ASEAN users’ privacy concerns and security in using online social networks

Narumon Sriratanaviriyakul*, Mathews Nkhoma, Anna Lyza Felipe and Thanh Kim Cao

RMIT University Vietnam,
702 Nguyen Van Linh Boulevard,
District 7, Ho Chi Minh City, Vietnam
Email: narumon@rmit.edu.vn
Email: mathews.nkhoma@rmit.edu.vn
Email: anna.felipe@rmit.edu.vn
Email: kimthanh.cao@gmail.com
*Corresponding author

Quyen Ha Tran
University of Economics HCMC Vietnam,
59C Nguyen Dinh Chieu Street,
Ward 6, District 3, Ho Chi Minh City, Vietnam
Email: quyentran@ueh.edu.vn

Roger Epworth, Avinash Shankaranarayanan and Huy Le Quang

RMIT University Vietnam,
702 Nguyen Van Linh Boulevard,
District 7, Ho Chi Minh City, Vietnam
Email: roger.epworth@rmit.edu.vn
Email: avinash.shankaranarayanan@rmit.edu.vn
Email: huy.lequang@rmit.edu.vn

Abstract: As the ASEAN consumers are increasingly moving online, the number of internet users according to UBS increase to 32% across the region and 112% penetrated by mobile technology. More than 50% of ASEAN users are participating to online social network (OSN). This research is to investigate the awareness and influence of security and privacy issues on internet users' trust, and building a safer OSN landscape in South East Asian region by examining the relationships among online privacy concerns, security, trust, and intention. Using structural equation modelling, the findings shows that ‘privacy’ correlates with ‘security’ but these two variables do not have significant impact on users’ trust. Moreover, only ‘trust’ and ‘security’ affect users’ intention to use OSN.

Keywords: online social network; OSN; privacy concerns; security; trust.


1 Introduction

Over the past 30 years of development since the day TCP/IP protocol was standardised creating a worldwide network of interconnected computers, the internet has deeply impacted on the way we live, think, behave, and has revolutionised the way we...
communicate with each other. The internet has been an indispensable medium for mutual collaboration, interaction, and especially a platform for social networking among individuals regardless of their geographic location. Online social network (OSN) sites, such as Facebook, MySpace, Twitter, or LinkedIn, have rapidly gained popularity with millions of users all over the world, many of whom, particularly the younger generation, have grown up fully wired to the internet, and consider OSNs more than just a means of keeping in touch but also an integral part of life.

As defined by Boyd and Ellison (2007), social networking sites let users create a profile, link with others’ profiles to create a list of connections, and view and interact with their connections, as well as connections belonging to others. There are hundreds of social networking sites that offer a wide variety of purposes and usages, but most of them share the same core feature: a profile, which is an online representation or persona of the user (Gross and Acquisti, 2005). When creating a profile, a user generally responds to a series of questions about themselves, such as name, age, birthday, relationship status, interests and hobbies, or contact details. The visibility of such personal information either can be by ‘system default’ to the general public or it can vary depending on the user’s discretion. What makes OSNs popular is they not only allow individuals to keep in touch and maintain already established real life relationships but also OSNs make it easier for individuals to create new social connections based on the information users provide on their profiles.

Most OSN providers offer customised privacy settings so that users have the flexibility to choose which information is publicly disclosed or to create more complicated privacy settings to restrict data to the view of a certain (limited) group of connections. Nevertheless, there are still many users who are either negligent or unknowledgeable about what information is shown on their profiles or how it is used. The revelation of personal information to mere acquaintances or strangers often poses privacy or security threats to users who can be stalked, or have their identity or credit card or other sensitive information stolen. Users’ online privacy and security concerns have attracted the attention of researchers, but there are still very few studies on ASEAN region. WhiteHat Security reported that in 2013, 46% of social networking sites were exposed to serious vulnerabilities year-round (‘serious vulnerabilities’ is defined as websites that can be easily taken total control over by an attacker which compromise users’ accounts and their personal information). This poses a concern for the OSN users’ security when people all over the world continue to spend more time on OSNs than other types of websites (Nielsen, 2012) and internet users in Southeast Asia, specifically, spend more than 80% of their online time on OSNs (ComScore, 2013).

