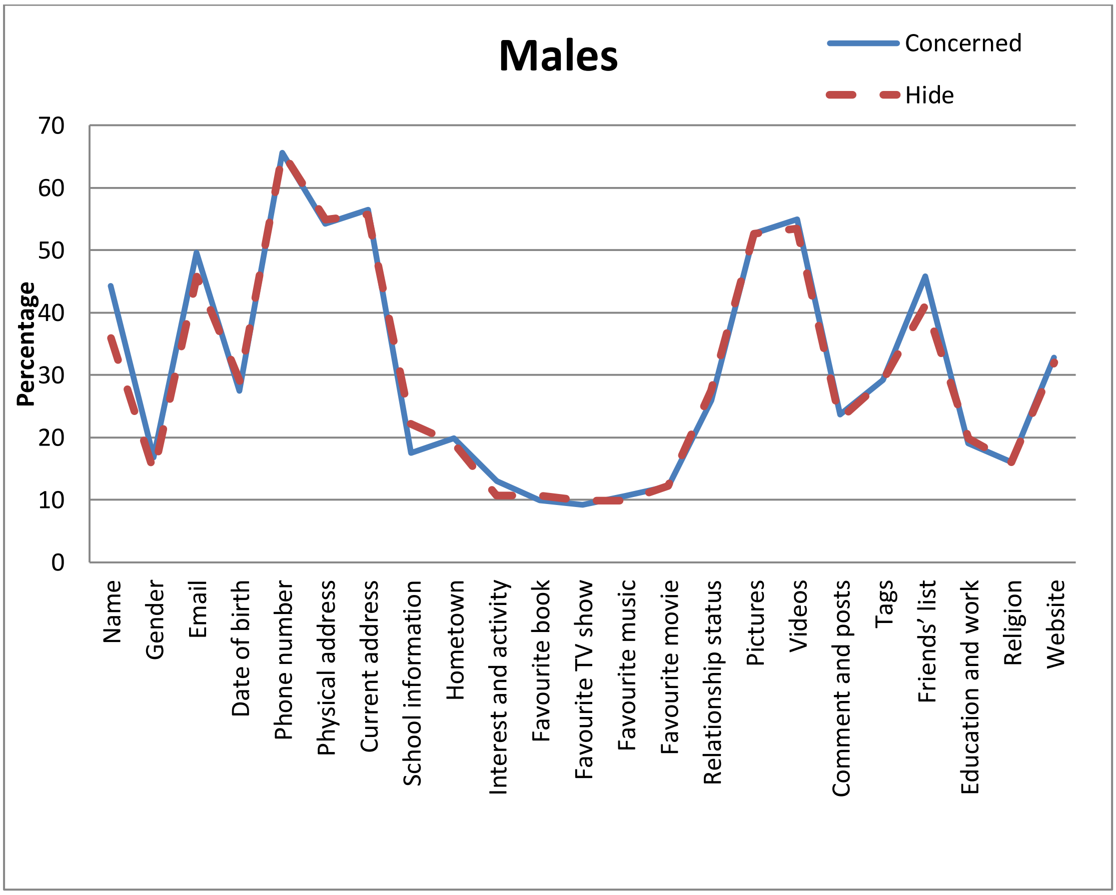


Figure 5.9: Male views of personal information that should or must be hidden

Figure 5.10 shows the findings for females, and there were some obvious differences in comparison with Figure 5.9. Females were more concerned and careful about sharing personal information items than males. For example, as can be seen from Figure 5.9, only about 65% of males hid their mobile phone numbers, but Figure 5.10 shows that about 90% of female respondents hid them. This is evidence of the sensitivity of this item for females. When classifying items by level of importance, it is clear that some items have a medium level of importance for males but a high level for females. For example, name has a medium sensitivity for males (about 50%) but for females this is higher (about 63%). However, although such differences are evident, the majority of both genders agree that some items should be hidden.

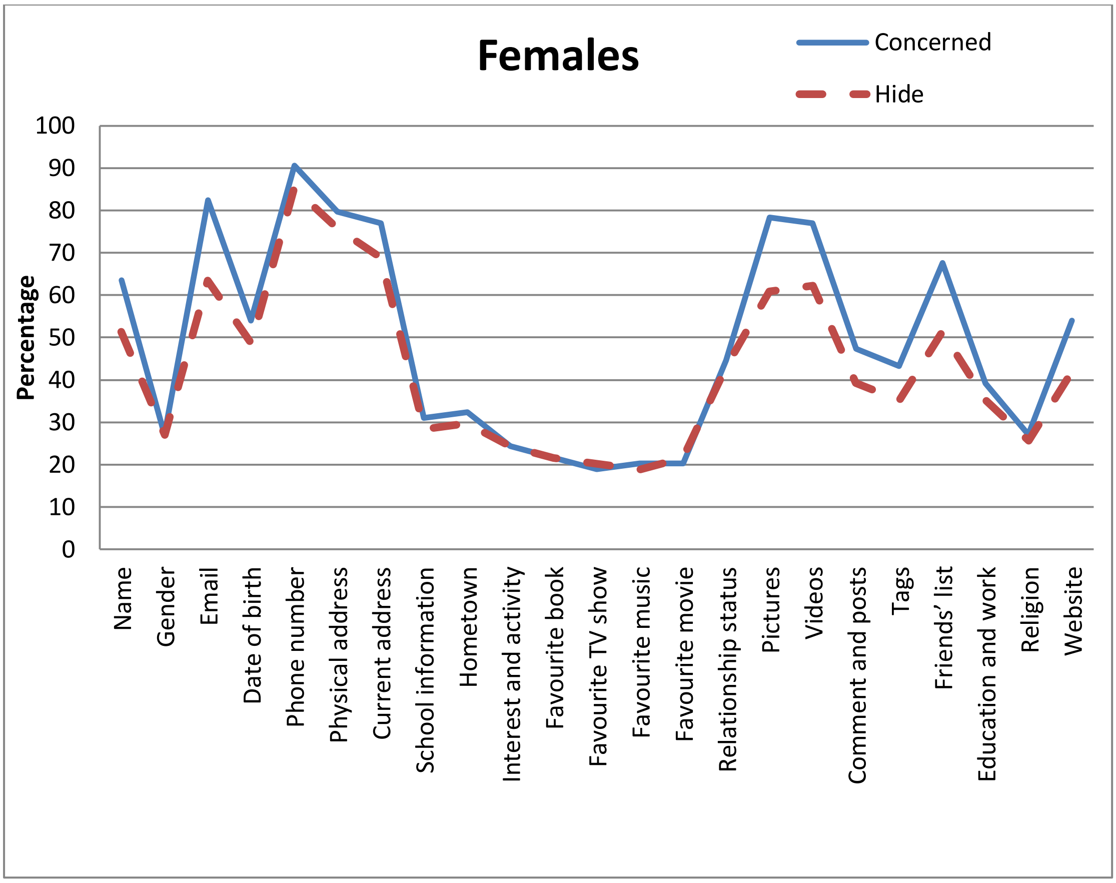


Figure 5.10: Female views of personal information that should or must be hidden

5.4 The Proposed Privacy System

This section provides a report on the implementation of the applied system. It consists of several steps and each step will be described in the following headings:

- The first heading will describe the creation of several accounts in Server 1 (privacy system) and will present all the created privacy policies for each user.
- The second heading will present the process of creating new users in Server 2, 3 and 4 and defining the authorisation access to Server 1.
- The last heading will show the results of implementing a privacy policy on each site for all users.

5.4.1 Implementation results of creating privacy policies in Server 1 (privacy system)

There were several steps to check the efficiency of the system. The author created four different users in the Server 1 database and established three different privacy policies for each user. The process of creating users and privacy policies was successful and all details are shown in Table 5.13.

User	Gender	Password	The security levels of each privacy policy		
			High level	Medium level	Low level
Alice	Female	123	Default settings	Custom settings	Custom settings
Bob	Male	abc	Default settings	Custom settings	Default settings
John	Male	456	Custom settings	Default settings	Custom settings
Sam	Female	def	Custom settings	Default settings	Custom settings

Table 5.13: Create accounts in Server 1

Each user had three different levels of privacy policies (high, medium and low). The purpose for creating these policies was to test the Smart Wizard System and to set different access policies for each site. Table 5.14 shows the results of creating these policies and the impact on each personal information item.

Personal information item	Alice			Bob			John			Sam		
	HL	ML	LL	HL	ML	LL	HL	ML	LL	HL	ML	LL
Name	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓
Gender	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Email	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
Date of birth	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓
Phone number	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
Physical address	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
Current address	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
School information	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✓
Hometown	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓
Interest and activity	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓
Favourite books	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Favourite TV shows	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Favourite music	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Favourite movies	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Relationship status	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓
Pictures	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓
Videos	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✓
Comments and post	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗	✓
Tags	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✓
Friends list	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
Education and work	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
Religion	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓
Website	✗	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✓

(✗ means that the item is not allowed for sharing, ✓ means that it is allowed for sharing)

Table 5.14: The created privacy policies

Diversity in the creation of multiple privacy policies offers a chance to apply different access policies to read values from the Server 1 database. In the next section, the researcher presents the results of creating four different accounts for the previous users.

5.4.2 Implementation results of applying privacy policies in Servers 2, 3 and 4

In this step, the researcher created four different accounts in each server and set a privacy policy for each user to be applied on this site. Table 5.15 shows the login details for all created accounts in each server and the applied privacy policies.

User	Password	The applied privacy policy on all servers		
		Server 2	Server 3	Server 4
Alice1	123	Low level	Medium level	High level
Bob1	abc	High level	Low level	Medium level
John1	456	Low level	High level	Medium level
Sam1	def	Medium level	Low level	High level

Table 5.15: Login details and the applied privacy policies for each server

As seen from the previous table, all users have been subscribed in servers 2, 3 and 4, and different privacy policies have been set for each site. All personal information items have been reviewed for each user and compared with the results in Table 5.13. The findings show that all the hidden items were not shared with these servers as shown in Appendix J.

Repeating the previous processes of setting different privacy policies on servers allowed users to control the process of distributing their personal information details. Table 5.16 shows all the applied privacy policies based on the values in Table 5.15. The implemented system gave each user the authority to limit access to their personal information details from Server 1.

In this implementation, the researcher set different privacy policies for each server. To verify the success of the system on Servers 2 and 3, a comparison was made between the findings and the values in Table 5.14. Comparison results were compatible and in line with the initial system. Table 5.17 presents the results of applying the defined privacy policies on these servers, the similarity for both Table 5.14 and Table 5.15 can be seen.

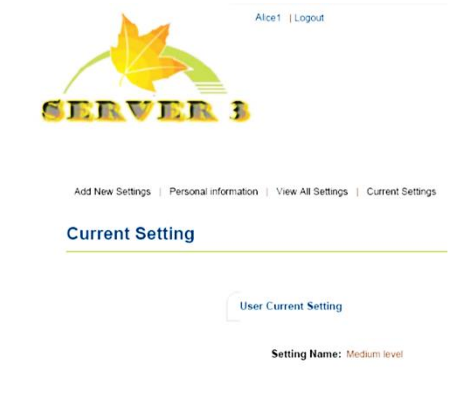
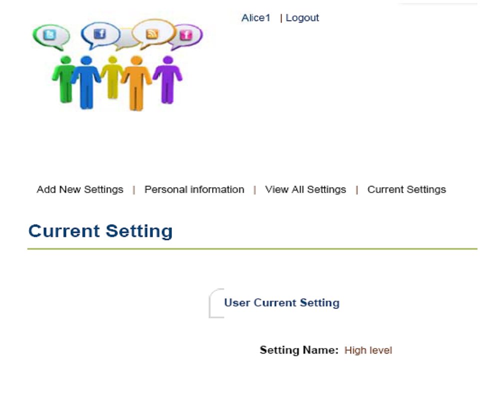
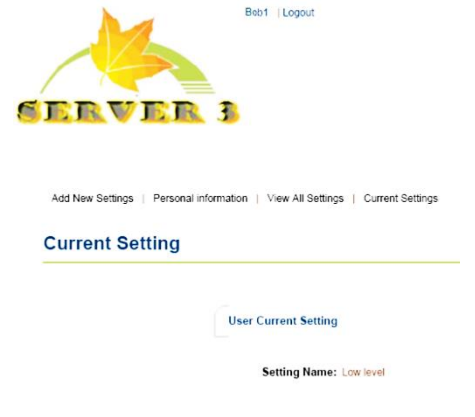
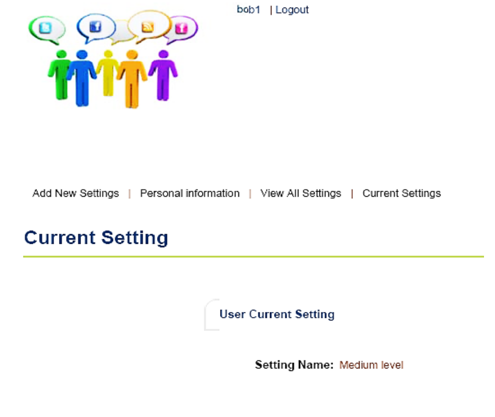
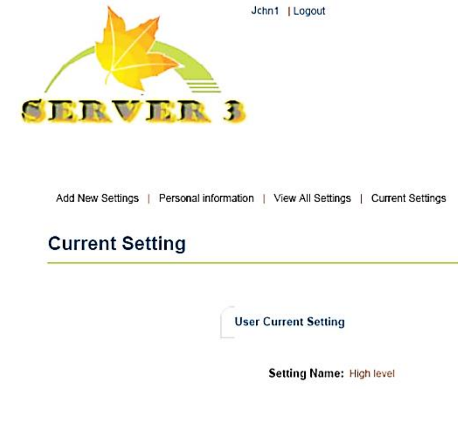
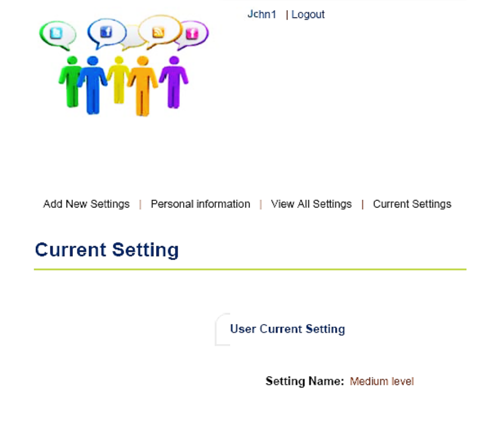
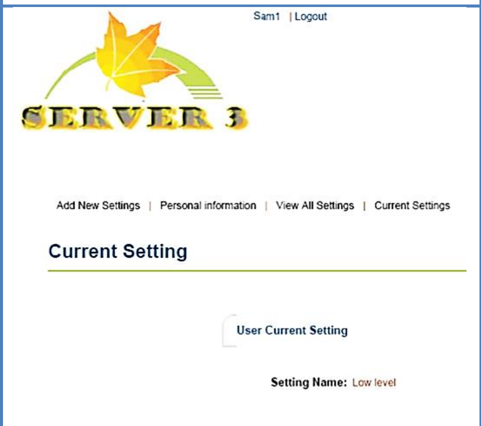
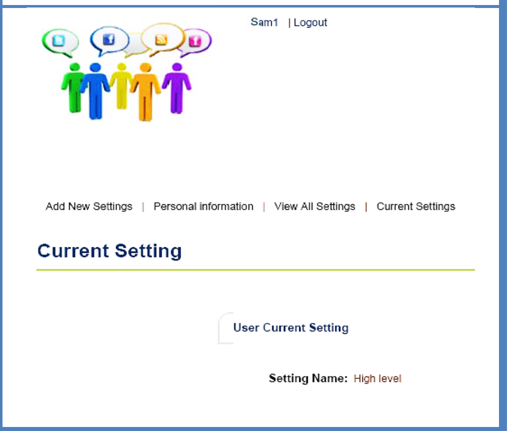
<table>
<tr><th></th><th>Server 3</th><th>Server 4</th></tr>
<tr><td>Alice</td><td> Alice1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: Medium level</td><td>Alice1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: High level</td></tr>
<tr><td>Bob</td><td> Bob1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: Low level</td><td>bob1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: Medium level</td></tr>
<tr><td>John</td><td> Jchn1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: High level</td><td>Jchn1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: Medium level</td></tr>
<tr><td>Sam</td><td> Sam1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: Low level</td><td>Sam1 | Logout
Add New Settings | Personal information | View All Settings | Current Settings
Current Setting
User Current Setting
Setting Name: High level</td></tr>
</table>

