Information Disclosure and Generational Differences in Social Network Sites

Laurence Brooks
Information Systems and Computing, Brunel University, London, Middlesex, United Kingdom., laurence.brooks@dmu.ac.uk

Valentine Anene
Brunel University, London, United Kingdom., valentine.anene@brunel.ac.uk

Follow this and additional works at: http://aisel.aisnet.org/amcis2012

Recommended Citation
http://aisel.aisnet.org/amcis2012/proceedings/SocialIssues/10

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Information Disclosure and Generational Differences in Social Network Sites

Laurence Brooks  
Brunel University, UK  
laurence.brooks@brunel.ac.uk

Valentine Anene  
Brunel University, UK  
valentine.anene@brunel.ac.uk

ABSTRACT

Despite recent media reports regarding the negative consequences of disclosing information on social network sites (SNSs), young adults are generally thought to be unconcerned about the potential costs of this. Given the widespread use and potential dangers associated with online communication, an understanding of SNSs features and how people are using these sites is critical to educating users about protecting their information and themselves. This study compares attitudes of 18-24 with 40+ year olds, to identify differences in privacy concerns. The study finds that the picture is more nuanced than usually portrayed, with remarkable similarities between the two groups with regards to privacy concerns and user attraction to SNSs. The 40+ age group are more knowledgeable about privacy in general (offline and online), so lack of knowledge rather than lack of concern regarding privacy may be a reason why the 18-24 group act in Facebook in a seemingly unconcerned manner.

Keywords

Social networks, information disclosure, generational differences

INTRODUCTION

Social network sites (SNSs) are one of the most remarkable technological phenomena of the 21st century (Hogben, 2007) and are changing the nature of social relationships (Boyd & Ellison, 2008). However, the growing popularity of SNSs has been overshadowed by the privacy problems they pose (Krasnova et al., 2010). Specific privacy concerns include inadvertent disclosure of personal information, damaged reputation due to rumors and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft (Boyd & Ellison, 2008). Despite these threats, people continue to reveal massive amounts of personal information on SNSs (Acquisti and Gross, 2006). Given the obvious potential for abuse, it would appear that the benefits outweigh the potential costs, for most SNSs users. In addition, there are assumptions that all users of SNS behave similarly (at the grand scale), in terms of attitudes and strategies. However, this is a very crude approach, and ideas about generations, and how the different generations within society behave differently (with respect to computer based technology) is becoming more acceptable (Tapscott, 2009). In addition, there appears to be a phenomenal growth rate in ‘mature’ users engaging with SNS, such as Facebook which has seen growth of over 275% for 35-54 year olds (compared with only 20% for 18-24 year olds) for US participants alone (Corbett, 2009). A Pew Research Center’s Internet & American Life Project report on how older adults and social media agrees, reporting ‘Social networking use among internet users ages 50 and older has nearly doubled—from 22% to 42% over the past year’ (Madden, 2010).

However, with the rise in identity fraud and concerns over privacy and bullying (Brenner, 2010), there are questions over whether online communities are able to sufficiently protect themselves (Fried, 2001). This study aims to investigate what influences how 18-24 and 40+ years old disclose and control information on Facebook, to see what generational patterns there are. These can then be used to explore the implications for education and development of further social networking tools.

LITERATURE REVIEW AND BACKGROUND TO SOCIAL NETWORK SITES (SNS)

The development of the Internet means that individuals are changing the ways they communicate and socialize. Previously people relied heavily on postal letters/telegrams for long distance communications; these were replaced with telephone and email. Currently SNSs seem to have replaced these as a preferred means of communications, especially among 18 to 40 year olds, who are more likely than any other age group to have a SNS profile and engage in high levels of use (Peluchette & Karl, 2008; eMarketer.com, 2010; Alexa.com, 2010).
Online SNSs enable people to communicate and interact with each other through the use of Information and Communication Technologies (ICTs), particularly the Internet. Face to face interactions which are typical of traditional social networks (physical communities) have now been replaced with online relationships which are mediated by computer networks (Ahn et al., 2007). SNSs utilize and build upon the strengths and benefits of traditional social networks. With the absence of physical boundaries, SNS enable members to share information irrespective of their geographical/ physical locations (Lea et al, 2006). The benefits of SNSs come through building stronger personal connections with offline friends as well as through meeting and building relationships that are purely virtual (Gangadhаратла, 2008). The most important benefit of online networks is probably the social capital resulting from creating and maintaining interpersonal relationships and friendship (Ellison et al, 2007).