With what being said, there is a need to investigate how users adopt OSN services. As a result, this investigation is directed at understanding privacy and security concerns in using OSNs within the context of ASEAN countries, where little is known regarding this issue for this region. ASEAN is a geo-political and economic organisation consisting of ten countries locating in Southeast Asia: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam (ASEAN, 2013). ASEAN is being examined instead of Southeast Asia as a whole because East Timor is a newly independent country where internet penetration is still very low with only 0.11% in 2012 (Paul Budde Communication Pty Ltd., 2012). Consequently, this research aims to
investigate ASEAN countries users’ awareness of privacy and security concerns on the selection and use of OSNs

2 examine ASEAN countries users’ trust and intention in using OSN.

A modified version of Shin’s (2010) social networking service (SNS) acceptance model is applied to understanding the influence of privacy and security concerns on users’ trust and intentions in the use of OSN.

2 Privacy, security, trust, and intention in OSN

Privacy involves an individual’s process of regulating the extent to which his personal information is disclosed to others and his control over how such information is disseminated (Berman and Bruening, 2001; Van De Garde-Perik et al., 2008). Nevertheless, privacy is a broad and multidimensional concept which should be evaluated and examined within a particular context and any applicable rules or policies (Solove, 2002). Having said that, the primary concern of privacy resides in an individual’s right to control information about oneself (Hugl, 2011). In the context of OSN, privacy refers to a user’s control over identity anonymity (the ability to stay anonymous online), a user’s personal space privacy (the visibility of the user’s online self-representation), and a user’s communication privacy (data regarding the user’s network connection, such as IP address, length of connection or user’s other messages (Zhang et al., 2010). Moreover, Bellman et al. (n.d) discover that privacy regulation preferences reflect differences in cultural values. These cultural values have been indexed based on Hofstede’s (1980, 1991) cultural dimensions: power distance index (PDI), individualism (IND), masculinity (MAS), and uncertainty avoidance index (UAI). These indices have been found to have significant effect on information privacy concerns in most countries (Bellman et al., n.d). For instance, information privacy has positive correlation with PDI, IND and MAS, but is negatively associated with UAI. Empirical research, however, shows contrasting results. Maynard and Taylor (1996) find that Japanese students (IND = 46 ) and Germany (IND = 67) show more concern about privacy than the USA (IND = 91).

Privacy concerns are related to an individual’s awareness of the site or service provider’s practices and handling of their personal data and the risks of sharing information about themselves (Hugl, 2011; Smith et al., 1996). Several studies provide insights into privacy concerns towards the use of OSN (Chin et al., 2012; Dwyer et al., 2007; Krishnamurthy and Wills, 2008; Malhotra et al., 2004; Mohamed and Ahmad, 2012; Stutzman, 2006; Tan et al., 2012), but the findings are inconsistent because privacy is usually examined as a multidimensional variable and does not address the unique characteristics of OSN usage (Krasnova et al., 2009). In the Krasnova et al. (2009) group’s study, two focus groups were conducted to explore internet users’ privacy concerns in attempt to provide more validated ‘privacy concern’ measurements in the OSN context. The content analysis of the study showed that there are four main privacy concerns about OSNs: general accessibility (fear of personal information being viewed by unwanted parties, such as parents, bosses, or unauthorised parties like stalkers); social threats (other users’ actions they cannot control, such as being tagged in a photo or posting humiliating content on the user’s profile); organisational threats (the misuse of
personal information by OSN providers and third parties such as online marketing agencies); and identity theft.

In the Krasnova group study, the focus groups consisted of German students whose culture is very different from ASEAN countries. A research study by Cho et al. (2009) investigating the extent that cultural differences impact on internet users’ perception and behaviour, found that users from high individualism countries have a stronger desire to protect their private life and are more concerned about potential privacy intrusion, which makes them tend to share less of their information online. Furthermore, the participants in Krasnova focus group study were mainly users of Facebook and StudiVZ (a popular social network platform among European students which has strong similarities with Facebook) and the research was carried out in 2008. Facebook’s privacy control has been reinforced over the last few years and the privacy settings button now is made more visible to users so that they are aware of the possibility of controlling their privacy. Nevertheless, the qualitative findings from the Krasnova group’s research served as the basis for questionnaire items designed to gain an exploratory understanding of users’ privacy concerns.