Table 5.16: The current applied privacy policy on each server for all users

Personal information item	Server 3				Server 4			
	Alice	Bob	John	Sam	Alice	Bob	John	Sam
Name	✗	✗	✗	✓	✗	✗	✗	✓
Gender	✓	✓	✗	✓	✓	✓	✓	✓
Email	✗	✗	✗	✓	✗	✗	✗	✗
Date of birth	✓	✓	✗	✓	✗	✗	✗	✗
Phone number	✓	✗	✗	✓	✗	✗	✗	✗
Physical address	✗	✗	✗	✗	✗	✗	✗	✗
Current address	✗	✗	✗	✗	✗	✗	✗	✗
School information	✓	✓	✗	✓	✗	✓	✓	✗
Hometown	✓	✓	✗	✓	✗	✓	✓	✗
Interest and activity	✓	✓	✗	✓	✗	✓	✓	✗
Favourite books	✓	✓	✗	✓	✓	✓	✓	✓
Favourite TV shows	✓	✓	✗	✓	✓	✓	✓	✓
Favourite music	✓	✓	✗	✓	✓	✓	✓	✓
Favourite movies	✓	✓	✗	✓	✓	✓	✓	✓
Relationship status	✓	✓	✗	✓	✗	✗	✗	✗
Pictures	✗	✗	✗	✓	✗	✓	✗	✗
Videos	✗	✗	✗	✓	✗	✓	✗	✓
Comments and post	✗	✓	✗	✓	✗	✓	✓	✓
Tags	✓	✓	✗	✓	✗	✓	✓	✗
Friends list	✓	✗	✗	✓	✗	✗	✗	✗
Education and work	✓	✗	✗	✓	✗	✗	✗	✗
Religion	✓	✓	✗	✓	✗	✓	✓	✗
Website	✓	✓	✗	✓	✗	✓	✓	✗

(✗ means that the item is not allowed for sharing, ✓ means that it is allowed to share it)

Table 5.17: The applied privacy policies on server 3 and 4.

5.5 Comparing the Whole Framework with Other Models

This section discusses the results from applying the proposed framework privacy system to other social network systems. The comparison will indicate several points of difference when applying those systems, all related to the privacy of personal information details.

- ***Default privacy settings for males in Facebook and in the proposed model***

Having different social networking profiles creates additional tasks for users in managing their privacy settings. Most of these sites offer a default privacy setting for new users. To investigate this point, the researcher compared the results from applying the proposed model of this study with the default privacy settings in the Facebook application.

This subheading compared the default privacy settings for Facebook site (it has been checked in 12/8/2014) with the three different levels for the proposed framework in this study. As mentioned in the previous chapter, the proposed system will provide the user with three levels of privacy of low, medium and high, while Facebook provides him with only one default setting. In the proposed framework in this study, the low level of privacy protects users' information by reaching the lower level of protection of accessing this information. The medium level of privacy provides more security in accessing this information compared with the low level. The default high privacy level provides the recommended privacy policy for people who need more security in accessing their personal information.

Item	**Facebook**	**The proposed system**		
		Low	Medium	High
Name	1	0	0	0
Gender	1	1	1	1
Email	0	0	0	0
Date of birth	0	1	0	0
Phone number	0	0	0	0
Physical address	None	0	0	0
Current address	1	0	0	0
School information	1	1	1	0
Hometown	1	1	1	1
Interests and activity	1	1	1	1
Favourite books	1	1	1	1
Favourite TV shows	1	1	1	1
Favourite music	1	1	1	1
Favourite movies	1	1	1	1
Relationship status	1	1	0	0
Pictures	1	0	0	0
Videos	Condition*	0	0	0
Comments and posts	Condition*	1	1	1
Tags	1	1	1	0
Friends list	1	0	0	0
Education and work	1	0	0	0
Religion	0	1	1	1
Website	1	1	1	0

* This item needs an action from the user to hide or show it.

("0" means that the item is hidden, "1" means that it is apparent)

Table 5.17: Default privacy settings for males.

As can be seen from Table 5.17, twenty personal information items are shared on Facebook sites. These items include identification information that may guide others to identify the user, such as photos, name or address. In this comparison, the name Bob, as an example of the male gender, was used to create accounts in both Facebook and the proposed system that used the default system privacy settings. In the proposed system, there are three different default levels of privacy (low, medium and high), whereas Facebook has only one status level. In the default privacy settings for a Facebook account, some personal information is visible to others. This information may include some important information enabling others to identify the user, and potentially cause harm or misuse, such as name, current address and photo (Facebook

2014). In the proposed system, all three privacy levels would give the user greater confidence by hiding most of the information that could be used to identify him, with the percentage of hidden items, differing from one level to the next. Table 5.19 shows the percentage of hidden items, based on the twenty elements shared between Facebook and the proposed system for males.

Type of privacy	Percentage
Facebook	20.00%
Low privacy level	35.00%
Medium privacy level	45.00%
High privacy level	60.00%

Table 5.19: Percentage of hidden items, for males.

To compare the sensitivity of hiding selected personal information items, Facebook at present only hides 20% of the total number of 20 items, whereas even at the low privacy level of the proposed model, 35% of the items are hidden. As can be seen from Figure 5.11, Facebook only hides 4 of the 20 items, while the low privacy level of the proposed model hides 7 items. Furthermore, uploading videos or posting comments on Facebook requires an additional action from the user to select the type of sharing, such as whether sharing them with the public or friends, or whether hiding them from all.

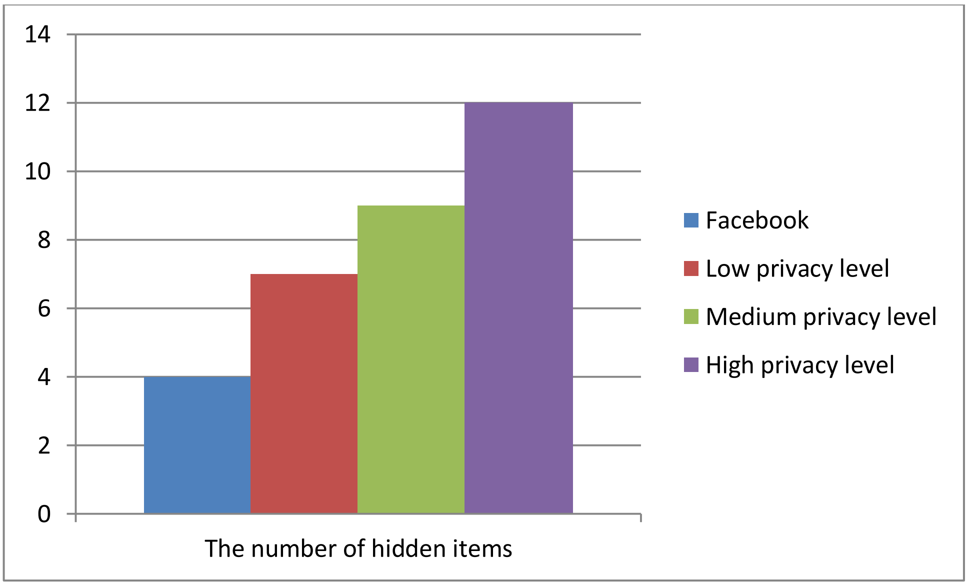


Figure 5.11: A comparison between the default privacy settings in Facebook and in the proposed system for males.

- ***Default privacy settings for females on Facebook in comparison with the proposed model***

In this study, a survey was done on different online social networking sites, such as Facebook, Twitter and Myspace, to discover whether there are special default privacy settings for females. The result of the survey showed that there is no site with special default privacy settings for females. Facebook, as one of the most famous online social networking sites, was used to create a comparison between the mechanisms for applying default settings for females. The reason for selecting it was that it has 20 items in common with the proposed framework. Therefore, this study will compare the results of applying the proposed framework for females with the default privacy settings in Facebook.

Item	**Facebook**	**The proposed system**		
		Low	Medium	High
Name	1	1	0	0
Gender	1	1	1	1
Email	0	0	0	0
Date of birth	0	0	0	0
Phone number	0	0	0	0
Physical address	None	0	0	0
Current address	1	0	0	0
School information	1	0	0	0
Hometown	1	0	0	0
Interests and activity	1	1	1	0
Favourite books	1	1	1	1
Favourite TV shows	1	1	1	1
Favourite music	1	1	1	1
Favourite movies	1	1	1	1
Relationship status	1	0	0	0
Pictures	1	0	0	0
Videos	Condition*	0	0	0
Comments and posts	Condition*	0	0	0
Tags	1	0	0	0
Friends list	1	0	0	0
Education and work	1	0	0	0
Religion	0	1	1	0
Website	1	1	0	0

* This item needs an action from the user to hide or show it.

("0" means that the item is hidden, "1" means that it is apparent)

Table 5.20: Default privacy settings for females.

As can be seen from Table 5.20, about 20 items were the same between Facebook and the proposed model, and this number is similar to the previous comparison. Two items were excluded, namely videos and posting comments, because on Facebook these items require an action from the user to define their sharing status. Moreover, the default privacy settings for the female gender on Facebook are similar to those for the male. So, it becomes clear that Facebook only uses one set of default privacy settings for both genders, unless the user has customised their sharing status for any of those items. This shows that the design of Facebook did not take into account the results of previous studies, as mentioned in the literature review, which showed that women are more sensitive about sharing information than men. However, under the current situation, when they use the default privacy settings in Facebook, female users will share several items that may be misused by others, such as current address, school information, photos and friends' lists. In the design of the proposed privacy model it was important to take into the account this aspect. So, the proposed model offers three different default privacy levels for females, and these levels are different from the levels for males. These levels were designed on the basis of the previous studies, as mentioned before, and the results were collected from the survey conducted for this study. A comparison of Facebook privacy with even the low privacy level of the proposed model shows that the difference in the number of hidden items is large. The default low privacy level of the proposed model for females will hide eleven shared personal information items, while Facebook hides only four items. Table 5.21 presents the percentage of hidden items based on the twenty elements shared between Facebook and the proposed system.

Type of privacy	Percentage
Facebook	20.00%
Low privacy level	55.00%
Medium privacy level	65.00%
High privacy level	75.00%

Table 5.21: Percentage of hidden items for females.

A comparison of Table 5.19 with Table 5.21 shows that females have more privacy than males on the proposed system, while on Facebook there is no consideration for the differences between the genders. While the sensitivity rating of the low privacy level for males is higher than the default settings in Facebook, the sensitivity percentage for females is higher than both of them. On the proposed system, the hidden items for males are 35% of the total number of shared items, but for females the percentage of hidden items is 55%. This means that the design of the proposed system took into account the difference between females and males, and this can also be seen in the other privacy levels.

Figure 5.12 shows a comparison between the total number of hidden items in Facebook, and in the three privacy levels of the proposed model. It shows that the default settings for the high privacy level of this model hide 15 of the 20 items shared with Facebook, and the low level hides 11 items. A comparison of the number of hidden items between males and females in the proposed model shows that the model gives greater privacy to the information for females than for males, and this was established based on the results of the previous surveys.

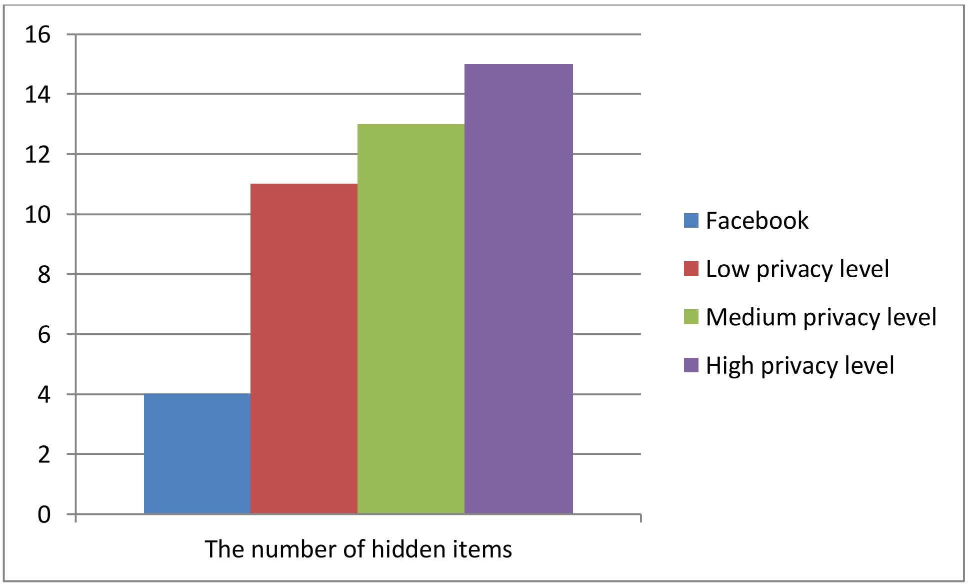


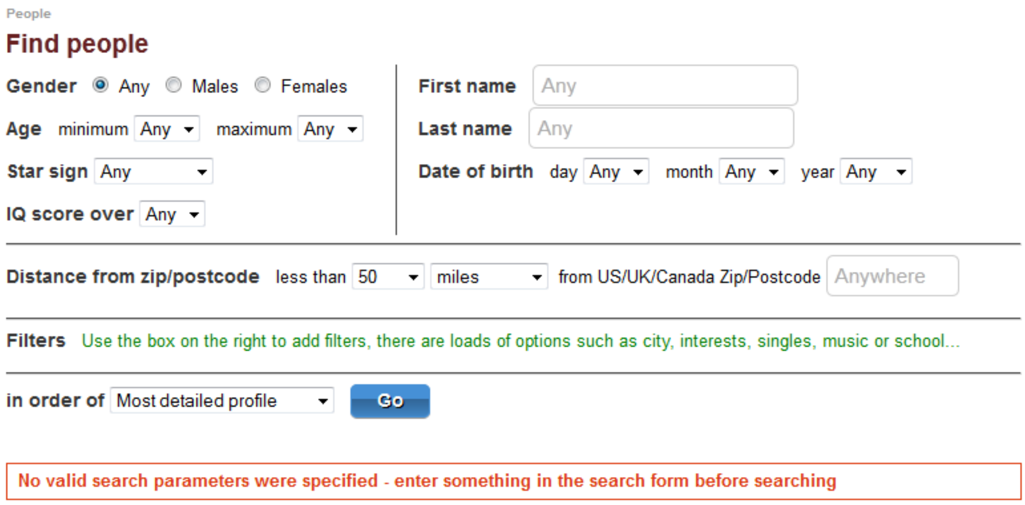
Figure 5.12: A comparison between selected default privacy settings in Facebook and in the proposed system for females.

- ***Accessing users' profiles via other websites***

In this section, the study will present a comparison between the results of the proposed privacy system and existing online systems from the perspective of accessing personal information via other sites. In this comparison, another site (www.profileengine.com) was used to show the differences in relation to another model, and the benefits obtained by applying the proposed model.