SNSs can be said to generally serve three main purposes – connection, collaboration and communication. Facebook, a social communication tool, designed to allow members to contact and communicate with other Facebook users, has grown from 350 million users in 2009 to 500 million users in July 2010 (www.Facebook.com; alexa.com). This phenomenal growth has made Facebook the fastest growing online community and the second most visited site worldwide, (Alexa.com, 2010). Although the popularity of SNSs have greatly improved the way people communicate with each other, there are some unanticipated side effects. As a pervasive technology, SNSs tend to deeply penetrate their users’ everyday life and become invisible, ubiquitous, and taken for granted once they are adopted (Debatin et al., 2009). Specific privacy concerns include inadvertent disclosure of personal information, damaged reputation due to rumors, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, hacking and identity theft (Boyd & Ellison, 2008).

There have been a number of high profile breaches of privacy reported in the media. In July 2009 the wife of the British MI6 Chief, Lady (Mrs) Sawers disclosed personal details about their life, including the whereabouts of their children, their parents, the location of their London flat, and their friendship with senior diplomats, simply because she had not imposed any privacy protection on her Facebook account (BBC News, 2009). In July 2010, Ron Bowles an online security consultant, published personal details of more than a fifth of Facebook’s estimated 500 million users to the internet in order to highlight its “terrifying” privacy fears (Emery, 2010).

But what is privacy? An adequate privacy theory would help to distinguish between the conditions of privacy (i.e., what is required to have privacy) and a right to privacy, and between a loss of privacy and a violation of privacy.

Privacy theories

Privacy is a complex concept and it is difficult to get a consensual definition of what constitutes privacy, possibly because attitudes to privacy are culturally determined (Milberg et al., 1995). Nevertheless, many definitions of privacy share a common core: control over transactions (interactions, communications) that regulate access to self and that, as a consequence, reduce vulnerability and increase decisional and behavioral options.

The control theory of privacy says that privacy is not simply an absence of information about a person in the minds of others, but the control that a person has over information about themselves (Fried 1968). This recognizes the choice aspect that an individual has by being able to grant, or deny, individuals access to information about oneself. A person has privacy if and only if s/he has control over information about self. A major criticism is the assumption that a person is able to have complete control over every piece of information about oneself. This is not possible as the prospect of someone disclosing all of their personal information and still somehow retaining personal privacy, merely because s/he retains control over whether to reveal that information, is counter to the way we ordinarily view privacy (Tavani, 1999). Molony & Bannister (2009) suggest that Fried’s view of privacy is somewhat incomplete, in that privacy can be interpreted as the control that a person has over information about themselves that they wish to keep from others.

Privacy can be seen as more complex, in which information is authorized to flow to specific people, at specific times (Moor, 1997). In a highly computerized culture, it is not possible to control all personal information that resides on computer systems around the world. Therefore, the best way to protect privacy is to make sure that the right people have access to relevant information at the right time. This view of privacy, unlike control theory, recognizes the importance of setting up contexts or zones of privacy (Tavani, 1999). One problem is that it tends to ignore that someone who has privacy can choose to grant as well as to limit/deny others access to information about oneself.

Information Boundary Theory (IBT) posits that individuals form a physical or virtual informational space around them with clearly defined boundaries. Depending on the situational and personal conditions, an attempt by an external entity to penetrate these boundaries may be perceived by the individual as an intrusion. The motivation to reveal or withhold information is governed by “boundary opening” and “boundary closure” rules (Petronio 2002). These rules involve dynamic
psychological processes that are affected by the nature of the relationship, the expected use of the disclosed information, and the benefits of disclosing the information (Petronio 2002). Thus, the rules emerge from an individual’s articulation of a personal “calculus” of boundary negotiation which is influenced by the conditions in which disclosure is deemed acceptable or unacceptable.

**IBT concepts in information privacy imply:**

1. Each individual constructs a personal informational space with their own defined boundaries.
2. The information space boundary depends on the nature of the information and the individual’s own personality and environmental characteristics.
3. When the individual detects a request for information disclosure, they initiate a calculus process. The risks of disclosure are evaluated, along with estimation of how much control the individual has over the disclosed information.