Some authors may have wrong perception in treating two concepts ‘Privacy’ and ‘Security’ as one and use them interchangeably. However, privacy and security should be treated as two separate variables. As previously defined, privacy concerns refer to the users’ awareness of an OSNs handling of their personal information, such as the kind of data that is being collected, where the information will be stored, or how it will be used, which is usually disclosed when a user creates a site profile. The risk of breaching privacy is also informed in the policy. Security, on the other hand, involves the technical practices and mechanisms that OSN providers employ in order to ensure that their users’ personal data is being well handled and their privacy is being protected so that the users are free from danger (Flavián and Guinalíu, 2006).

Sharbaugh and Le Trang (2012) conducted qualitative research to gain an exploratory understanding of Vietnamese’ online personal privacy. Their study revealed that the Vietnamese perceived privacy as a mean of keeping their own personal information from individuals who might use such information for malevolent purposes. The Vietnamese are more concerned about privacy threats from individuals (e.g., friends, colleagues, hackers, thieves) than from entities (e.g., government, corporations, and marketers). Regarding the security of their personal information, the Vietnamese think that it is the individual’s, and not the service provider’s responsibility to preserve the information. It is thus worth examining the connection between users’ perceived privacy and security with regard to OSNs. Hence, this study hypothesised that:

H1 Users’ concerns regarding privacy have a positive correlation to security with regard to OSNs.

OSN providers keep track of all user interactions and information and store the data in a server for data mining and to improve their networking platforms. Several researchers have investigated the threats OSN users might face when such personal information being stored is leaked. Krasnova et al. (2009) pointed out several OSN security issues including digital dossier collection by unauthorised parties, cyber stalking and cyber bullying. Gao et al. (2011) had also surveyed all possible OSN security attacks, dividing them into four main categories: privacy breach; viral marketing, such as spams and phishing; network structural attacks such as Sybil attacks (one user can create and control several accounts
and identities and link with each other in order to promote credibility and reputation enough to reach their attack goals); and malware attacks.

Such possible security threats and attacks that users might face on the internet often determine the users’ perception reliability of any internet website or service. The technologies and systems employed by OSN providers to maintain users’ digital safety is an important factor determining users’ trust (O’Neill, 2012). Jøsang et al. (2007) also stated that when security mechanisms provided by OSNs protect users from malicious parties, the websites are deemed more reliable and trustworthy by users. In fact, several studies have examined the link between privacy concerns, perceived security, and trust in internet shopping, and the findings show that consumers have low level of trust towards an e-commerce website if they fear their transactions are insecure, that those websites might share their personal data with third parties, or that their credit card information might be hacked and stolen (Belanger et al., 2002).

Mayer et al. (1995) define trust as an individual’s intention to depend on other parties based on their actions or attributes that are deem important to the trustor regardless of trustor’s inability to affect or control the other parties’ behaviours. The perceived trustworthiness of the trustee and the extent to which an individual is willing to trust are formed based on trustee’s ability, honesty, and good will (Mayer et al., 1995). In the context of online representations, there are some studies carried out to learn which factors of a website can obtain users’ trust. For example, it was noted by Cyr (2008) that it was more likely for a website to be perceived as trustworthy if it had information of good quality and attractive visual design, whereas Awad and Ragowsky (2008) found a correlation between word-of-mouth quality and perceived trustworthiness in online bulletins.

In this research within the context of OSNs, little is known about the connections among perceived privacy, security, and trust towards the intention to use OSNs in ASEAN countries. With that being said, the following hypotheses are proposed for purposes of this study:

H2 Users’ concerns regarding security have a positive correlation to trust in OSNs.

H3 Users’ concerns regarding privacy have a positive correlation to trust in OSNs.