Profile Technology is one of the largest companies which specifically designs advanced social network search engines, and its most famous search engine is called the Profile Engine. This offers profile information for about 450 million people, of whom about 50 million users have their information accessed through their social networking accounts, without their giving permission to have their information collected (Profile Technology, 2014). This engine accesses profile pictures, date of birth, name, friends' list and other information.

As seen from Figure 5.13, the visitor is able to find other users by typing some information. Typing further information will reduce the results until the required person is identified. In this study, the researcher examined this search engine and checked what information it was able to reach without receiving permission from the profile owner, and then compared it with the access control process of the current study.



People

Find people

Gender ● Any ○ Males ○ Females

Age minimum Any maximum Any

Star sign Any

IQ score over Any

First name Any

Last name Any

Date of birth day Any month Any year Any

Distance from zip/postcode less than 50 miles from US/UK/Canada Zip/Postcode Anywhere

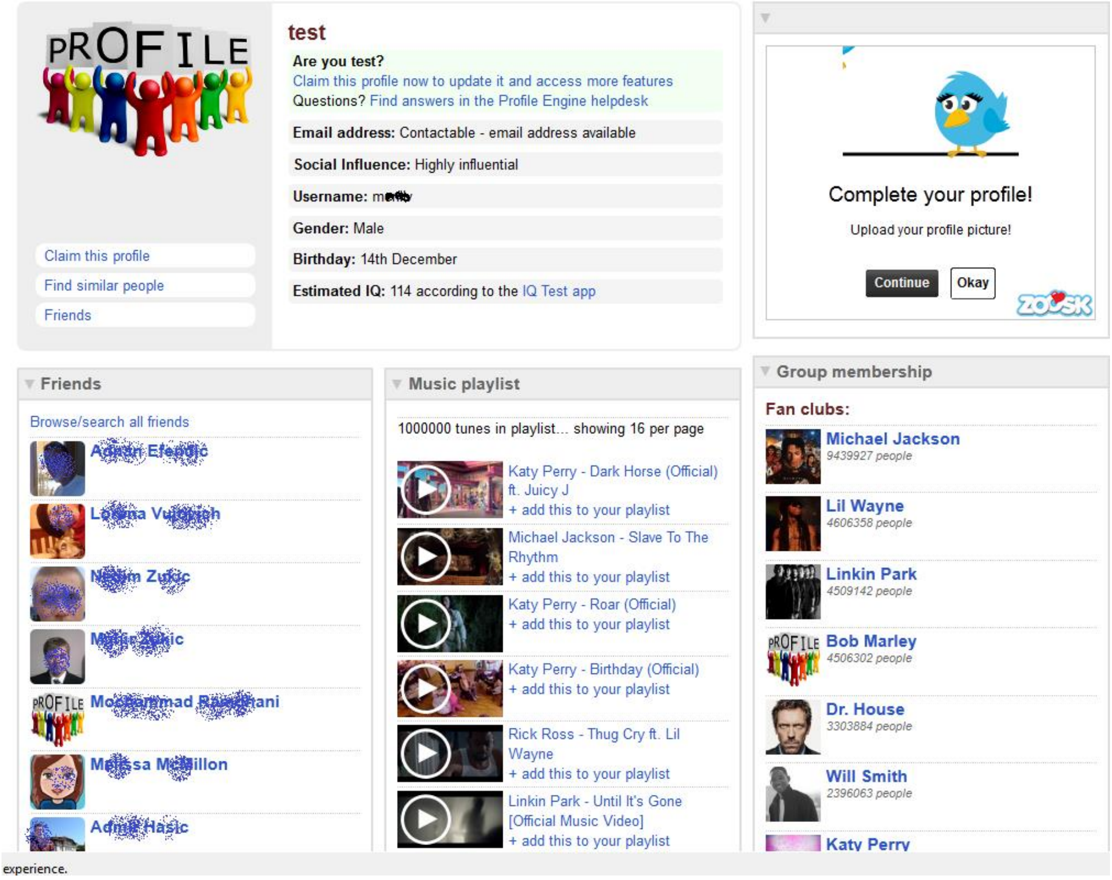
Filters Use the box on the right to add filters, there are loads of options such as city, interests, singles, music or school...

in order of Most detailed profile

No valid search parameters were specified - enter something in the search form before searching

Figure 5.13: Profile Engine search page

In this experiment, the value "test" used was the first name of a person, and it showed 21 exact matches for the search criteria. Selecting one of these results would then present different information about the user. Figure 5.14 presents the collected information about one randomly selected user.



test

Are you test?
Claim this profile now to update it and access more features
Questions? Find answers in the Profile Engine helpdesk

Email address: Contactable - email address available

Social Influence: Highly influential

Username: me[redacted]

Gender: Male

Birthday: 14th December

Estimated IQ: 114 according to the IQ Test app

Claim this profile
Find similar people
Friends

Complete your profile!

Upload your profile picture!

Friends

Browse/search all friends

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Music playlist

1000000 tunes in playlist... showing 16 per page

Katy Perry - Dark Horse (Official) ft. Juicy J
+ add this to your playlist

Michael Jackson - Slave To The Rhythm
+ add this to your playlist

Katy Perry - Roar (Official)
+ add this to your playlist

Katy Perry - Birthday (Official)
+ add this to your playlist

Rick Ross - Thug Cry ft. Lil Wayne
+ add this to your playlist

Linkin Park - Until It's Gone [Official Music Video]
+ add this to your playlist

Group membership

Fan clubs:

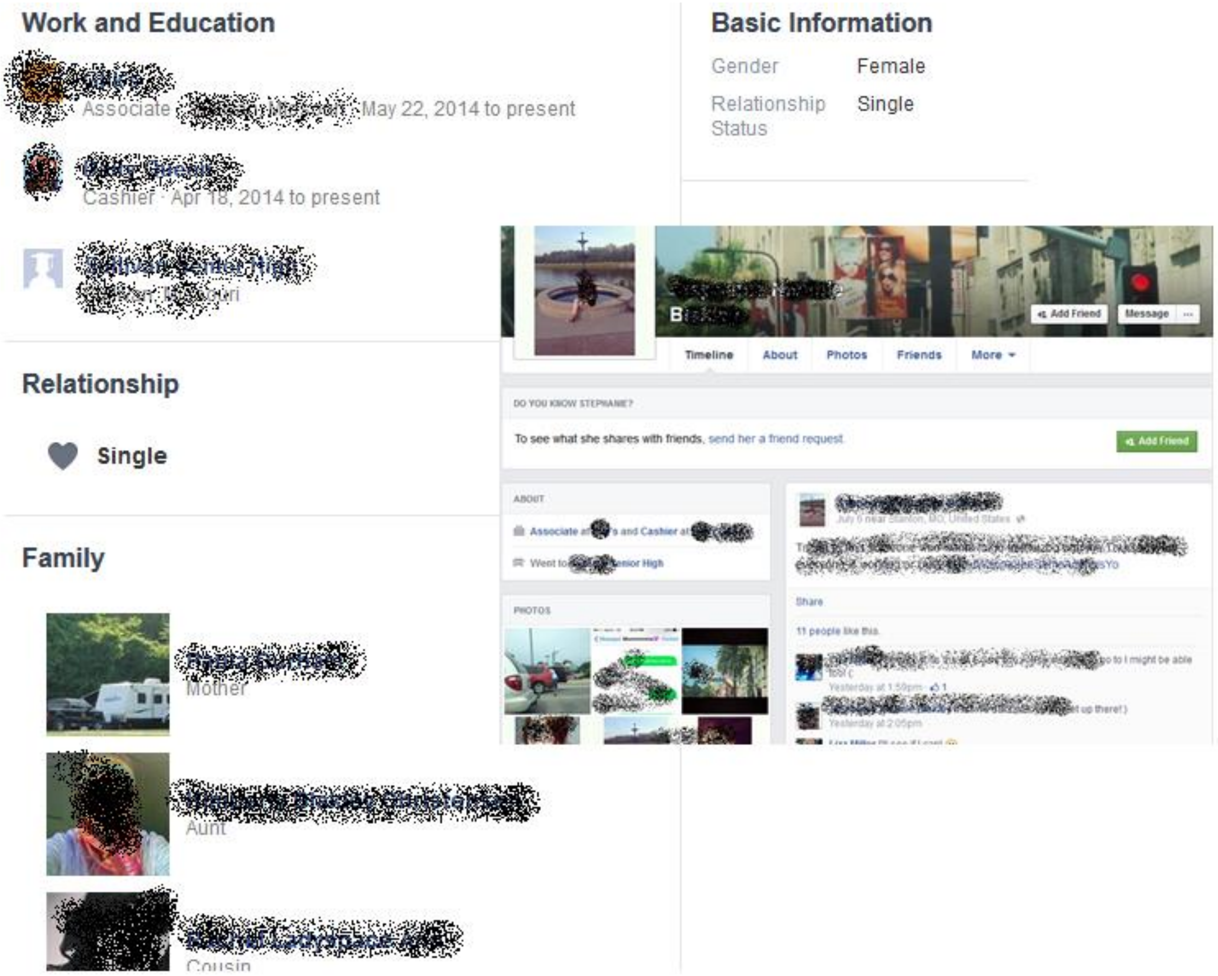
Michael Jackson	9439927 people
Lil Wayne	4606358 people
Linkin Park	4509142 people
Bob Marley	4506302 people
Dr. House	3303884 people
Will Smith	2396063 people
Katy Perry	

experience.

Figure 5.14: The result from selecting one user.

In this example, the Profile Engine viewed several items of personal information related to the user "test", such as username, date of birth, gender, friends' list and other information. It accessed the information that was presented in the Facebook profile. So, the information about Facebook users, and that from other social networking sites, has been shared without the users' knowledge and permission. The main privacy risk of the current online social networking sites is that the user is not the main administrator controlling his information privacy by setting a policy for sharing this information with other sites. However, the results from applying the proposed privacy framework show that the framework provides the users with greater privacy management, enabling them to control the sharing of their personal information with other sites.

To compare the current status of accessing personal information details in Facebook accounts via Profile Engine, an experiment was done to find more personal information about a random user. The first step was typing a random name into the field for the first name in the Profile Engine site. Clicking on the "go" button showed thousands of users with the name and one user (a female) was selected randomly. At this stage, Profile Engine presented several items of personal information about the user that could be used to identify her. The information extracted about the user included her name, gender, date of birth, friends list, favourite music, pictures, education and work. The next step for collecting more information about the user was to use the Facebook search engine to find the person who had these details. The results from applying the research statement led to the exact person, and this included the name and the profile photo. As seen from Figure 5.15, browsing the profile information assisted the researcher in this experiment to find more details that easily identified the user, such as family members, photos, videos, work and education, relationship status and even her comments and posts.



Work and Education

[redacted] Associate [redacted] May 22, 2014 to present

[redacted] Cashier · Apr 18, 2014 to present

[redacted]

Relationship

Single

Family

[redacted] Mother

[redacted] Aunt

[redacted] Cousin

Basic Information

Gender	Female
Relationship Status	Single

[redacted] B[redacted]

Add Friend Message ···

Timeline About Photos Friends More ▾

DO YOU KNOW STEPHANIE?

To see what she shares with friends, send her a friend request. Add Friend

ABOUT

Associate at [redacted]'s and Cashier at [redacted]

Went to [redacted] Senior High

PHOTOS

[redacted]

July 6 near Stanton, MO, United States

[redacted]

Share

11 people like this.

[redacted] so I might be able too! (:

Yesterday at 1:50pm · 1

[redacted] it up there!)

Yesterday at 2:05pm

Figure 5.15: The results of searching for the user on the Facebook site.

Therefore, the decision to share personal information with other sites among the current online social networking sites is not one of the user privileges, and personal information can be leaked and saved in other sites. So, one of the main ideas when designing the privacy framework of this study was to give users full control in managing the process of sharing their personal information with other sites.

- ***The differences in sharing information with other sites***

Traynor (2014) defined the social networking policy as a contract between the user and the service provider involving conduct that provides guidelines for the user who posts content on the internet. The goal of accepting this agreement is protecting the company from exposing it to legal problems or public embarrassment. Furthermore, a privacy policy is defined as a document or agreement that explains how the company handles and protects any user's information in its operation (Rutsaert et al. 2014). Thus, the social networking sites should also show the user in the privacy page any personal identifiable information that will be stored in the system such as name, age, date of birth, credit card details, as well as ways of protecting this information.

This point compares several differences between the results of applying the proposed framework and current social networking systems. As can be seen from Table 5.22, the comparison measured several standards that show the advantages of using the proposed system. It shows the differences between implementing the proposed framework and the current social networking sites. It presents the differences between the systems and shows some features that have been measured when applying the proposed framework.

Element of comparison	Current social networking sites (Facebook, Instagram and Myspace)	The proposed Framework
Saving personal information	Each site saves user information in a local database.	There is a centralised database to save personal information details and the created privacy policies
Accessing information from the local database via other sites	Other sites can access information without permission from the user.	Only the user can give permission to access his information on that site.
Copy the user information	It is possible to copy this information and this happened in the previous example (Profile Engine).	There is limited permission for other sites to read the defined information only and to view it via the main privacy server.
Distributing personal information when the user sets up an account	To create a new user, it is necessary to distribute his information to each site.	The user needs only to save his profile on the main server and to give defined permission to other sites to read some of the information.
Creating privacy policies	Some sites provide some custom-made privacy settings and the user needs to create a privacy policy on each site.	The system provides the option of creating several privacy policies and applying one policy to several sites without repeating the process of creating the policy.
Using a wizard tool to help the user set a privacy policy	They do not provide a wizard tool to help the user select the privacy settings.	It provides the user with a wizard tool to facilitate the selection of information to be shared.
Sharing personal information with other sites	The user has no management over his profile to control the sharing process with other sites.	The user must provide access permission before his information will be shared with other sites.

Table 5.22: A comparison between the implementation of the proposed system and other applications.

From the previous table it can be seen that the proposed privacy system in this study solved some privacy issues that can be found in other privacy systems such as Facebook, Instagram and Myspace. It provided the user with more permissions for controlling and creating the privacy policy by himself and apply it as the approved privacy policy applied on a specific site.

- ***Comparison of sharing information with a third party***

In this comparison, the researcher compared the situation when a third party required access to some profile details on a site. It presents the differences between the results of applying the proposed model and applying the current settings in Facebook to a case where a third party, or website, wants to access some information.

According to the privacy information instructions in Facebook about sharing profile information with a third party, it was recognised that the third party applicant would be able to access the public profile information, and should the user not want to share this information the application would not be successful. It also states that the user is able to increase the access privileges, but some information cannot be hidden from the public profile. In this case, the third party application can violate the user's privacy, especially when using their profile picture (Facebook, 2009).

The difference between the implemented framework in this study and the situation described with Facebook is that when the third party applicant wants to access profile information he will be prevented from even entering the system. This is because profile information is saved in the main privacy system, and other websites are only allowed limited access to view this data, without the ability to save this information to a local database. Moreover, this limited access also needs authorisation from the user, as mentioned before, before data in the main server can be accessed.

However, in the proposed framework the user is the main controller of the authentication process controlling access to information. This section shows what information can be accessed when the site provides the applicant with its login details. In this case, what access the applicant will have to the published profile information. As seen from Figure 5.16, the study argues the case from the default settings of both Facebook and the implemented framework of this study. Using the default privacy settings in Facebook will allow the applicant to access about 80% of the twenty shared items, but in the proposed framework the percentage of shared information will range from 65% at the low privacy level, to 40% in the high privacy level for the male gender. Females, as mentioned before, will have greater privacy, so the third party applicant will be able to access 45% of information where the low privacy information is selected, or 25% where the high privacy level is selected.