Based on the outcome of risk-control assessment, the individual deems the disclosure as acceptable or unacceptable. If the disclosure is acceptable, the individual is not likely to perceive privacy intrusion and so a boundary opening follows and personal information is revealed. Where the disclosure is evaluated as unacceptable, the individual perceives this as privacy intrusion, which may give rise to privacy concerns and boundary closing may follow and the information withheld (Xu et al., 2008).

**Factors influencing information disclosure**

Despite the potential risks identified, SNSs users still continue to disclose a huge amount of personal information. Some factors that drive this disclosure in SNSs include (Tufekci 2008; Gross & Acquisti, 2005; Dwyer et al., 2007; Stutzman 2006):

- **Signaling** - the perceived benefit of selectively disclosing information to strangers may appear larger than the perceived costs of possible privacy invasions. SNSs are extremely popular and provide a high level of gratification. Studies have found that users continually negotiate and manage the tension between perceived privacy risks and expected benefits (Tufekci, 2008).
- **Peer pressure and herding behavior** – users can identify themselves as being part of something; a trend or a larger community.
- **Identity management**: the asynchronous form of communication in Facebook is conducive to impression management and offers a highly controlled environment for self-presentational behavior where users can carve out a particular persona which could be different from their real lives (Boyd, 2008; Krasnova et al., 2010).
- **Relaxed attitudes towards (or lack of interest in) personal privacy.**
- **Ignorance about the possible privacy implications of information disclosure.**
- **Convenience of maintaining relationships** (Ellison et al., 2007).
- **Faith in the networking service or trust in its members.** Moloney and Bannister, (2009), argue that the degree of trust individuals have in a third party affects their perception of the level of risk involved in any transaction with that third party, i.e. trust enables the individual to feel more in control of a situation when the risks of the situation are unknown.

Given the vast amount of information that can be shared and the number of users, concerns regarding security and privacy issues are a recurring issue (Acoca, 2008). Although some of these concerns have surfaced in the popular media, there is little empirical investigation documenting how much users differ in the information disclosed in their profiles to provide clues as to who is most likely to be at risk.

**RESEARCH METHODOLOGY**

This study adopts a qualitative research approach to provide richer information on user’ preferences, since it does not seek to prove or disprove a hypothesis, rather it seeks to identify, explore and explain how people perceive their world, both individually and collectively in groups and to try to understand the phenomena through the meanings and values that people assign to them (Oates, 2006). The core focus of this study is on understanding people’s behavior with regards to how they
disclose personal information and the privacy concerns therein. Using qualitative research the authors aim to gain insight into people's attitudes, behaviors, concerns, motivations, culture or lifestyles with regards to SNS usage.

Primary data for this research was collected through an online qualitative survey. Pilot testing was carried out with a small set of respondents in a trial run. Feedback was received via email and suggestions were incorporated into the final version of the survey. The survey was open to respondents for 9 weeks. Content analysis will be used to systematically and objectively comb the data, identifying the number of times something occurs in a set of documents and assigning codes (Oates, 2006). Content analysis is especially useful for tabulating the results of open-ended survey questions and multiple interviews, thus enabling synthesis of the answers. It can also be used to examine differences between groups on issues of interest. Tabulating the results classified the data, reducing it into manageable categories of information that are clear to understand.

The survey was open to anyone over 18 and a member of Facebook and/or another SNS. The respondents were recruited through a variety of methods, including creation of an open Facebook group with links to the online survey; emailing requests and posting physical copies of the survey to personal contacts. In all cases, respondents were notified of the scope of the survey in the invitation containing the survey address (link) and were required to indicate their consent and understanding of what their participation involved. In total 76 respondents completed the survey (59 online, 15 the electronic document, and 2 the paper version). While not enough to prove any conclusions, it is sufficient to give some indicators of the privacy attitudes of the two age groups (while it might be better to have a wider range of age groups, in a study of this scale there are limited resources and so these two age groups are chosen as representative of differing generations that could be accessed).

RESEARCH FINDINGS AND RESULTS

This section presents the qualitative survey findings, not as a statistical analysis, but as a way to identify the major themes. The results are grouped and tabulated in order to segment the text for content analysis.