There have been several researchers examining how privacy and security concerns affect users’ online behaviours. Krasnova et al. (2009) considered the impact of privacy concerns on users’ online self-disclosure. Their findings revealed that users had a tendency to share less of their personal information and were more attentive to the type of information being disclosed due to their privacy concerns. Tufekci (2008), on the other hand, found little to no relationship between users’ online privacy concerns and information disclosure; users managed the audiences they wanted to share information with rather than restricting the type of information being disclosed.

Several other studies (Belanger et al., 2002; Flavián and Guinalíu, 2006) found a direct correlation between online security and users’ willingness to make online purchases. These results showed that if a website engaged in electronic commerce mishandled consumers’ personal details, such as by selling data to a third parties that resulted in spam being sent to consumers’ internet mailboxes, those consumers were unlikely to continue using the service and website loyalty decreased correspondingly (Belanger et al., 2002; Flavián and Guinalíu, 2006). Boyd (2007) examined the way teenagers build their social network profiles and the findings showed that teenagers in the
study fabricated their personal information such as name, age, and location or limited who could see the content of their personal social sites as a response to privacy concern against their parents. In another research surveying Malaysian students by Mohamed and Ahmad (2012), it was shown that the more participants were concerned with their data privacy, the more likely they would employ measures to protect their information.

Consequently, it is worth examining how the two antecedents, privacy concerns and security, affect users’ intention in using OSNs among users in ASEAN countries as a whole.

H4 Users’ concerns regarding security have a positive correlation to intention in using safe OSNs.

H5 Users’ concerns regarding privacy have a positive correlation to intention in using safe OSNs.

Trust also plays an important part in determining users’ intention to adopt a service being offered online (Jøsang et al., 2007). McKnight et al. (2002) developed and examined a model of consumer trust regarding their intention to adopt an electronic commerce services or to make an online purchase. There are two interrelated components in online trust, which are trusting beliefs (users’ perceptions of the website, particularly its competence, benevolence, and integrity) and trusting intentions (users’ willingness or intentions to depend and become vulnerable when using the website) (McKnight et al., 2002). Trusting beliefs being used in this research on OSNs usage stem from users’ perceived privacy and the data security that OSNs offer. With that being said, this study will examine how those ASEAN users’ trust and beliefs will impact their intentions to use OSNs. As a result, we hypothesised the following:

H6 Users’ trust has a positive correlation to intention in using safe OSNs.

Without a doubt, it is worth exploring the connections among the three antecedents, privacy concerns, security, and trust, in relation to intention within the OSN context in ASEAN countries. Our research model is developed and modified based on Shin’s (2010) SNS acceptance model, which was well validated by a survey of SNS users in South Korea and was employed to predict users’ intention towards using SNS. Dhami et al. (2013) also examined user’s willingness to disclose personal data on OSNs in regards of their level of privacy, security and trust. The findings showed positive correlations between security and trust and information sharing while privacy did not effect on the users’ sharing behaviour. Nevertheless, the participants of this research came from all over the world with different cultures and perceptions towards privacy. In addition, Dhami et al. focus on usage behaviour on social networking sites with reference only to Facebook. Instead, this research attempts to explore the relationship among privacy concerns, security, and users’ trust among users from the same geographical sites or similar cultures with wider reference to all social networking sites, which is also the aim of this research that is to give a preliminary understanding of ASEAN users’ intentions towards using OSN. This investigation utilises the conceptual research model depicted in Figure 1.
Figure 1 Conceptual research model depicting relationships among privacy, security, trust, and intention

3 Research methodology and results

Quantitative research methodology was applied in this study to achieve the research objectives. Data were collected via an online survey through Qualtrics platform at https://rmit.asia.qualtrics.com. After launching, there were 679 respondents who used at least one OSN answering the questionnaire including five-point Likert scale questions that explored issues of privacy, security, trust, and intention. The respondents were from Vietnam, Brunei, Cambodia, Laos, Malaysia, Philippines, Singapore, and Thailand, which are the countries of ASEAN but due to preservation of privacy, they were not asked about their locations and therefore, this piece of information is unidentifiable. To resolve the six hypotheses indicated in the conceptual research model as shown in Figure 1, IBM SPSS Analysis of Moment Structures (AMOS) software version 20 was employed to analyse the dataset with regard to the structural equation modelling (SEM). According to Kline (2011), Jöreskog (1993), and Jöreskog and Sörbom (1982), SEM model allows both confirmatory and exploratory modelling, meaning the model is suited to both theory testing and theory development and therefore is appropriate for this study.