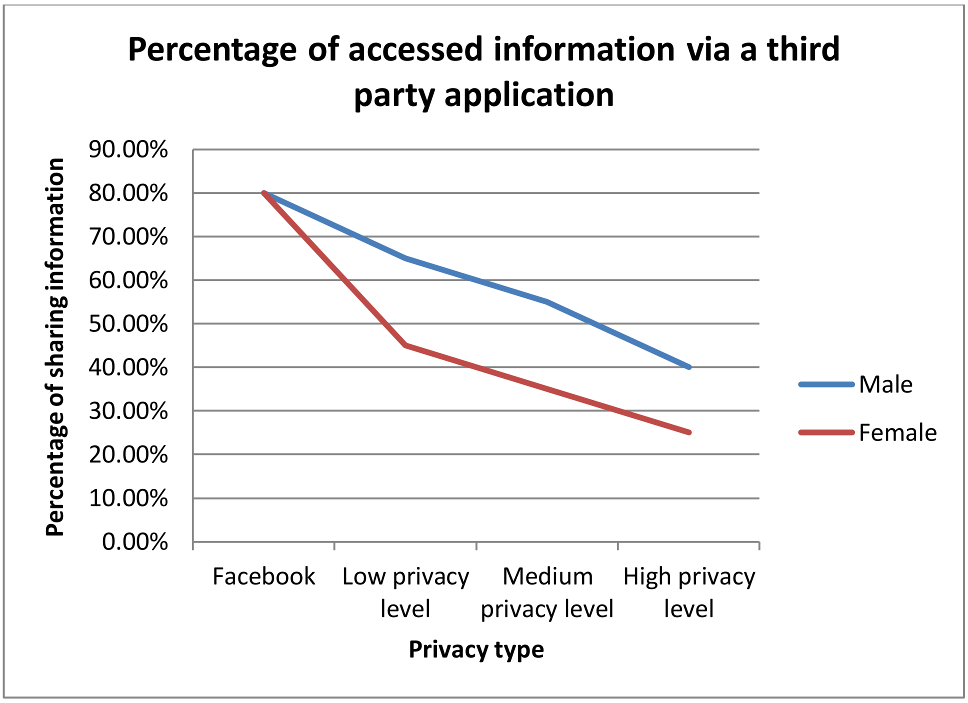


Figure 5.16: Percentage of items that can be accessed via a third party application.

5.5 The Results of Implementing the Whole Privacy System

As mentioned before, the design of the system contained several stages to reach the final results. Applying the whole privacy system offered some advantages that characterised this system from other privacy systems. These advantages are as follows:

- ***Usability***

This feature can be shown by minimising both the following factors: the content in the question window and the number of options to answer the wizard questions. All questions were understandable with each question having two or three options to answer it. This small amount of content contributed to fitting it within the size of an Internet mobile device's screen. Another factor showing the usability of the system is minimising the process of writing and distributing personal information details through the internet. Alice, Bob, John and Sam typed and stored their personal information details only once in Server 1. When they created different accounts in other servers, there was no need to type any personal information details. This can help users of Internet mobile devices to subscribe with any social network site without the need to rewrite their personal information. So users—whether they use Internet mobile devices or PCs—are able to subscribe with the server without repeating the process of writing their details.

- ***Flexibility***

Another feature discovered when applying the system was the flexibility in the signup process at different sites. Each social site or server has a convention to access the Server 1 database that will allow a new user to sign up quickly and share their required personal information details. This contributes to adjusting the process of exchanging personal information when taking into account the increase in the number of social networking sites. The user is therefore able to increase his/her subscriptions over a large number of sites without the need to fill his/her personal information again.

- ***Security***

One of the main features of the system is security. The implemented system was designed to minimise the process of distributing personal information via different websites. As seen from the previous implementation, Alice, Bob, John and Sam only saved their personal information in the Server 1 database. They created several access policies to be applied for each site. Servers 2, 3 and 4 were not able to access the restricted items, and users received the value 'not allowed' from Server 1. Moreover, the centrality of personal information in Server 1 facilitated the subscribe process on the other servers because users only needed to enter a few details (such as username and password) for that site.

As discussed in the literature review and the methodology chapters, it is important for any organisation to consider taking a security by design approach to be able to provide security seamlessly in its applications. So, the security approach in this study is markedly similar to the PayPal system. In PayPal, the user needs to save their credit card details in the local database. When they want to buy an item from another site that supports PayPal payments, they only need to authorise the payment and define a specific amount of money. The implemented privacy system has a similar idea. In Server 1, users are required to save their personal information details in the local database. When users want to subscribe to a site that has a compatibility connection with Server 1, they only need to authorise that site to access the Server 1 database and define the suitable privacy policy to be applied to it. The experiment of using PayPal for payment methods offers more flexibility for users to buy items from different websites. So, with the rapid growth of social networking sites, users can subscribe at any social network site and can confidently take advantage of its services. They will be able to identify the information they will share with the site, and modify the current applied privacy policy at any time without requiring permission from that site.

5.6 Conclusion

This chapter presented the findings of the study and discussed each part separately. It consists of four main parts that include a statistical analysis and a detailed description presenting the results. The parts discussed the findings of both questionnaires and the results of implementing the Smart Wizard System and the whole privacy system.

This chapter discussed the questionnaire results in a statistical manner. The results have been verified and tested by checking the reliability and validity of the survey. The results show that participants have concerns about the misuse of certain personal information items, and hence the current privacy settings methods require more development. They also show that Internet mobile devices are used widely to browse the Internet, but the current methods of controlling privacy policies are not always suitable for the size of internet mobile screens.

In addition, the results classified personal information items into three levels: high, medium and low. Both male and female genders are sensitive to sharing any item that can assist in determining their identities. Therefore, the next step of this study was to design a flexible framework that would assist users to control their privacy settings irrespective of whether they used Internet mobile devices or others.

The second goal of this study was to code software that included two sub-applications: the Smart Wizard System and the whole privacy system. The first application was tested and the accuracy of the system was calculated. While the Smart Wizard System is a recommended system that gives the user a suggested privacy policy based on answering certain questions, the calculation of its efficiency yielded a high success rate. The second application has been designed to allow the main server (Server 1) to create various privacy policies by using the Smart Wizard System. It authorises access from other servers to read restricted personal information details from its local database.

The implementation results found that in Server 1 the user was able to save their personal information only in that server. It was also shown that the included Smart Wizard System allowed the user to create different privacy policies and to save them with different names. When the user wanted to subscribe in one server—or to a social network site—they simply needed to create a login account without having to enter personal information. After creating the account, the user was permitted to determine a suitable privacy policy to be applied on the site through an authentication process with Server 1. As a result, the whole privacy system offers several features that enable the ownership of many social network site accounts without losing control of exchanging personal information details with other sites.

Chapter 6: Conclusion

6.1 Introduction

In recent years, the use of different online social networking services has increased with the number of users varying from one site to another. The competition between these sites to attract more users encourages them to develop new services. For example, Instagram is characterised by sharing pictures and KeeK by publishing videos. Furthermore, the characteristics of internet mobile device design have contributed to expanding the use of these services to a wide range of people. They have begun using different internet services such as browsing, chatting and sharing files on mobile devices every day. As a result, internet mobile devices are no longer limited to making phone calls; nowadays, they are used to communicate more broadly with other people such as by exchanging different files and information with them through the web.

The diversity of these services has led to the dissemination of a large amount of information through the web. Some users are not aware of the risk of anonymous people or hackers misusing their information. Some of them have decided to refrain from the use of these services, and some others have contented themselves with only using one service. However, the developers of online social networking sites are also concerned about privacy issues. Therefore, they have designed several privacy frameworks to protect users' privacy. The online social networking sites Facebook and Google Plus are examples of sites that provide different options and controls for users to modify their privacy settings. The separate development of security techniques at an individual site does not fix the issue of sharing personal details over a variety of online sites. From this perspective, it was necessary to develop a framework that facilitates the control of privacy while sharing personal information via different sites, and also to support this control when using internet mobile devices.

This study showed the impact of distributing personal information via different internet sites and users' concerns about the misuse of these details. It also presented the current privacy frameworks that have privacy controls on sharing personal information.

This chapter will review the research statement, suggestions and findings. It will discuss the findings based on a statistical analysis and explore the relationships between them. All the hypotheses developed in this study will be reviewed. Moreover, this chapter will present the Smart Wizard System and the proposed privacy framework. It will show the operations for implementing both of them. Finally, this chapter will review the limitations of the study and summarise future work.

6.2 Summary of the Study

This section provides a summary of the research problem and outlines the general questions that were investigated in this study. It will also show a brief description of the hypotheses and the research methodology. Furthermore, the findings relating to applying the methodology will be discussed.

6.2.1 Research problem

Online social network use is not limited to adults; high numbers of children in some countries also have accounts. Livingstone, Ólafsson and Staksrud (2011) found that about 77% of European children 13–16 years of age have profiles in at least one social network. A survey by Ai Ho, Maiga and Aimeuer (2009), which included 200 participants, revealed some problems with privacy issues. The most pressing issue was that sites did not clearly inform users of the risk that divulged personal information could be misused. The very fact of the large number of SNS users may encourage an increase in the number of malicious attacks (Feldman et al. 2012), thus affecting privacy in various ways. While the use of online SNS offers many benefits, such as finding friends and jobs, the placement of ever-more personal information on such sites can create privacy risks for some users; this is particularly the case if a user is not sophisticated (Alsalibi et al. 2013). Therefore, Yuan et al. (2010) emphasised that protection of user privacy is the responsibility of the service provider.

While communication has become easier with online social networking applications, protecting users' privacy has become more complicated, especially with the differences between these applications. Each online social network provider uses different settings and protection methods. Furthermore, trust is an important element for protecting privacy, and it can be divided into two parts: trusting the provider and trusting the user (Hughes 2009). Boyd (2011) found that people with internet knowledge are more aware of SNS privacy issues because of their general knowledge of security settings and privacy risks. A study done by Pavlou and Fygenson (2006) found that users with knowledge about using both SNS and online transactions have more privacy concerns, but their concern about online transactions is higher than about SNS. Moreover, there are simple ways to increase users' knowledge of privacy concerns. Lipford, Besmer and Watson (2008) found that showing an example of privacy settings will enable users to understand their privacy settings better and help them find out who can see their personal information. In addition, Bae and Kim (2010) suggested that, in order to achieve a high level of privacy, the user should be given the authority to control the privacy settings when he/she receives or requests a service related to his/her personal information. As another practical solution, Bekara, Kheira and Laurent (2010) developed a framework for enhancing privacy in identity management by introducing a middle-ware privacy level to give users more control of personal information. In addition, Kolter and Pernul (2009) emphasised that design simplicity, especially of the interface and tools of a privacy program, allowed users to protect personal information optimally.

In recent years, internet mobile devices have gradually begun pulling the rug from under desktop computers. The popularity of browsing the internet using mobile devices or tablets services has increased. For this reason, different internet mobile companies, such as Apple and Samsung, have produced several types of mobile web devices. The strong competition between them leads to the development of new devices with added hardware and software techniques that make using mobile devices for internet services easier and more effective. According to Lane et al. (2010), some factors have affected the increased sales of internet mobile devices around the world. Some of these reasons include the low cost of embedded sensors and chips as well as the availability of different kinds of internet mobile applications and offering applications that support sharing real-time activities with others, such as Facebook or Twitter applications. Beach et al. (2010) pointed out that the online social networks such as Facebook, Twitter and MySpace will impact support for mobile web devices. A study done by Bullas (2012) showed that in August 2010, 30 million users of the Instagram application shared about 150 million photos. Various companies have developed mobile-specific internet browsers including versions of Opera, Internet Explorer and Safari (Lewis & Moscovitz 2009). Today, most mobile internet browsers support various programming languages including HTML and JavaScript, but they do not browse as effectively as laptops or PCs do because the screens and keyboards are smaller (Guan 2011).

However, several studies have discussed different types of privacy risks related to personal information details on online social networks, and a few studies have discussed the usability of internet mobile devices for browsing. None of them, however, have suggested a system or an idea to facilitate the use of internet mobile devices to control personal information privacy settings in order to protect the user from distributing his/her personal information on different online social networking sites. Thus, the current study focuses on designing a framework to keep pace with the development in internet mobile devices and enhance privacy awareness for users in order to control their personal information privacy settings in mobile web systems.

Based on the previously outlined research problem, the main research question for this thesis was:

How can online personal information privacy issues be addressed satisfactorily in an integrated services scenario, involving different types of mobile devices, in order that the confidence of users in the effective protection of their personal details from misuse can be increased?

Therefore, the main research objectives that underpinned the main research question for this study were to:

❖ Propose a privacy-aware framework supporting most internet mobile devices to increase the confidence of mobile device users.

The developed privacy framework in this study allowed the user from being familiar with knowing which information can share with other sites. It gave the user a full authority to share his personal information rather than being a partial controller.

❖ Develop a privacy model that is suitable for controlling personal information settings through internet mobile devices.

The use of the smart wizard tool facilitated the difficulty in some internet mobile devices of controlling the privacy policies . It was based on selecting few options that answering some quick questions to recommend a suitable privacy policy for the user.

- ❖ Develop a privacy management model to support users' ability to manage their personal information.

The centralised of the privacy system offered a solution of distribution personal information among the web several times to subscribe in different applications. It allowed the user of creating a main account that contains all personal information details. In case of subscribing in any other social media sites he only needs to define which information will be allowed to be accessed from the main account without a repetition of typing these personal information details again.

- ❖ Design a prototype system to verify the framework and models.

The prototype system was designed and tested and the smart wizard tool was included to the main privacy system (server 1). The tool was tested successfully and evaluated by more than 400 participants and the accuracy of it was calculated mathematically as mentioned before. Moreover, the simulation of the system was designed also. There were virtual users created to check the success of the system and three sites to have access to the main privacy server. The connection between them was created and the access policies for these sites to reach some personal information was also achieved. Therefore, the prototype system was successfully built.

As shown in the previous chapter, the suggested framework assisted internet users to increase their confidence in using different accounts for different social networking sites. With the smart wizard tool, the process of creating a privacy policy has become easier and faster. Creating these policies gives the user full control of accessing and sharing his/her personal information via other sites. It also prevents a recurrence of the dissemination of information. In this study the user was able to create an account in the main privacy system and save their personal information. The next step was to create different privacy policies via the smart wizard tool. When users create any profile in any other site, they only require to link this profile with the main privacy site and define the suitable privacy policy authorised to access only selected information. All these processes can be performed simply via using different types of mobile devices.

6.2.2 Research hypotheses

To answer the previous research question and achieve the objectives, the researcher formulated several hypotheses based on justifying and grounding security on social networking sites and trust and usability on internet mobile devices from the existing relevant literature on privacy concerns. . The four hypotheses of this study were the following:

H1: Users can manage their created privacy policies through internet mobile devices and add a new privacy policy at any time in a simple way.

As seen from the previous chapter the proposed framework in this study offered an easy way to manage the privacy settings through mobile phones or tablets. This can be seen clearly by avoiding the repetition of typing personal information details in the case of creating a new account for any social networking site. It also used the smart wizard tool that simplified the operation of zooming the page view to see the contents and minimise the number of hidden or shown items within the twenty three items of his/her personal information profile.

H2: Users have the authority to set a privacy policy for any internet site to control access to their personal information.

The framework presented in this study has made the user an administrator defining which information may be shared with any new linked site when it is connected to the main privacy system. The user was able to save this information in the main server and create different access policies that give other sites an authorisation to access specific information only. So, the only way to access this information is based on user's permission followed by the specification of the created privacy policy.

H3: Each internet site has limited access to reach a user’s personal information, created previously by the user. It also does not have any authority to save any personal information detail, and it is only able to read.

As seen from the previous chapter, the created accounts for Alice, Bob, John and Sam in the main privacy server have their personal information details. Other accounts for them in other websites have only the local login details (username and password). These users gave each site an access to only read some personal information from the main server based on the defined privacy policy for this site. Therefore, this hypothesis has been verified in the proposed framework.