<table>
<thead>
<tr>
<th>Age</th>
<th>18-24</th>
<th>40+</th>
<th>Overall %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>20</td>
<td>22</td>
<td>55.3%</td>
</tr>
<tr>
<td>Female</td>
<td>21</td>
<td>13</td>
<td>44.7%</td>
</tr>
<tr>
<td>Overall (no. of respondents)</td>
<td>41</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Overall (% of respondents)</td>
<td>53.9%</td>
<td>46.1%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 1: Demographic Data

<table>
<thead>
<tr>
<th>Age</th>
<th>18-24</th>
<th>40+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why did you choose to join SNS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To socialize with friends</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>To connect with old friends</td>
<td>88.5%</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td>17.1%</td>
<td></td>
</tr>
<tr>
<td>What do you use SNS for?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To socialize with friends</td>
<td>90.25%</td>
<td></td>
</tr>
<tr>
<td>To connect with old friends</td>
<td>88.5%</td>
<td></td>
</tr>
<tr>
<td>Dating</td>
<td>9.75%</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td>17.1%</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: User Attraction to Facebook (Reason for Joining Facebook)

All 18-24 year olds respondents said they chose to join the SNS “to socialize with friends”; further most 18-24 year olds use the SNS “to connect with friends”, with about 10% respondents also choosing “dating”. For 40+ the reason for joining a SNS was slightly different with most choosing “to connect with old friends” and/or “to network”; 17.1% use Facebook for business and networking. The findings would appear to suggest that the 40+ group use SNS mainly to maintain or re-establish existing offline networks and for semi-official purposes; whereas the 18-24 year olds seem to use SNS as a means for establishing new contacts, many of whom remain just virtual friends.
Interestingly, a reasonable high percentage of both age groups thought that Facebook is an efficient and effective means of communication with their friends and that they would have less contacts with their friends if they didn’t have a Facebook profile (Figure 3b). However, a strong difference is found in the perceived importance of Facebook, with over 60% of the 40+ responding that Facebook does not play a very importance role in their lives (Figure 3a). This is contrary to expectations that people use Facebook mainly for online social interactions, this result suggests that Facebook is fast becoming a communication tool of choice among both sets of ages.
Figure 4 shows that about 90% 18-24 year olds respondents had more than 160 friends (one having 736 friends), compared to over 71% 40+ having less than 50 Facebook friends. This result was expected since 18-24 year olds are more likely to engage in severe Facebook usage, and also use Facebook to actively seek for new relationships.

On a typical day, how many times do you visit your Facebook profile?

The majority of 40+ users their Facebook profiles 1-3 times daily (Table 5). This differs from the 18-24 group whose frequency of usage ranges from low (1-3 times daily) to high (5-7 times daily). Of these, about 36% stayed 24 hours at every visit. This could be those people with smartphones who are constantly connected to their Facebook profile. This result shows a strong difference in usage and time spent on Facebook between the age groups. It would appear that the more friends a user has, the more they log on to their profile and stay longer at every visit.

Respondents were asked which of the following they include on their Facebook profile in order to see how personal information are disclosed and managed by users.
This study finds that over 90% of both age groups include their real names and self-pictures in their Facebook profile, whereas 0% of both age groups also include their addresses and phone numbers (Figure 6). This similarity would suggest that there is some information users are not willing to readily divulge. Users seem to have a “ranking” of information that is more personal to them and therefore they are reluctant to include it in their Facebook profile. There is also a strong difference between the age groups about email addresses, with over 77% of the 40+ group including their email address on Facebook. In addition, over 97% of 18-24 year olds include information about their interests, compared to about 37% of the 40+. When asked if they wrote on other people’s profile pages, 100% 18-24 year olds responded yes and 85.7% of over 40s responded yes.

Figure 6: Identifiable personal information on Facebook

Figure 7 displays strong differences between the two age groups and third party application usage. Respondents were asked if they tag pictures of themselves and others. 95.1% of 18 -24 year olds said yes, whereas only 11.4% of 40+ respondents said yes. When asked if they used Facebook applications, 100% of 18 -24 year olds said yes, whereas only 5.7% 40+ respondents agreed.