To validate the SEM output, it is necessary to analyse the reliability, convergent validity and discriminant validity to examine the reliability of the scale and data validity as proposed by Straub et al. (2004) as demonstrated in Table 1.

Based on the reliability of the scale, a Cronbach’s alpha coefficient whose value is greater than 0.7, indicates a reliable and consistent scale; however, according to Hair et al. (2006), sometimes the cut-off point of 0.5 is acceptable. In this study, the Cronbach’s alpha coefficient of the constructs of ‘privacy’, ‘security’, ‘trust’, and ‘intention’ are 0.821, 0.804, 0.684, 0.825, respectively; hence, indicating that the scale is reliable.

In term of convergence in data validity, the scale is adequately convergent when the average variance extracted (AVE) of each construct is at least 0.5. In order to prove discriminant validity, the square root of AVE for each construct should be much larger
than the correlation of the specific construct with any of the other constructs in the model (Chin, 1998), and should be at least 0.5 (Fornell and Larcker, 1981). The calculated numbers shown in Table 1 reveal that the data obtained in this research do not have sufficient convergent validity because the AVE of all instruments are slightly less than 0.5; however, the data have discriminant validity due to the criteria previously mentioned. Thus, the data from this research were acceptable.

Figure 2  SEM indicating relationships among ‘privacy’, ‘security’, ‘trust’, and ‘intention’ (see online version for colours)

<table>
<thead>
<tr>
<th>Construct</th>
<th>AVE</th>
<th>( \text{Square root AVE} )</th>
<th>Privacy</th>
<th>Security</th>
<th>Trust</th>
<th>Intention</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Privacy</td>
<td>0.352</td>
<td>0.593</td>
<td>1</td>
<td>0.667</td>
<td>-0.021</td>
<td>0.031</td>
</tr>
<tr>
<td>2 Security</td>
<td>0.414</td>
<td>0.643</td>
<td>1</td>
<td>0.058</td>
<td>0.156</td>
<td></td>
</tr>
<tr>
<td>3 Trust</td>
<td>0.380</td>
<td>0.616</td>
<td>1</td>
<td>0.360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Intention</td>
<td>0.475</td>
<td>0.689</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Before interpreting the output of the SEM model, the overall fitness of the model must be examined. There are primary indices of fit measures that can be utilised to make this determination, particularly chi-square, normed chi-square/df (CMIN/df), P-value of chi-square test, goodness of fit index (GFI), Tucker-Lewis index (TLI), comparative fit index (CFI), and root mean-square error of approximation (RMSEA).

**Table 2**  
Fit indices for SEM model

<table>
<thead>
<tr>
<th>Fit measures</th>
<th>Standards of fitness</th>
<th>Model fitness</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-square</td>
<td>As small as possible</td>
<td>1,040.992</td>
<td>Acceptable</td>
</tr>
<tr>
<td>CMIN/df</td>
<td>Not greater than 2 is good, but sometimes not greater than 3 is acceptable (Carmines and McIver, 1981)</td>
<td>2.783</td>
<td>Acceptable</td>
</tr>
<tr>
<td>P-value</td>
<td>Greater than 0.05</td>
<td>0.000</td>
<td>Not supported</td>
</tr>
<tr>
<td>GFI</td>
<td>Greater than 0.9 (Bentler and Bonnet, 1980)</td>
<td>0.907</td>
<td>Good</td>
</tr>
<tr>
<td>TLI</td>
<td>Greater than 0.9 (Bentler and Bonnet, 1980)</td>
<td>0.885</td>
<td>Acceptable</td>
</tr>
<tr>
<td>CFI</td>
<td>Greater than 0.9 (Bentler and Bonnet, 1980)</td>
<td>0.901</td>
<td>Good</td>
</tr>
<tr>
<td>RMSEA</td>
<td>Not greater than 0.05 is good, but sometimes not greater than 0.08 is acceptable (Steiger, 1990)</td>
<td>0.051</td>
<td>Good</td>
</tr>
</tbody>
</table>

The model used is proven to fit the population data because of the indicators shown in Table 2: the chi-square/df is smaller than 3 (chi-square/df = 2.783 < 3) (Carmines and McIver, 1981); almost the GFI, TLI, and CFI indicators are larger than 0.9 (GFI = 0.907 > 0.9; TLI = 0.885; CFI = 0.901 > 0.9) (Steiger, 1990); and the RMSEA is less than 0.08 (RMSEA = 0.051 < 0.08) (Steiger, 1990). Although the P-value measure does not support the model fitness, all the other indices do.