H4: The wizard is a tool that helps users to create different privacy policies in the data server through an internet mobile device and to provide users with the ability to hide or show the items in the created privacy policy. The user will be able to use it to create different privacy policies.

The created smart wizard tool in this study was based on analysis of the participants' answers. The idea of designing it was by grouping the status of hiding or showing some personal information by using simple questions about showing some common elements such as favourite movies, favourite music and favourite books. This tool has been tested, and all the modifications that had been done by the participants in the suggested settings for the created privacy policy were taken into account. As a result, after the successful accuracy of this tool shown by the percentage of participants attitudes favouring it , it has been included as a part of the design of the proposed framework in this study.

The testing of these four hypotheses was used to design a framework that enhances privacy awareness for users by controlling the process of sharing personal information via different websites. It is also suitable to be controlled by internet mobile devices.

6.3 Research Methodology

The purpose of the methodology in this research was to present the methods that were used to design a framework to enhance the privacy level of exchanging personal information via the web and provide the user with more tools to control the sharing processes. The methodology consisted of five sequential stages and each stage was carried out with scientific method.

The first task was collecting data using a qualitative approach. The findings were then used to design the first tool of the framework. This task examined the use of online social networking sites, privacy concerns, the usability of internet mobile devices and the privacy significance of personal information items. The total number of respondents who completed the survey was 185.

The second task was designing a Smart Wizard System that recommends a privacy policy for the user based on answering a few questions. This system was built upon the results of the previous task. It used short questions that asked the user to allow or deny some items to be shared. The simplicity in the interface assists the user to select these options via an internet mobile device.

The third task was testing the Smart Wizard System and determining the suitability of it. There were 439 participants who implemented the Smart Wizard System.

The fourth step was designing the whole privacy framework. In this task, the researcher set different techniques and strategies to design the system. The previous Smart Wizard System was included as part of the system. Regarding the nature of the whole privacy system, the user is only required to save his/her personal information details in the privacy server and then he/she will be able to create different privacy policies. Thus, when the user wants to subscribe to any other website that needs access to some personal information items, he/she need only login to the privacy system via that site and define a specific privacy policy to enable the application.

The last task of the methodology was implementing the whole privacy system and then discussing the findings. The implementation was applied based on creating different users and setting different privacy policies for each user on different sites. The main purpose of these steps was to check the validity of applying this system in a real world environment.

6.3.1 Conclusions about the collected data from task 1

Several facts were found from the analysis of the survey findings. The results showed that about 45% of respondents had more than one online social networking account and about 66.5% were concerned about privacy issues on online social networks. In addition, the survey showed that about 37% of respondents had had social networking accounts for more than three years and that this percentage had more than doubled in the last three years. Another finding that emerged from the results is that participants used their mobile phones for a variety of uses. Most respondents used mobile services, such as accessing email, chatting and accessing social networks, but only

34% of them changed the privacy settings for their online social accounts through their internet mobile devices. Furthermore, another aspect found was that most users rated some personal information items as highly sensitive items that they prefer to hide from others. These were items that can identify the users, such as photographs, mobile number and addresses. These results were used to design the Smart Wizard System.

6.3.2 Conclusions about the Smart Wizard System from task 2

The Smart Wizard System has been designed based on the results from the previous task. The design of the system was based on tree structures that ask the user some questions about giving permission to share some personal information items with other sites or not. The overall design of the system was built to recommend a suitable privacy policy based upon the user's choices. The next task was implementing this system and testing how satisfied participants were with the recommended privacy policy.

6.3.3 Conclusions about implementing the Smart Wizard System from task 3

This task consisted of two parts: implementation of the Smart Wizard System and measuring the concerns of users about others misusing their personal information items. A total of 439 respondents implemented the wizard and completed the participation process. The results showed that the percentage of user satisfaction with the recommended privacy policy given by the system was satisfactory. It achieved 98.4% of the total percentage of satisfaction for the recommended privacy policy. The second part of this task involved concerns about hidden personal information items.There were 205 respondents who completed this part of the survey. The results showed that females were more concerned about the misuse of their personal information than males, but this does not mean boys were not concerned about these details. Both genders were concerned about all items that can identify their personal identity. Hence, the majority of respondents who have concerns about these items hide them in their current profiles.

6.3.4 Conclusions about designing the whole privacy system from task 4

This task, as mentioned previously, was designing a framework that helps users to control the process of sharing their personal information with other sites. Each user needed to create a main account in the privacy server that contained his/her personal information details. The next step would be creating different privacy policies and saving them in this server. These privacy policies would be used when the user creates other accounts on different sites and authorises them to access some personal information details by applying one privacy policy. This system was designed based on SQL Server structures and ASP.Net as programming languages. The final design of the framework achieved several goals. The user of this system would be able to save his/her personal information securely in one database and there was no need to distribute these details among other sites. It also offers more usability to control the privacy settings by using internet mobile devices. In addition, creating different privacy policies to be applied on other sites is a unique idea. To know more about the results of testing the system, the next task would be to browse them.

6.3.5 Conclusions about the implementation of the whole privacy system from task 5

This task was conducted to test the privacy system and define the efficiency of it. The main privacy server was set on one site and the other servers (servers 2, 3 and 4) were set on different sites to simulate the real connections between different sites, such as the communication between EBay and PayPal websites. In the experiment, four users were created and each user had three different privacy policies to access specific personal information items. For other sites, the researcher assumed that each user selected one privacy policy to be applied on this site from the main privacy server via a secure connection that links this site with the privacy server. As a result of creating these accounts, each user was able to authorise any site to access specific personal information items without distributing his/her personal information more than once. There were also several advantages found by this experiment. The usability was one of the important findings. It offered more flexibility to easily subscribe and control the personal information privacy settings. This feature enabled this privacy system to be used from internet mobile systems. It also provided users with more confidence when they subscribe to any site, because they would be sure that the site does not have any authority to communicate with the privacy server unless they gave it permission and set a specific privacy policy on it.

6.3.6 Conclusions concerning the results of the research hypotheses

H1: Users can manage their created privacy policies through internet mobile devices and add a new privacy policy at any time in a simple way.

Dhar and Varshney (2011) discussed the present and future high-speed networks used by the mobile web; for instance, 4G technology offers high-speed access for the mobile web, and it will create new market opportunities. Moreover, Lenhart et al. (2010) showed that approximately 55% of adults use their mobile phones to connect to the internet. Furthermore, Schmiedl, Seidl and Temper (2009) suggested that, in the future, mobile phones, rather than desktop computers, will be the main device for browsing. So, this system took into account the suitability in the design (interface design) for supporting the process of controlling privacy settings via internet mobile devices. The privacy framework used two techniques to increase the usability percentage in mobile systems. Firstly, the framework used the tree structure technique for designing the Smart Wizard System. This technique was used to minimise the number of changes to the status of different personal information items. In the study, the Smart Wizard System allowed the user to adjust the sharing status of 23 items by answering a few questions, which did not exceed eight questions in the extreme case. Secondly, it reduced the amount of personal information details that were required to create an account on any social networking site. In this study, the user only needed to enter a username and password to be a member of this site and this can easily be done by using different types of mobile devices. So, with the usage of the Smart Wizard System, the user can easily add a new privacy policy in a simple and fast way.

H2: Users have the authority to set a privacy policy for any internet site to have access to their personal information.

The significant amount of personal information about existing users on social networking sites makes the concept of privacy widely used in terms of personal information in social networking sites, and the risks are unpredictable (Dwyer, Hiltz & Widmeyer 2008). Indeed, the misuse of such information may generate an opportunity for some people to exploit individuals' information in different ways, such as identity theft, financial transactions and extortion (Son & Kim 2008). Furthermore, Bae and Kim (2010) suggested that, in order to achieve a high level of privacy, the user should be given the authority to control privacy settings when he/she receives or requests a service related to his/her personal information. Therefore, one of the main aims of the study was to design a framework that gave users the authority to specify different access specifications for any site that wanted to access personal information. In the implemented privacy system, all users (Alice, Bob, John and Sam) were able to create different privacy policies in server 1. Each user applied one privacy policy on each server to access some personal information items from the server 1 database. For example, John applied the privacy policy on server 3, which does not allow this site to read any personal information items. Thus, server 3 was not allowed to access any personal information item. This can be applied on all other servers to define which items are allowed or not allowed to be shared with them.

H3: Each internet site has limited access to reach a user's personal information, and this was created previously by the user. It also does not have any authority to save any personal information detail, and it is only able to read.

One of the major challenges for online systems, specifically e-commerce systems, is the security of personal information. Although the extent of cybercrime is not clear, it has been on the rise since 2007. Cybercrime in e-commerce targets classified personal information, thereby exposing individuals to risks of fraud that may lead to significant uninsured losses (Panigrahi 2009). Since the idea of the research approach is similar to the commercial procurement process through PayPal, it was necessary to focus on the stages of designing the frameworks for the protection of personal information. Therefore, to provide more security procedures on the system, it was suggested in this study to deny any other site from copying any personal information items. Repeating the copy process of the data in many servers may lead to spreading these data among different sites, and this may cause a weakening in the proposed privacy system. Centralised personal information details on an online system and giving a read access was another idea of the framework. When Alice or any other user authorised a website to access the privacy system database, this site was only able to save the identification information for the applied privacy system. It would save the name of the selected privacy policy and the identification number in the local database. The processes of reading and browsing personal information items from servers 2, 3 and 4 windows would be done via browsing these details through direct access with the server 1 database. Hence, servers 2, 3 and 4 would call the allowed values after checking the type of the authorised policy to be presented in the local window.

H4: The wizard is a tool that helps users to create different privacy policies in the data server through an internet mobile device and to provide users with the ability to hide or show the items in the created privacy policy.

Touch screen technology has gained wide acceptance and is used in mobile phones, iPods, music players and other devices (McGookin, Brewster & Jiang 2008). Several studies have been done focusing on the usability of internet mobile devices based on information needs and diversity in the use of internet services. Sohn et al. (2008) conducted a study about mobile information needs and found that 72% of participants used internet mobile devices to collect information about activities, locations, times and conversations with others. Similarly, Church and Smyth (2009) found that 67% of participants used internet mobile devices for collecting information about locations, times, activities and social communications. In most current social networking sites, users can customise privacy settings and policies. They may restrict access to photographs, videos or other personal data (Dwyer et al. 2010). Several techniques are available to simplify systems used to select privacy settings. Therefore, Toch, Sadeh and Hong (2010) suggested the development of a wizard allowing users to decline to share their locations with others. In this study, designing a Smart Wizard System was a main goal to distinguish this framework from others. This wizard was included as a main part in the design of the privacy system. It will assist users by providing them with different recommended privacy policies based on their answers. The accuracy of the created wizard system was tested by a total of 439 respondents and it achieved 98.4% of the total percentage of satisfaction for the recommended privacy policy. The wizard also has the ability to modify the recommended privacy settings. It allows the user to change the status of sharing any personal information items before or after saving the recommended privacy policy. Therefore, this tool was designed to provide users with privacy recommendations to adjust the privacy settings for their personal information items in a simple way that supports different types of internet mobile devices.

6.4 Contributions of the Study

This study provides several practitioner contributions for different areas such as the literature, online social networking site users and privacy system developers. The researcher summarised these contributions as outlined below.

6.4.1 Contributions to the literature

This study provided several contributions to the literature that may help other researchers to discuss different issues. It provided the reader with a better understanding and new insights about the risks involved in online social networks, privacy concerns and the concerns about the misuse of some personal information details. It also provided the reader with more knowledge about the current privacy systems and the technologies used to secure their details. In addition, it showed why the idea of using PayPal for payment was and still is successful.

The topic of using mobile web systems to surf the internet was another issue that may assist other researchers to open their minds in developing some research in this area. The study showed the rapid increase in the use of internet mobile devices and how the current privacy applications need to be compatible with the use of mobile devices.

Furthermore, from the analysis of the findings, it was clear that respondents were concerned about others misusing their personal information. A high percentage of them used internet mobile devices for different internet services. It also showed that current privacy systems face difficulties when the user controls them via an internet mobile device. Finally, the research indicated that trusting the developer is an important element for users in deciding whether or not to use the services provided.

6.4.2 Contributions for social network site users

This study contributes to increasing the practical knowledge of users and developers. It provides users with awareness of personal information privacy in both theory and practical aspects. It assists users to be aware of privacy concerns and the side effect of distributing their personal information among different websites. Reading the literature (Chapter 2) will draw a security picture in users' minds about the risks of others misusing their personal information. Similarly, it emphasised that trust is an essential factor in building a successful relationship between users and application developers.

On the other hand, the practical aspect in this study provides users with practical solutions for controlling privacy settings through internet mobile devices. They will be able to modify or add a new privacy policy easily through these devices. It also offers the feature of managing the privacy settings for different sites via only one main site. Hence, they are able to subscribe or create different social networking accounts on the web without needing to re-enter personal information.

6.4.3 Contributions for social network site developers

As seen from the literature review (Chapter 2), there are millions of users who have online social networking accounts. Each site has its own privacy system and the competition between them has become fierce. Application developers should be aware of users' privacy concerns about the misuse of their personal information. They also have to notice that the use of internet mobile devices is on the rise. Therefore, this study suggested creating a developers' union for online social networking sites. They should work together to design a main privacy system that secures all users' information. This study presented a privacy system that contains a Smart Wizard System as a tool so users do not have to set different privacy policies. This tool can be used from different types of mobile devices. Furthermore, the proposed framework provides an application that described the work nature of the system. It showed how the user is able to create different privacy policies in the main server and how other websites can access some personal information items based on the applied privacy policy.

6.5 Limitations of the Study and Future Research Opportunities

As in all research, there are some limitations to this study. Some findings may be affected by the limitations. These constraints occurred during the study and were caused by circumstances imposed on the researcher. Nevertheless, some of the limitations discussed in this section can be used to open new areas of research and encourage other researchers to conduct studies on them. The following paragraphs will discuss some limitations of the study and suggest guidelines for future research.

Firstly, there were some limitations in the study's first task that may have affected the data collection techniques. These limitations were related to sampling issues and the required time to collect the questionnaire. There were several efforts to collect data from many different sources, but it was only collected from two countries. As the questionnaire was hard copy it was difficult to combine and apply all the questions in more than one locality: in Saudi Arabia, for instance, the sample was collected from males only because of some religious conditions and the nature of society. The required time to collect data was also limited based on the approved timeline. Therefore, lack of diversity in the sample may contribute to decreasing the accuracy of the results.

Secondly, in the third research task (the implementation of the Smart Wizard System), the invitation to participate was sent via email and it was also posted on some Facebook sites interested in information technology. Despite efforts to invite more participants for this implementation, the consequences of posting the invitation on these sites tended to restrict the classification of the sample to Facebook users. This limited the researcher's ability to do a comparison between the selected privacy levels of online social network users based on their choices, for example, comparing the selected privacy levels of Facebook with Instagram users. However, this presents an opportunity to do further studies in this area.

On the other hand, the second part of the third task, which was about measuring the concerns of users about the misuse of some personal information items from their profiles and whether or not to hide these items, is likely to be affected by respondent fatigue bias (Lavrakas 2008). Respondents were asked to evaluate 23 items by defining their concern about each item and the status of sharing it with others on their profile. This may have caused them to become fatigued.

Secondly, time constraints were a source of concern to the researcher regarding the time taken for collecting data and designing the whole privacy framework. The time taken for collecting data in the first and the third tasks of the study set various constraints such as getting approval to collect data, contacting different administrators and giving the volunteers a chance to collect the questionnaire. Indeed, collecting data was based on the permission provided by the University of New England and the acceptance from participants. In the first task of the study, collecting data was more complicated because it was applied in two different countries and the permission was needed from both universities (in Australia, it was provided by the University of New England and in Saudi Arabia it was provided by the University of Dammam). The short time for data collection in Saudi Arabia narrowed the sample to one college in the University of Dammam. This constraint did not help to make an extra comparison to find the difference between the selected privacy answers for students from various colleges. This point can also be used to do further studies and discover new areas.