Figure 7: Third party applications
How would you feel, if you learned that your SNS could pass your information to third parties without your permission?

Figure 8: Third Party Concern

Figure 8 shows that both groups are concerned about their information being passed on to third parties without their consent, yet Figure 7 above shows that 95.1% and 100% of 18-24 year olds tag photos and use Facebook applications respectively.

Facebook privacy concerns/perceptions

100% of both age groups are aware of the privacy settings on their profile and know how to change their Facebook privacy settings.

Are you concerned about who can view your profile?

Figure 9: Individual privacy concern

Figure 9 shows that over 80% of both groups are not very concerned about who can view their profile. This contrasts with Figure 6, where 82.5% of 18-24 year olds are not happy for family members to view certain information on their profile. This could be attributed to the overall feelings about privacy for this age group, which believe that their privacy isn’t being eroded (21.9%), or concerned about any loss (41.4%) (see Figure 10). This result could be attributed to the perceived benefit of SNSs usage outweighing any privacy concerns for this age group. By contrast 97.1% of 40+ are very concerned about data loss and 80% are bothered about privacy loss.
Which best describes your overall feelings about privacy?

![Figure 10: Feelings about Privacy](image)

Respondents were asked what concerns them the most about using Facebook (Figure 11). This was an open-ended question that ascertained the cost users’ associate with disclosure. Answers ranged from stalking, identity theft, information getting into the wrong hands, government snooping. The findings suggest that overall respondents are concerned about the cost of using Facebook.

What concerns you the most about using Facebook?

![Figure 11: Facebook Usage Concerns](image)

In your opinion, who has the most important role in protecting your online privacy?

![Figure 12: Online Privacy Responsibility](image)

58.5% of 18-24 year olds believe that the online websites have the most important role in protecting their online privacy. In contrast over 94% of 40+ believe that the individual is responsible for protecting their online privacy (Figure 12).
It is important to me to protect my identity information
I am concerned with the consequences of sharing identity information
I am likely to share my identity information online in the future
I believe my identity information is well-protected online

Figure 13: Information Sharing

Over 97% of both age groups believe that it is important for them to protect their online identity information and 73.1% and 100% respectively are concerned about the consequences of sharing their identity information (Figure 13). However, 78% of 18-24 year olds are likely to share their identity information in the future against 28.57% of 40+. One explanation for this could be that users of both age groups do engage in privacy calculus; however the benefit of sharing information outweighs the cost for the 18-24 year olds.

DISCUSSION

Information disclosure on Facebook

Involuntary Information Disclosure on Facebook

Even though users think they can control access to self, the findings show strong differences in the way 18-24 year olds and 40+ use Facebook third party applications. The literature suggests some third party applications access personal information that are unnecessary to deliver the application (Felt & Evans, 2008, cited in Hoy and Milne, 2010). However, 18-24 year olds continue to use these applications, due to the trust this age group have in Facebook or because of the perceived benefits of using the applications outweigh the potential costs of information disclosure.

Perceived Benefit of Information Disclosure on Facebook

As expected, this study finds that the convenience of maintaining relationship is an important factor in self disclosure, especially among the 18-24 year olds. Convenience arises from the SNS design which places users “one click away” from each other. Interestingly both age groups thought that Facebook is an efficient and effective means of communication with friends. Contrary to expectations that most people use Facebook mainly for online social interactions, this suggests that Facebook is fast becoming a communication tool of choice among different age groups.

According to interpersonal theories, an intention to develop new friendships is often tightly connected to information disclosure (Gibbs et al., 2006). The result shows that the 40+ use SNS tend to maintain and/or re-establish existing offline network and for semi-official (networking and business) purposes; whereas the 18-24 year olds use SNS as a means for establishing new contacts, many of whom remain just virtual friends. Therefore it is not a surprise that the 18-24 year olds, in seeking to develop new friendship, might see the benefits outweigh the cost of disclosing personal information.
**Perceived trust on Facebook**

**Trust in SNSs**

Users’ trust in the SNS provider reduces their perceived privacy risk of disclosing on Facebook. Surprisingly, 58.5% of 18-24 year olds believe that the online websites have the most important role in protecting their online privacy. Facebook allows granular individual privacy settings, which gives the users the impression of being in charge of their information, which is a pre-condition to mitigate privacy risks and improve trust (Culnan and Armstrong, 1999, cited in Krasnova et al., 2010).