**Table 3**  
Regression weights generated by SEM in Figure 2

<table>
<thead>
<tr>
<th>Estimate</th>
<th>P-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Privacy</td>
</tr>
<tr>
<td>Trust</td>
<td>Security</td>
</tr>
<tr>
<td>Trust</td>
<td>Privacy</td>
</tr>
<tr>
<td>Intention</td>
<td>Trust</td>
</tr>
<tr>
<td>Intention</td>
<td>Privacy</td>
</tr>
<tr>
<td>Intention</td>
<td>Security</td>
</tr>
</tbody>
</table>

Note: *** is smaller than .001.

The P-value and the sign of the estimate of the regression weights shown in Table 3 demonstrate that ‘privacy’ has a positive significant impact on ‘security’ (P-value < 0.001), confirming H1; ‘trust’ and ‘security’ have a positive significant impact on ‘intention’ (both P-values < 0.001), confirming H6 and H4 respectively; and ‘security’ and ‘privacy’ have no significant correlation with ‘trust’, therefore not confirming H2 and H3; and finally that ‘privacy’ has no significant correlation with ‘intention’, therefore not confirming H5.

The estimate of standardised regression weights shown in Figure 3 demonstrates that ‘privacy’ makes a tremendous impact on ‘trust’ [Coefficient (privacy) = 0.671]. Within ‘Trust’ and ‘security’, ‘trust’ makes bigger positive impact on ‘intention’ [Coefficient
(trust) = 0.401; Estimate (security) = 0.250]. The final outcomes of the research are summarised in Table 4.

Figure 3 Standardised regression weights utilised in the path model

Note: In the path model, (***)) denotes significance at 99.9% confidence level.

4 Discussion

The first objective of this study was to understand ASEAN users’ awareness of privacy and security concerns on the selection and use of OSNs. It is statistically proven in Table 3 that ASEAN users are concerned about their online privacy and the security threats they might encounter on OSNs, and privacy concerns have a positive correlation with security. More than 50% of the respondents said that they were concerned about their inability to control other users’ actions on OSNs and that other user might say something undesirable about them. 60% of respondents were concerned that the information they disclosed on OSNs could be taken advantage of or misused by other users or shared with third parties by OSN providers. Furthermore, the study participants were concerned that someone could use their personal information to sign up to another website for malevolent purposes and so 66% of them did not add strangers as ‘friends’ on their OSNs. The majority of respondents reported concerns that they might encounter malicious computer/information security problems, such as viruses or hacking, on the OSN sites.

The second objective of this study was to examine ASEAN online users’ trust and intention in using OSN. The data analysis revealed that both privacy and security had no significant relationship with users’ trust. This contrasts with findings from other research studies discussed in the literature review, which suggest that privacy concerns and security affect users’ perceived trustworthiness of an online service (Belanger et al., 2002; Jøsang et al., 2007; O’Neill, 2012). A study by Krasnova et al. (2009) also showed that users were concerned about their privacy which resulted in less sharing of their information and more attention to the kinds of information that ought to be disclosed. ASEAN country users, on the other hand, are not affected by privacy concerns in regards of their online information sharing which is also aligned with what had been found in the
2013 research by Dhami et al. A possibility for this result is the difference between Eastern culture and Western cultures that were the basis of other research studies. Particularly, people living in collectivist cultures (e.g., Vietnam, Singapore, Thailand) feel more comfortable disclosing their personal information than those living in individualistic cultures, such as Western countries, where users feel a greater sense of urgency to protect their individual online privacy (Cho et al., 2009). It is also reported that Asian users are not as concerned as European users about their online privacy, and that Asian users are willing to share their personal information for rewards in form of free services or better targeted online advertisements (Huan, 2012). Nevertheless, users will be more likely to utilise privacy measures in order to protect the information they share on OSNs as a case in Malaysia (Mohamed and Ahmad, 2012).