Moreover, further work can be done based on the findings of this study. Researchers can do some research about trusting the services provided by online social network providers, developing other privacy frameworks and creating an approach for the development of agreements between social network providers and other aspects. Additionally, in general terms, the experiment of centralised personal information details in one server and giving access to other sites to reach limited data was successful and adding a Smart Wizard System as a tool helped internet mobile users to control their privacy settings on different websites. These points are important to start thinking about developing the current privacy system to suit the increase in the number of internet mobile users and the number of online social networking sites that require users to enter some personal information details. This study also opens other issues to discuss the designing of some security systems that encrypt the communication among servers and the data storage such as adding the net token as an additional tool for authentication. Hence, it is suggested to continue this study and explore further investigations to provide a high and flexible system that protects the privacy of online users.

6.6 Summary

The goal of this study was to design a framework that enhances privacy awareness in mobile web systems. This system allowed users to save their personal information system in one main server so there is no need to repeat the saving of them again in other servers. When the user wants to create a new account on a social networking site that requires entering personal information details, he/she only needs to authorise it to reach some personal information items from the main server. One of the framework’s features is the ability to create different privacy policies for controlling the sharing process with other sites. The creation of these policies can be done using a Smart Wizard System that allows the user to create them quickly and easily. This tool and the method of creating a new account make the framework suitable for use via mobile web systems.

For this purpose, the research developed a conceptual model that simulates the nature of the proposed framework. It described the structure of the system and the method of accessing information. It also showed how this system differs from other systems. The methodology section provided a clear description of all the executed steps to implement the system.

The results gave insights about users' attitudes and concerns about sharing some personal information items. It also tested the Smart Wizard System and the privacy framework by allowing the participants to implement the recommended privacy policies and use virtual examples to set different privacy policies for different sites. All findings were statistically analysed and found to be statistically significant. The major results of this study were that users have concerns about sharing personal information with others, especially any item that can verify the identity of the user such as mobile number, photographs and addresses. Although all users have some concerns, females were more concerned than males about sharing these items. It also showed that a high number of users used mobile web devices to browse the internet and the current privacy frameworks require more development to become suitable for use with mobile devices. Moreover, the idea of using a Smart Wizard System as a mobile tool to enhance a privacy policy for 23 personal information items was successful. It attained a high percentage of satisfaction based on the respondents' answers. Furthermore, centralising personal information details in one server was a unique idea. It allowed the user to minimise the distribution processes of his/her personal information among different websites and provided him/her with full authority to control the sharing process and apply different privacy policies on other sites. This idea simplified the registration and control of privacy settings via mobile devices to suit the expanding number of online social networking sites and the use of mobile devices for browsing these sites.

In conclusion, this study had some limitations in terms of collecting data and the sample size. One of the main shortcomings is the lack of female respondents in the first task of the study and the required time to collect data in both countries. In addition, the third part of the study also faced some limitations in collecting data. Some invitations were posted on Facebook sites and this may tend to bias the selection of privacy settings based towards the attitude of Facebook users. The results could have varied if respondents were from other social networking sites and this may encourage other studies in future to do some research in this area. Also, the second part of the third task is likely to be affected by respondent fatigue bias because they were asked to evaluate 23 items by defining their concerns about each item and the status of sharing it with others. Despite these shortcomings, the study has provided a solid basis to further privacy protection via mobile devices, as well as pointing to other opportunities for further studies to improve the wizard smart system and the whole privacy framework.

References

ABOBA, B. & CALHOUN, P. 2003. RADIUS (remote authentication dial in user service) support for extensible authentication protocol (EAP). RFC 3579, September.

ACCENTURE. 2012. *Mobile Web Watch 2012* [Online]. Accenture. Available: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Mobile-Web-Watch-Internet-Usage-Survey-2012.pdf [Accessed 4/12/2013.

ACQUISTI, A. & GROSS, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. Privacy enhancing technologies, 2006. Springer, 36-58.

ACQUISTI, A. & GROSS, R. 2009. Predicting Social Security numbers from public data. *Proceedings of the National academy of sciences,* 106**,** 10975-10980.

ADOBE. 2014. *Customer security alert* [Online]. Adobe. Available: http://helpx.adobe.com/x-productkb/policy-pricing/customer-alert.html [Accessed January 28, 2014.

ALLISON, P. D. 2000. Multiple imputation for missing data: A cautionary tale.

ALLY, M., TOLEMAN, M. & CATER-STEEL, A. Traditional and alternative internet payment systems: the merchant perspective. Proceedings of the 5th International Conference on Qualitative Research in IT & IT in Qualitative Research: The Traditions and Innovations of Qualitative Approaches in ICT Research (QualIT 2010), 2010. QualIT.

ALSALIBI, B. A., ZAKARIAH, N. & ELMADHOUN, A. M. 2013. A Study of A Privacy Recommender System Using Collaborative Filtering Among Palestinian Online Communities.

ANDERSEN, P. 2007. *What is Web 2.0?: ideas, technologies and implications for education,* JISC Bristol, UK.

ANDERSON, D. R., SWEENEY, D. J. & WILLIAMS, T. A. 2011. *Statistics for business and economics,* Cengage Learning.

ANDREWS, D., PREECE, J. & TUROFF, M. A conceptual framework for demographic groups resistant to online community interaction. System Sciences, 2001. Proceedings of the 34th Annual Hawaii International Conference on, 2001. IEEE, 10 pp.

ANDREWS, D. C. 2002. Audience-specific online community design. *Communications of the ACM,* 45**,** 64-68.

APPLE. 2013. *iPhone User Guide For iOS 7 Software* [Online]. Available: http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf [Accessed October 12, 2013].

ARDAGNA, C. A., CREMONINI, M., DE CAPITANI DI VIMERCATI, S. & SAMARATI, P. 2008. A privacy-aware access control system. *Journal of Computer Security,* 16**,** 369-397.

BABU, A. R., SINGH, Y. & SACHDEVA, R. 1997. Establishing a management information system. *BE Swanson, RP Bentz, and A. J. Sotranko.(Eds.), Improving agricultural extension (A reference manual)***,** 161-169.

BADEN, R., BENDER, A., SPRING, N., BHATTACHARJEE, B. & STARIN, D. Persona: an online social network with user-defined privacy. ACM SIGCOMM *Computer Communication Review,* 2009. ACM, 135-146.

BAE, S.-H. & KIM, J. 2010. Development of Personal Information Protection Model using a Mobile Agent. *JIPS,* 6**,** 185-196.

BAKER, D. B., BARNHART, R. M. & BUSS, T. T. PCASSO: applying and extending state-of-the-art security in the healthcare domain. *Computer Security Applications Conference,* 1997. *Proceedings.,* 13th Annual, 1997. IEEE, 251-260.

BARTHE, G., DATTA, A. & ETALLE, S. 2011. *Formal aspects of security and trust: 8th international workshop, FAST 2011 Leuven, Belgium, September 12-14, 2011: revised selected papers*, Springer Verlag.

BEACH, A., GARTRELL, M., XING, X., HAN, R., LV, Q., MISHRA, S. & SEADA, K. Fusing mobile, sensor, and social data to fully enable context-aware computing. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, 2010. ACM, 60-65.

BECK, T. 2008. *Web 2.0: user-generated content in online communities: a theoretical and empirical investigation of its determinants*, Timo Beck-Diplomica Verlag.

BEKARA, K. & LAURENT, M. Enabling user privacy in identity management systems. *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on,* 2010. IEEE, 514-520.

BELL, D. E. Looking back at the bell-la padula model. *Computer Security Applications Conference, 21st Annual*, 2005. IEEE, 15 pp.-351.

BEN ABDESSLEM, F., HENDERSON, T., BROSTOFF, S. & SASSE, M. A. 2011. Context-based Personalised Settings for Mobile Location Sharing.

BERLATSKY, N. 2013. *Cybercrime,* Greenhaven Press, A part of Gale, Cengage Learning.

BERRY, M. & SCHLESER, M. 2014. *Mobile Media Making in an Age of Smartphones,* Palgrave Macmillan.

BILLINGS, R. E. & BILLINGS, J. A. 2009. Using Hidden Secrets and Token Devices to Create Secure Volumes. Google Patents.

BINDER, J., HOWES, A. & SUTCLIFFE, A. The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 2009. ACM, 965-974.

BLANC, M., GROS, D., BRIFFAUT, J. & TOINARD, C. Mandatory access control with a multi-level reference monitor: PIGA-cluster. *Proceedings of the first workshop on Changing landscapes in HPC security,* 2013. ACM, 1-8.

BLEKAS, A., GAROFALAKIS, J. & STEFANIS, V. Use of RSS feeds for content adaptation in mobile web browsing. *Proceedings of the 2006 international cross-disciplinary workshop on Web accessibility (W4A): Building the mobile web: rediscovering accessibility?,* 2006. ACM, 79-85.

BONHARD, P. & SASSE, M. 2006. 'Knowing me, knowing you'—Using profiles and social networking to improve recommender systems. *BT Technology Journal,* 24**,** 84-98.

BOONE, H. N. & BOONE, D. A. 2012. Analyzing likert data. *Journal of Extension,* 50**,** 2TOT2.

BOLSTER, N. M., GIARDINI, M. E., LIVINGSTONE, I. A. & BASTAWROUS, A. 2014. How the smartphone is driving the eye-health imaging revolution. *Expert Review of Ophthalmology,* 9**,** 475-485.

BOUGUETTAYA, A. & ELTOWEISSY, M. 2003. Privacy on the Web: facts, challenges, and solutions. *Security & Privacy, IEEE,* 1**,** 40-49.

BOYD, A. W. 2011. A Longitudinal Study of Social Media Privacy Behavior. *arXiv preprint arXiv:1103.3174.*

BOYD, D. M. & ELLISON, N. B. 2010. Social network sites: Definition, history, and scholarship. *Engineering Management Review, IEEE,* 38**,** 16-31.

BRAKE, D. R. 2014. Are we all online content creators now? Web 2.0 and digital divides. *Journal of Computer-Mediated Communication,* 19**,** 591-609.

BRASS, D. J., BUTTERFIELD, K. D. & SKAGGS, B. C. 1998. Relationships and unethical behavior: A social network perspective. *Academy of Management Review,* 23**,** 14-31.

BROWN, J. D. 2011. Likert items and scales of measurement. *Shiken: JALT Testing & Evaluation SIG Newsletter,* 15**,** 10-14.

BROWN, P. & INSTITUTE, P. L. 2010. *Information Technology Law Institute 2010: Opportunities in Cloud Computing, Blogs, Brand Protection and Targeted Marketing*, Practising Law Institute.

BRUNS, A., HIGHFIELD, T. & BURGESS, J. 2013. The Arab Spring and Social Media Audiences English and Arabic Twitter Users and Their Networks. *American Behavioral Scientist,* 57**,** 871-898.

BRYMAN, A. & BELL, E. 2007. *Business research methods*, Oxford University Press.

BUFFINGTON, J. 2010. *Data protection for virtual data centers*, John Wiley & Sons.

BULLAS, J. 2012. *48 significant social media facts, figures and statistics plus 7 infographics* [Online]. Available: http://www.jeffbullas.com/2012/04/23/48-significant-social-media-factsfigures-and-statistics-plus-7-infographics/ [Accessed October 22, 2013

BUNNIG, C. & CAP, C. H. Ad hoc privacy management in ubiquitous computing environments. *Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2009. CENTRIC'09. Second International Conference on,* 2009. IEEE, 85-90.

BUOTE, V. M., WOOD, E. & PRATT, M. 2009. Exploring similarities and differences between online and offline friendships: The role of attachment style. *Computers in Human Behavior,* 25**,** 560-567.

BURDON, M., REID, J. & LOW, R. 2010. Encryption safe harbours and data breach notification laws. *Computer Law & Security Review,* 26**,** 520-534.

CAMPISI, P., MAIORANA, E. & NERI, A. Privacy protection in social media networks a dream that can come true? *Digital Signal Processing, 2009 16th International Conference on,* 2009. IEEE, 1-5.

CARMICHAEL, J. & SMERDON, G. 2012. Systems and methods for processing access control lists (ACLS) in network switches using regular expression matching logic. Google

Patents.

CASAROSA, F. 2010. Child Privacy Protection Online: How to Improve It through Code and Self-Regulatory Tools. *Available at SSRN 1561570.*

CAVOUKIAN, A. 2009. Privacy by design. *Take the Challenge. Information and Privacy Commissioner of Ontario, Canada*.

CHANG, H. H. & CHEN, S. W. 2008. The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator. *Computers in Human Behavior*, 24**,** 2927-2944.

CHIU, P.-Y., CHEUNG, C. M. & LEE, M. K. 2008. Online Social Networks: Why Do "We" Use Facebook? *The open knowledge society. A computer science and information systems manifesto.* Springer.

CHRISTOFIDES, E., DESMARAIS, S. & MUISE, A. 2010. *Privacy and Disclosure on Facebook: Youth and Adult's Information Disclosure and Perceptions of Privacy Risks*, University of Guelph.

CHUA, A. Y., BALKUNJE, R. S. & GOH, D. H.-L. Fulfilling mobile information needs: a study on the use of mobile phones. *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*, 2011. ACM, 92.

CHURCH, K. & OLIVER, N. Understanding mobile web and mobile search use in today's dynamic mobile landscape. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, 2011. ACM, 67-76.

CHURCH, K. & SMYTH, B. Understanding the intent behind mobile information needs. *Proceedings of the 14th international conference on Intelligent user interfaces*, 2009. ACM, 247-256.

CHURCHER, K. M., DOWNS, E. & TEWKSBURY, D. 2014. "Friending" Vygotsky: A Social Constructivist Pedagogy of Knowledge Building Through Classroom Social Media Use. *The Journal of Effective Teaching***,** 33.

COLLIS, J. & HUSSEY, R. 2009. *Business research: A practical guide for undergraduate and postgraduate students*, Palgrave Macmillan.

CONGDON, P., ABOBA, B., SMITH, A., ZORN, G. & ROESE, J. 2003. IEEE 802.1 X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. *RFC3580, September*.

CONSOLVO, S., SMITH, I. E., MATTHEWS, T., LAMARCA, A., TABERT, J. & POWLEDGE, P. Location disclosure to social relations: why, when, & what people want to share. *Proceedings of the SIGCHI conference on human factors in computing systems*, 2005. ACM, 81-90.

CORPORATION, M. 2011. *Improving Web Application Security: Threats and Countermeasures: Threats and Countermeasures* [Online]. Microsoft Press. Available: http://books.google.com.au/books?id=Cmw5sPdEL1AC [Accessed 10/11/2013.

CRAIG, T. & LUDLOFF, M. E. 2011. *Privacy and big data*, O'Reilly Media, Inc.

CRANE, D. 2013. System and methods for marketing communications and promotion automation. US Patent App. 13/743,883.

CRESWELL, J. W. & CLARK, V. L. P. 2007. *Designing and conducting mixed methods research*, Wiley Online Library.

CROTTY, M. 1998. *The foundations of social research: Meaning and perspective in the research process*, Sage.

CUI, Y. & ROTO, V. How people use the web on mobile devices. *Proceedings of the 17th international conference on World Wide Web*, 2008. ACM, 905-914.

CUTILLO, L. A., MOLVA, R. & STRUFE, T. 2009. Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE,* 47**,** 94-101.

DAHLEN, M. 2002. Learning the web: Internet user experience and response to web marketing in Sweden. *Journal of Interactive Advertising,* 3.

DAR, H. & SHAH, A. Analysis of SNs popularity from different perspectives among users. *Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on*, 2013. IEEE, 1-4.