**Perceived control**

Even though trust can be an important means of risk reduction, it does not allow users control over the behavior of others. The concern about relinquishing control over personal information is evident in both theory and practice, which indicates that individuals need to feel in control of their privacy at all times. Further, it is clear that individuals’ privacy concerns are based on both real risks, such as identity theft, stalking, etc. and a personal desire for privacy, even where no real risks exist. This study finds that over 82% of both age groups are concerned about who can view their Facebook profile. Trust enables the individual to feel more in control of a situation when the risks of the situation are unknown. Essentially, the degree of trust that individuals have in a third party affects their perception of the level of risk involved in any transaction with that third party.

**Privacy concerns with Facebook**

As expected, both age groups were concerned about the cost side of information revelation. Concerns ranged from stalking, identity theft, information getting into the wrong hands, government snooping. However it was not obvious if these concerns discouraged users from revealing personal information or if they actually engaged in any privacy calculus before disclosing it. One explanation for this could be mitigating factors, which reduce users’ perception of risk with regard to information disclosure: perceived control and trust in Facebook. Thus, functional features, such as privacy settings and clear information on privacy-related procedures may be significant means of reducing the privacy risk. Furthermore, results show that the feeling of being in control enhances the user trust in Facebook. By providing the right spectrum of functional controls SNSs providers have a means to ensure users’ trust in the network provider and indirectly encourage communication. In a similar fashion, available control options, such as the ability to limit one’s profile or report other users, give users the feeling of being protected and therefore increase trust within the users.

**Attitude to privacy**

IBT posits that each individual forms a physical or virtual informational space around them with clearly defined boundaries. This study finds that no users of both age groups include their phone numbers or house addresses on their Facebook profile. This suggests that in setting up their profile users do engage in privacy calculus and tend to only include information they are happy for other to see. Users tend to set personal information boundaries, where certain information are in the highest categories, which users are not willing to readily divulge to others. Users are finding a balance between the total amount of information they disclose and the amount of information they need to disclose in order to have a successful and meaningful SNSs experience.

Surprisingly, and contrary to media portrayal of 18-24 year olds not being concerned about their online privacy, the study finds that expressed attitudes towards privacy are nearly the same for the two age groups. However the study also finds that higher number of 18-24 year olds believe that the SNS has the responsibility to protect their privacy. So lack of knowledge rather than lack of concern regarding privacy may be a reason why the 18-24 year olds engage in Facebook in a seemingly unconcerned manner.

**CONCLUSION**

The aim for this study was to investigate the factors that influence how specific age groups, 18-24 year and 40+ disclose and control of information on Facebook, in order to see if there are any generational differences in disclosure (due to the limited survey set, the outcomes are seen as indicative rather than conclusive). The study finds that even though the respondents think they have control over their Facebook personal information, some of their online behaviors betray their efforts to protect their identity.
IBT deals with privacy as an interpersonal boundary regulation process and this study finds that in the context of Facebook, combinations of some aspects of the various privacy theories are required for users to maintain sufficient privacy in the disclosure and control of personal information. However they do not sufficiently cover online privacy concerns as users’ information can be disclosed by third parties (applications and users) and or users’ own friends. Regarding personal information disclosure and management on Facebook, what is common is that people would like personal information to be known by a small circle of close friends, families, and not by strangers. Although in some cases, people are willing to reveal particular personal information to anonymous strangers, but not to those who know them better. In either case, users’ information disclosure can be helpful to other users, companies and third parties. Particularly, private information is very valuable as the information of many people gathered on SNSs provides source

Contrary to the cliché that young people do not care about privacy, this study finds that younger people do care about privacy. It appears that both age groups share a lot of similarities with regards to privacy concerns. The difference however, arises in the higher number of 18-24 who believe that the SNS has the responsibility to protect their privacy, compared to those 40+ who believe that the individual is responsible for protecting their online privacy. Also a higher number of 18-24 use Facebook applications and tag pictures of themselves and friends. This may be because the older age group are more knowledgeable about privacy in general (offline and online), so a lack of knowledge rather than lack of concern regarding privacy may be the reason why the 18-24 engage in Facebook in a seemingly unconcerned manner.

REFERENCES