DE AZEVEDO, R. C., DE OLIVEIRA LACERDA, R. T., ENSSLIN, L., JUNGLES, A. E. & ENSSLIN, S. R. 2012. Performance Measurement to Aid Decision Making in the Budgeting Process for Apartment-Building Construction: Case Study Using MCDA-C. *Journal of Construction Engineering and Management,* 139**,** 225-235.

DEMUYNCK, L. & DE DECKER, B. Privacy-preserving electronic health records. Communications and Multimedia Security, 2005. Springer, 150-159.

DESHMUKH, R. Interactive Remote Authentication Dial in User Service (RADIUS)

Authentication Server Model. ICWMC 2012, *The Eighth International Conference on Wireless and Mobile Communications*, 2012. 238-241.

DHAR, S. & VARSHNEY, U. 2011. Challenges and business models for mobile location-based services and advertising. *Communications of the ACM,* 54**,** 121-128.

DHONDGE, K., SONG, S., JANG, Y., PARK, H., SHIN, S. & CHOI, B.-Y. Video: WiFi-honk: smartphone-based beacon stuffed WiFi Car2X-communication system for vulnerable road user safety. Proceedings of the 12th annual international conference on Mobile systems, applications, and services, 2014. ACM, 387-387.

DILLMAN, D. A. 2011. *Mail and Internet surveys: The tailored design method--2007 Update with new Internet, visual, and mixed-mode guide,* John Wiley & Sons.

DIMICCO, J., MILLEN, D. R., GEYER, W., DUGAN, C., BROWNHOLTZ, B. & MULLER, M. Motivations for social networking at work. *Proceedings of the 2008 ACM conference on Computer supported cooperative work,* 2008. ACM, 711-720.

DINEV, T., BELLOTTO, M., HART, P., RUSSO, V., SERRA, I. & COLAUTTI, C. 2006. Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems,* 15**,** 389-402.

DING, Y. & ROSS, K. W. Technical Report: November 16, 2012.

DIOGENES, Y. & SHINDER, T. W. 2010. *Deploying Microsoft® Forefront® Protection 2010 for Exchange Server,* O'Reilly.

DÖTZER, F. Privacy issues in vehicular ad hoc networks. Privacy enhancing technologies, 2006. Springer, 197-209.

DRNASIN, I. & GRGIC, M. The use of mobile phones in radiology. ELMAR, 2010 PROCEEDINGS, 2010. IEEE, 17-21.

DROMS, R. & SCHNIZLEIN, J. 2005. Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option. *Internet Engineering Task Force, Request for Comment,* 4014**,** 1-7.

DWYER, C., HILTZ, S. R. & PASSERINI, K. Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. *AMCIS*, 2007. 339.

DWYER, C., HILTZ, S. R., POOLE, M. S., GUSSNER, J., HENNIG, F., OSSWALD, S., SCHLIESSLBERGER, S. & WARTH, B. Developing reliable measures of privacy management within social networking sites. *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010. IEEE, 1-10.

EDM. 2014. *Why Should You Have a Centralized System?* [Online]. Effictive Database Management. Available: http://www.effectivedatabase.com/why-should-you-have-a-centralized-system [Accessed 12/01 2014].

ELLISON, N. B. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer‐Mediated Communication*, 13**,** 210-230.

ELLISON, N. B., STEINFIELD, C. & LAMPE, C. 2007. The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer‐Mediated Communication*, 12**,** 1143-1168.

ENCK, W., GILBERT, P., CHUN, B.-G., COX, L. P., JUNG, J., MCDANIEL, P. & SHETH, A. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. OSDI, 2010. 255-270.

ERIKSEN, A. M. 2008. Glitch Opens Bebo Users' Private Details to Others. *The New Zealand Herald*.

ERNST, T. 2007. Network mobility support goals and requirements.

ETHERINGTON, D. 2013. Android Nears 80% Market Share In Global Smartphone Shipments, As iOS And BlackBerry Share Slides, Per IDC. *Retrieved*, 9**,** 2013.

FACEBOOK. 2009. *Facebook's Privacy Policy - 3. Information You Share With Third Parties* [Online]. Available: https://www.facebook.com/note.php?note_id=%20322336955300 [Accessed July 10, 2014.

FACEBOOK. 2013a. *News room, Key Facts, statistics,* [Online]. Facebook. Available: https://newsroom.fb.com/Key-Facts [Accessed September 12, 2013.

FACEBOOK. 2013b. Available: https://www.facebook.com [Accessed November 12, 2013.

FACEBOOK. 2013c. *How does privacy work for minors?* [Online]. Available: http://www.facebook.com/help/?page=214189648617074 [Accessed November 18, 2013.

FANG, L., KIM, H., LEFEVRE, K. & TAMI, A. A privacy recommendation wizard for users of social networking sites. *Proceedings of the 17th ACM conference on Computer and communications security*, 2010. ACM, 630-632.

FELDMAN, A. J., BLANKSTEIN, A., FREEDMAN, M. J. & FELTEN, E. W. Social networking with Frientegrity: privacy and integrity with an untrusted provider. *Proceedings of the 21st USENIX conference on Security symposium, Security*, 2012.

FELT, A. & EVANS, D. 2008. Privacy protection for social networking APIs. *2008 Web 2.0 Security and Privacy (W2SP'08)*.

FERRAIOLO, D., KUHN, D. R. & CHANDRAMOULI, R. 2007. *Role-based access control*, Artech House Boston.

FERRAIOLO, D. F. & KUHN, D. R. 2009. Role-based access controls. *arXiv preprint arXiv:0903.2171*.

FINANCE, B., MEDJDOUB, S. & PUCHERAL, P. Privacy of medical records: From law principles to practice. *Computer-Based Medical Systems, 2005. Proceedings*. 18th IEEE Symposium on, 2005. IEEE, 220-225.

FOGEL, J. & NEHMAD, E. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior,* 25**,** 153-160.

FORD, M. 2009. *Scams and Scoundrels: Protect Yourself from the Dark Side of Ebay and Paypal*

Michael Ford, United States, Elite Minds, Incorporated.

FORTE, D. 2009. Phishing in depth. *Network Security,* 2009**,** 19-20.

FUCHS, C. 2010. studiVZ: social networking in the surveillance society. *Ethics and Information Technology,* 12**,** 171-185.

FUKUYAMA, F. 1996. Trust Still Counts in a Virtual World" This disembodied organisation exists without institutions, without loyalties, without face-to-face interaction.". *Forbes,* 158**,** 33-35.

GANLEY, D. & LAMPE, C. 2009. The ties that bind: Social network principles in online communities. *Decision Support Systems,* 47**,** 266-274.

GAO, H., HU, J., HUANG, T., WANG, J. & CHEN, Y. 2011. Security issues in online social networks. *Internet Computing, IEEE,* 15**,** 56-63.

GEFEN, D., KARAHANNA, E. & STRAUB, D. W. 2003. Inexperience and experience with online stores: the importance of TAM and trust. *Engineering Management, IEEE Transactions on,* 50**,** 307-321.

GEORGE, A. 2006. Living online: The end of privacy. *New Scientist,* 2569**,** 1-50.

GHARIBI, W. & SHAABI, M. 2012. Cyber threats in social networking websites. *arXiv preprint arXiv:1202.2420*.

GIGONE, D. & HASTIE, R. 2013. The impact of information on group judgment: A model and computer simulation. *Understanding group behavior: Consensual action by small groups,* 1**,** 221-251.

GORP, P. V., COMUZZI, M., FIALHO, A. & KAYMAK, U. Addressing health information privacy with a novel cloud-based PHR system architecture. *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on,* 2012. IEEE, 1841-1846.

GRABNER-KRÄUTER, S. 2009. Web 2.0 social networks: the role of trust. *Journal of business ethics,* 90**,** 505-522.

GRABNER-KRÄUTER, S. & BITTER, S. Trust in online social networks: A multifaceted perspective. Forum for Social Economics, 2013. Taylor & Francis, 1-21.

GRIECO, L., RIZZO, A., COLUCCI, S., SICARI, S., PIRO, G., DI PAOLA, D. & BOGGIA, G. 2014. IoT-aided robotics applications: technological implications, target domains and open issues. *Computer Communications,* 54**,** 32-47.

GROSS, R. & ACQUISTI, A. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* 2005. ACM, 71-80.

GROVES, R. M., FOWLER JR, F. J., COUPER, M. P., LEPKOWSKI, J. M., SINGER, E. & TOURANGEAU, R. 2011. *Survey methodology,* John Wiley & Sons.

GUAN, Z., XIONG, H., LI, S. & CHEN, Z. Mobile Browser as a Second Factor for Web Authentication. *Parallel and Distributed Processing with Applications (ISPA), 2011 IEEE 9th International Symposium on,* 2011. IEEE, 276-281.

GUNDECHA, P., BARBIER, G. & LIU, H. Exploiting vulnerability to secure user privacy on a social networking site. *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining,* 2011. ACM, 511-519.

GUNTER, T. D. & TERRY, N. P. 2005. The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. *Journal of Medical Internet Research,* 7.

HAMEED, S., FU, X., HUI, P. & SASTRY, N. LENS: Leveraging social networking and trust to prevent spam transmission. *Network Protocols (ICNP), 2011 19th IEEE International Conference on*, 2011. IEEE, 13-18.

HARGITTAI, E. 2010. Facebook privacy settings: Who cares? *First Monday, Computer and Information Science*, (15)8, doi:10.1177/1354856507084416.

HEIMONEN, T. Information needs and practices of active mobile internet users. *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems*, 2009. ACM, 50.

HERNANDEZ, E. A. 2009. War of the mobile browsers. *Pervasive computing, IEEE,* 8**,** 82-85.

HINMAN, R., SPASOJEVIC, M. & ISOMURSU, P. They call it surfing for a reason: identifying mobile internet needs through pc internet deprivation. CHI'08 extended abstracts on Human factors in computing systems, 2008. ACM, 2195-2208.

HO, A., MAIGA, A. & AÏMEUR, E. Privacy protection issues in social networking sites. *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, 2009. IEEE, 271-278.

HODGE, M. J. 2006. Fourth Amendment and Privacy Issues on the New Internet: Facebook. com and Myspace. com, The. *S. Ill. ULJ,* 31**,** 95.

HOEPMAN, J.-H. 2014. Privacy design strategies. *ICT Systems Security and Privacy Protection.* Springer.

HOY, M. G. & MILNE, G. 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising,* 10**,** 28-45.

HU, Q. & MA, S. Does Privacy Still Matter in the Era of Web 2.0? A Qualitative Study of User Behavior towards Online Social Networking Activities. PACIS, 2010. 2.

HU, V. C., FERRAIOLO, D. & KUHN, D. R. 2006. *Assessment of access control systems,* US Department of Commerce, National Institute of Standards and Technology.

HU, X. 2011. *Social media business model analysis-Case Tencent, Facebook, and Myspace.* Master, Aalto University, Finland.

IJTIHADIE, R. M., CHISAKI, Y., USAGAWA, T., CAHYO, H. & AFFANDI, A. Offline web application and quiz synchronization for e-learning activity for mobile browser.

TENCON 2010-2010 IEEE Region 10 Conference, 2010. IEEE, 2402-2405.

JIN, X., KRISHNAN, R. & SANDHU, R. 2012. A unified attribute-based access control model covering dac, mac and rbac. *Data and Applications Security and Privacy XXVI.* Springer.

KAIKKONEN, A. Full or tailored mobile web-where and how do people browse on their mobiles? *Proceedings of the International Conference on Mobile Technology, Applications, and Systems,* 2008. ACM, 28.

KNOCHE, H., MCCARTHY, J. D. & SASSE, M. A. Can small be beautiful?: assessing image resolution requirements for mobile TV. *Proceedings of the 13th annual ACM international conference on Multimedia*, 2005. ACM, 829-838.

KOLTER, J. & PERNUL, G. Generating user-understandable privacy preferences. *Availability, Reliability and Security, 2009. ARES'09. International Conference on,* 2009. IEEE, 299-306.

KPCB. 2012. *Internet Trends* [Online]. Available: http://goo.gl/aXbVs [Accessed 14/2/2013.

KPCB. 2012. *Top Mobile Internet Trends* [Online]. Available: http://goo.gl/p8zU1 [Accessed 14/2/2013.

KRAJNC, E., KNOLL, M., FEINER, J. & TRAAR, M. 2011. A touch sensitive user interface approach on smartphones for visually impaired and blind persons. *Information Quality in e-Health.* Springer.

KRIPANONT, N. 2007. *Examining a technology acceptance model of internet usage by academics within Thai Business Schools.* Victoria University.

KULSHRESTHA, T. & KANT, A. R. 2013. Scale Development for Improving Education Quality: A Survey of Private Institutions Affiliated to UPTU. IJCSET.

LAI, L. S. & TURBAN, E. 2008. Groups formation and operations in the Web 2.0 environment and social networks. *Group Decision and Negotiation,* 17**,** 387-402.

LAMPE, C., ELLISON, N. & STEINFIELD, C. A Face (book) in the crowd: Social searching vs. social browsing. *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work,* 2006. ACM, 167-170.

LANE, N. D., MILUZZO, E., LU, H., PEEBLES, D., CHOUDHURY, T. & CAMPBELL, A. T. 2010. A survey of mobile phone sensing. *Communications Magazine, IEEE,* 48**,** 140-150.

LAVRAKAS, P. J. 2008. *Encyclopedia of survey research methods*, Sage.

LEBEK, B., UFFEN, J., NEUMANN, M., HOHLER, B. & H. BREITNER, M. 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review,* 37**,** 1049-1092.

LEE, I. 2011. *Transformations in E-Business Technologies and Commerce: Emerging Impacts*, Business Science Reference.

LEE, R., NIA, R., HSU, J., LEVITT, K. N., ROWE, J., WU, S. F. & YE, S. Design and implementation of faith, an experimental system to intercept and manipulate online social informatics. *Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on,* 2011. IEEE, 195-202.

LENHART, A. 2009. Adults and social network websites. Washington, DC: Pew Internet & American Life Project. Retrieved January 15, 2009 from http://www.pewinternet.org/pdfs/PIP_Adult_social_networking_data_memo_FINAL.pdf.

LENHART, A., PURCELL, K., SMITH, A. & ZICKUHR, K. 2010. *Social media & mobile internet use among teens and young adults*, Pew internet & American life project Washington, DC.

LEWIS, J. R. & MOSCOVITZ, M. 2009. Developing for small screens and the mobile web. *AdvancED CSS***,** 149-186.

LIN, H.-F. & LEE, G.-G. 2006. Determinants of success for online communities: an empirical study. *Behaviour & Information Technology,* 25**,** 479-488.

LIPFORD, H. R., BESMER, A. & WATSON, J. 2008. Understanding Privacy Settings in Facebook with an Audience View. *UPSEC,* 8**,** 1-8.

LIU, C., MARCHEWKA, J. T., LU, J. & YU, C.-S. 2004. Beyond concern: a privacy–trust–behavioral intention model of electronic commerce. *Information & Management,* 42**,** 127-142.

LIVINGSTONE, S., ÓLAFSSON, K. & STAKSRUD, E. 2011. Social networking, age and privacy. *London, EU Kids Online, London School of Economics*.

LO, J. Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. AMCIS, 2010. 110.

LO, J. & RIEMENSCHNEIDER, C. 2010. An Examination of Privacy Concerns and Trust

Entities in Determining Willingness to Disclose Personal Information on a Social Networking Site. paper presented to *America's Conference on Information Systems*, Lima, Peru, August 12-15, 2010.

LOCACCINO. 2013. *A User-Controllable Location-Sharing Tool* [Online]. Available: http://locaccino.org/ [Accessed December 12, 2013].

LUND, A. & LUND, M. 2013. *Cronbach's Alpha (α) using SPSS* [Online]. Lærd Statistics. Available: https://statistics.laerd.com/spss-tutorials/cronbachs-alpha-using-spss-statistics.php [Accessed 2/2 2014].

LUTZ, D. J. 2011. Bridging between SAML-Based Payment and Other Identity Federation Payment Systems. *Digital Enterprise and Information Systems.* Springer.

MADDEN, M. 2012. Privacy management on social media sites. *Pew Internet & American Life Project*, 24.

MADDEN, M. & FOX, S. 2006. Riding the waves of "Web 2.0.". *Pew Internet & American Life Project***,** 1-6.

MANDIANT. 2014. *M Trends Beyond the Breach* [Online]. Mandiant, A FireEye Company. Available: https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf [Accessed 16 - 2 - 2015].

MATSUNAGA, Y., MERINO, A. S., SUZUKI, T. & KATZ, R. H. Secure authentication system for public WLAN roaming. Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots, 2003. ACM, 113-121.

MCGOOKIN, D., BREWSTER, S. & JIANG, W. Investigating touchscreen accessibility for people with visual impairments. *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, 2008. ACM, 298-307.

MICROSOFT. 2013. *RADIUS Client* [Online]. Available: http://technet.microsoft.com/en-us/library/cc754033.aspx [Accessed October 16, 2013.

MILNE, G. R. & CULNAN, M. J. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18**,** 15-29.

MISHRA, S., CAPUTO, D. J., LEONE, G. J., KOHUN, F. G. & DRAUS, P. J. 2014. The Role Of Awareness And Communications In Information Security Management: A Health Care Information Systems Perspective. *International Journal of Management & Information*

Systems (IJMIS), 18**,** 139-148.

MISLOVE, A., MARCON, M., GUMMADI, K. P., DRUSCHEL, P. & BHATTACHARJEE, B. Measurement and analysis of online social networks. *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement,* 2007. ACM, 29-42.

MONTAGUE, D. A. 2010. *Essentials of online payment security and fraud prevention*, Wiley. com.

MUTHUKUMARAN, D., SAWANI, A., SCHIFFMAN, J., JUNG, B. M. & JAEGER, T. Measuring integrity on mobile phone systems. *Proceedings of the 13th ACM symposium on Access control models and technologies, 2008.* ACM, 155-164.

MYSPACE. 2013. Available: https://www.myspace.com [Accessed November 23, 2013.

NAHARI, H. & KRUTZ, R. L. 2011. *Web Commerce Security: Design and Development,* John Wiley & Sons.

NEHTA. July, 2008. *Privacy Blueprint for the Individual Electronic Health Record* [Online]. Australia: National E-Health Transition Authority Ltd. Available: http://www.audiology.asn.au/pdf/NEHTA_Privacy_Blueprint.pdf [Accessed 02/01 2014].

NI, Q., BERTINO, E., LOBO, J., BRODIE, C., KARAT, C.-M., KARAT, J. & TROMBETA, A. 2010. Privacy-aware role-based access control. *ACM Transactions on Information and System Security (TISSEC),* 13**,** 24.

NORRIS, C. 2010. *A Quick Start Guide to Online Selling: Sell Your Product on Ebay Amazon and Other Online Market Places*, Buy now from Kogan Page.

NOVAK, E. & LI, Q. 2012. A Survey of Security and Privacy in Online Social Networks. *College of William and Mary Computer Science Technical Report*.

NYLANDER, S., LUNDQUIST, T. & BRÄNNSTRÖM, A. At home and with computer access: why and where people use cell phones to access the internet. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2009. ACM, 1639-1642.

O'REILLY, T. 2007. What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies***,** 17.

PAINE, C., REIPS, U.-D., STIEGER, S., JOINSON, A. & BUCHANAN, T. 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, 65**,** 526-536.

PALLANT, J. 2010. *SPSS survival manual: A step by step guide to data analysis using SPSS*, McGraw-Hill International.

PANIGRAHI, S., KUNDU, A., SURAL, S. & MAJUMDAR, A. K. 2009. Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. *Information Fusion,* 10**,** 354-363.

PARK, J. & SANDHU, R. Towards usage control models: beyond traditional access control. Proceedings of the seventh ACM symposium on Access control models and technologies, 2002. ACM, 57-64.

PARK, J. & SANDHU, R. 2010. A Position Paper: A Usage Control (UCON) Model for Social Networks Privacy.

PASSANT, A., KÄRGER, P., HAUSENBLAS, M., OLMEDILLA, D., POLLERES, A. & DECKER, S. Enabling trust and privacy on the social web. *W3C workshop on the future of social networking*, 2009. 15-16.

PAVLOU, P. A. & FYGENSON, M. 2006. Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS quarterly***,** 115-143.

PENG, R., SUN, D. & TSAI, W.-T. Success factors in mobile social networking application development: case study of instagram. Proceedings of the 29th Annual ACM Symposium on Applied Computing, 2014. ACM, 1072-1079.

PLOTKIN, R. 2012. *Privacy, Security, and Cyberspace*, Facts On File, Incorporated.

POLGAR, J. & ADAMSON, G. 2013. *Web Portal Design, Implementation, Integration, and Optimization,* Igi Global.

PORTELA, I. M. & CRUZ-CUNHA, M. M. 2010. *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*, Information Science Reference.

Profile Engine. 2014. Available: https://www.profileengine.com [Accessed July 10, 2014.

RAMGOVIND, S., ELOFF, M. M. & SMITH, E. The management of security in cloud computing. *Information Security for South Africa* (ISSA), 2010, 2010. IEEE, 1-7.

PRUNEL, D., LEES PERASSO, E., ROY, A. & MOULIN, C. Environmental labelling of mobile phones: LCA standardisation process. ICT for Sustainability 2014 (ICT4S-14), 2014. Atlantis Press.

RAY, P. & WIMALASIRI, J. The need for technical solutions for maintaining the privacy of ehr. Engineering in Medicine and Biology Society, 2006. EMBS'06. *28th Annual International Conference of the IEEE*, 2006. IEEE, 4686-4689.

REPS, T. W. & RALL, L. B. 2003. Computational divided differencing and divided-difference arithmetics. *Higher-order and symbolic computation*, 16**,** 93-149.

RIZVI, S., MENDELZON, A., SUDARSHAN, S. & ROY, P. Extending query rewriting techniques for fine-grained access control. *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, 2004. ACM, 551-562.

ROSENBLUM, D. 2007. What anyone can know: The privacy risks of social networking sites. *Security & Privacy, IEEE,* 5**,** 40-49.

ROSS, J. I. 2009. *Cybercrime,* Chelsea House Publishers.

RUTSAERT, P., PIENIAK, Z., REGAN, Á., MCCONNON, Á., KUTTSCHREUTER, M., LORES, M., LOZANO, N., GUZZON, A., SANTARE, D. & VERBEKE, W. 2014. Social media as a useful tool in food risk and benefit communication? A strategic orientation approach. *Food Policy,* 46**,** 84-93.

SADEH, N., HONG, J., CRANOR, L., FETTE, I., KELLEY, P., PRABAKER, M. & RAO, J. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing,* 13**,** 401-412.

SAMARATI, P. & DE VIMERCATI, S. C. 2001. Access control: Policies, models, and mechanisms. *Foundations of Security Analysis and Design.* Springer.

SAMAVI, R. & CONSENS, M. P. Towards Smart Privacy on the Personal Web. Proc. of the *First Symp. on the Personal Web, Co-located with CASCO*, 2010.

SANDEEP, S. & JEFFREY, S. 2001. Acquisition of outside portfolio management services. *Journal of Pension Planning & Compliance,* 27**,** 40.

SANDHU, R. S. & SAMARATI, P. 1994. Access control: principle and practice. *Communications Magazine, IEEE,* 32**,** 40-48.

SAVAGE, M. 2012. *The PayPal Official Insider Guide to Internet Security: Spot Scams and Protect Your Online Business*, Peachpit Press.

SCHAFER, J. B., FRANKOWSKI, D., HERLOCKER, J. & SEN, S. 2007. Collaborative filtering recommender systems. *The adaptive web.* Springer.

SCHMIEDL, G., SEIDL, M. & TEMPER, K. Mobile phone web browsing: a study on usage and usability of the mobile web. *Proceedings of the 11th international Conference on Human-Computer interaction with Mobile Devices and Services*, 2009. ACM, 70.

SCHOORMAN, F. D., MAYER, R. C. & DAVIS, J. H. 2007. An integrative model of organizational trust: Past, present, and future. *Academy of Management Review,* 32**,** 344-354.

SEALE, C. 1999. Quality in qualitative research. *Qualitative inquiry,* 5**,** 465-478.

SEKARAN, U. 2006. *Research methods for business: A skill building approach,* Wiley. com.

SETH, K. 2009. *Cyber Laws in the Information Technology Age*, LexisNexis Butterworths Wadhwa Nagpur.

SHADLOU, S., KAI, N. J. & HAJMOOSAEI, A. 2011. Online Payment via PayPal API Case Study Event Registration Management System (ERMS). *International Journal of Web Portals (IJWP),* 3**,** 30-37.

SHEHAB, M. & TOUATI, H. Semi-Supervised Policy Recommendation for Online Social Networks. *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012),* 2012. IEEE Computer Society, 360-367.

SHIN, D.-H. 2010. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers,* 22**,** 428-438.

SOHN, T., LI, K. A., GRISWOLD, W. G. & HOLLAN, J. D. A diary study of mobile information needs. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008. ACM, 433-442.

SOLMS, S. V. & SOLMS, R. V. 2008. *Information security governance,* Springer Publishing Company, Incorporated.

SON, J.-Y. & KIM, S. S. 2008. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS quarterly,* 32**,** 503-529.

STAKSRUD, E. & LOBE, B. 2010. Evaluation of the implementation of the safer social networking principles for the EU Part I: general report.

STAMP, M. 2011. *Information security: principles and practice*, John Wiley & Sons.

STATISTICS, S. G. 2013. *Mobile vs. Desktop for 2013* [Online]. StatCounter Available: http://gs.statcounter.com/#mobile_vs_desktop-ww-monthly-201001-201304 [Accessed

4/12/2013.

STEINFIELD, C., ELLISON, N. B. & LAMPE, C. 2008. Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology,* 29**,** 434-445.

STUTZMAN, F. & KRAMER-DUFFIELD, J. Friends only: examining a privacy-enhancing behavior in Facebook. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 2010. ACM, 1553-1562.

SUHENDRA, V. 2011. A survey on access control deployment. *Security Technology.* Springer.

SZILAGYI, D., SOOD, A. & SINGH, T. 2009. RADIUS: A REMOTE AUTHENTICATION DIAL-IN USER SERVICE.

TANG, Q., GU, B. & WHINSTON, A. B. 2012. Content contribution for revenue sharing and reputation in social media: A dynamic structural model. *Journal of Management Information Systems,* 29**,** 41-76.

TAHERI, S., HARTUNG, S. & HOGREFE, D. Achieving receiver location privacy in mobile ad hoc networks. *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, 2010. IEEE, 800-807.

THAMPI, S. M., ZOMAYA, A. Y., STRUFE, T., CALERO, J. M. A. & THOMAS, T. 2012. *Recent Trends in Computer Networks and Distributed Systems Security: International Conference, Snds 2012, Trivandrum, India, October 11-12, 2012, Proceedings*, Springer London, Limited.

THELWALL, M. 2009. Social network sites: users and uses. *Advances in computers,* 76**,** 19-73.

TIMM, D. M. & DUVEN, C. J. 2008. Privacy and social networking sites. *New directions for student services,* 2008**,** 89-101.

TOCH, E., CRANSHAW, J., HANKES-DRIELSMA, P., SPRINGFIELD, J., KELLEY, P. G., CRANOR, L., HONG, J. & SADEH, N. Locaccino: a privacy-centric location sharing application. *Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing-Adjunct*, 2010. ACM, 381-382.

TOCH, E., SADEH, N. M. & HONG, J. Generating default privacy policies for online social networks. *CHI'10 Extended Abstracts on Human Factors in Computing Systems*, 2010.

ACM, 4243-4248.

TOMEI, L. A. 2011. *Advancing Education with Information Communication Technologies: Facilitating New Trends,* Igi Global.

TOWLE, H. K. 2009. Tenth Annual Institute on Privacy and Data Security Law. San Francisco, CA: Practising Law Institute.

TRAYNOR, A. 2014. SOCIAL MEDIA POLICY. *Policy,* 29**,** 05.

USC. 2013. *The 2013 Digital Future Report, Surveying The Digital Future, Year Eleven* [Online]. USC (University of Southern California) Annenberg School Center for the Digital Future Available: http://www.digitalcenter.org/wp-content/uploads/2013/06/2013-Report.pdf [Accessed November 25, 2013.

VAISHNAVI, V. & KUECHLER, W. 2004. Design research in information systems.

VALENZUELA, S., PARK, N. & KEE, K. F. 2009. Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, and Participation1. *Journal of Computer‐Mediated Communication,* 14**,** 875-901.

VAUGHAN-NICHOLS, S. J. 2008. The mobile web comes of age. *Computer,* 41**,** 15-17.

VEAL, A. J. 2005. *Business research methods: A managerial approach,* Pearson Education Australia/Addison Wesley.

WANG, W. & CUI, C. Achieving configural location privacy in location based routing for MANET. *Military Communications Conference, 2008. MILCOM 2008*. IEEE, 2008. IEEE, 1-7.

WANT, R. 2009. When cell phones become computers. *Pervasive computing, IEEE,* 8**,** 2-5.

WEBSENSE. 2013. *Using RADIUS Agent for Transparent User Identification* [Online]. Websense. Available: http://www.websense.com/content/support/library/web/v77/radius_agent/radius_agent.pdf [Accessed Sep 19, 2013.

WHITMAN, M. E., MATTORD, H. J. & GREEN, A. 2011. *Guide to Firewalls and VPNs, 3rd Ed,* Course Technology, Cengage Learning.

WILLIAMS, K., BOYD, A., DENSTEN, S., CHIN, R., DIAMOND, D. & MORGENTHALER, C. 2009. Social Networking Privacy Behaviors and Risks. *Seidenberg School of CSIS, Pace University, USA.*

WILSON, S., CRANSHAW, J., SADEH, N., ACQUISTI, A., CRANOR, L. F., SPRINGFIELD, J., JEONG, S. Y. & BALASUBRAMANIAN, A. Privacy manipulation and acclimation in a location sharing application. *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing,* 2013. ACM, 549-558.

WU, L. & ACKLAND, R. 2014. How Web 1.0 fails: the mismatch between hyperlinks and clickstreams. *Social Network Analysis and Mining,* 4**,** 1-7.

WU, X., ZHU, X., WU, G.-Q. & DING, W. 2014. Data mining with big data. *Knowledge and Data Engineering, IEEE Transactions on,* 26**,** 97-107.

XIANG, Z., MAGNINI, V. P. & FESENMAIER, D. R. 2015. Information technology and consumer behavior in travel and tourism: Insights from travel planning using the internet. *Journal of Retailing and Consumer Services,* 22**,** 244-249.

XU, H. 2009. Consumer responses to the introduction of privacy protection measures: an exploratory research framework. *International Journal of E-Business Research (IJEBR),* 5**,** 21-47.

YUAN, M., CHEN, L. & YU, P. S. 2010. Personalized privacy protection in social networks. *Proceedings of the VLDB Endowment,* 4**,** 141-150.

ZHANG, R. 2009. Combining public key encryption with keyword search and public key encryption. *IEICE transactions on information and systems,* 92**,** 888-896.

ZIKMUND, W. G., CARR, J. C. & GRIFFIN, M. 2012. *Business research methods,* CengageBrain. com.

ZUKOWSKI, T. & BROWN, I. Examining the influence of demographic factors on internet users' information privacy concerns. *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries,* 2007. ACM, 197-204.