Security also has no significant relationship with trust. A plausible explanation for this can be stemmed from a research done by Sharbaugh and Le Trang (2012) within the context of Vietnamese OSN users. Their findings showed that the Vietnamese participants perceive that securing personal information is more of an individual responsibility rather than a responsibility of the internet service providers (ISPs) to provide a secure framework to protect user data and they believe that a strong password created by the users themselves is the key to guard and secure users’ personal online worlds (Sharbaugh and Le Trang, 2012). As a matter of fact, 60% of respondents did not think that they could rely on OSN sites to do their part and 65% saying OSN sites did not have enough safeguards to make them feel comfortable. This is alarming because without acknowledging how websites secure their confidential data, they can be victims of shady websites disguised as OSNs in order to obtain and use their personal information for malicious purposes.

In examining the correlations of the three antecedents: privacy concerns, security, and trust, towards intention of joining OSNs, it appears that security and trust both have a significant effect on users’ intention. This finding confirms results reported in the research studies mentioned in the literature review that show that trust and the technical mechanisms which online service providers employ to secure their users’ private data play important roles in determining users’ choice of OSNs (Belanger et al., 2002; Flavián and Guinalíu, 2006; Jøsang et al., 2007). Privacy, on the other hand, does not appear to directly affect users’ intention to join OSNs among ASEAN users. Although as proven in Hypothesis 1, ASEAN online users are concerned about their privacy, this does not seem to affect their intention to share personal information and life experiences on OSNs. A plausible explanation for this insignificance is that ASEAN users do not have the tendency to add strangers as ‘friends’ on their OSNs (stated by 70% of respondents) and perhaps because living in a highly collectivist culture makes them feel at ease about sharing their personal information and life experiences with their circles of friends and other like-minded people, which was stated by more than 70% of participants as their purpose of sharing information on OSNs.

The findings of this research add to the learning of the OSN landscape in ASEAN region in terms of users’ perception and behaviour. This research gives an exploratory understanding of the correlations among privacy, security, trust, and intention among ASEAN OSN users. An important finding of this study was that ASEAN users neglected the importance of security framework that OSNs use to safeguard their private data. This poses a concern that ASEAN users might fall into the security traps of shady OSNs where their personal information might be compromised and be used for wrong purposes.
From this research, it is recommended that local authorities responsible for online safety should take actions in educating their users the threats they might face when spending their leisure time on OSNs.

5 Conclusions and limitations

To date, little has been known about the perceived privacy and security concerns of ASEAN OSN users. Accordingly, this study was conducted in order to gain an exploratory understanding of ASEAN users’ awareness of privacy and security issues relating to their OSN use, their trust and intentions with regard to joining and participating in OSNs. This research examined the connections among three antecedents: privacy concerns, security concerns, and users’ trust, and how each of these correlates with users’ intention. It is reported that 46% of social networking sites can be easily compromised and attacked which can affect users’ accounts and personal information (WhiteHat Security, 2013), while OSNs capture more than 80% of internet users’ online time in Southeast Asia (ComScore, 2013). The chance that users face online threats online is high and thus, the findings of this research can hopefully provide valuable insights for the implementation of enhanced OSN security measurements to avoid further threats to ASEAN OSN users.

This study statistically proves that ASEAN OSN users are aware of their online privacy and that privacy concerns, in turn, affect their awareness of security threats they might encounter on OSNs. Nevertheless, privacy and security concerns do not appear to affect ASEAN OSN users’ trust. This is possibly due to users believing individuals should be responsible for their own online security rather than a responsibility of the OSN providers (Sharbaugh and Le Trang, 2012). As a result, trust and security have a significant impact on users’ OSN intention because they believe in their own ability to protect their personal information from getting into the hands of strangers who might use such information for improper purposes. Privacy concerns, on the other hand, perhaps do not correlate well with OSN users’ intentions because users in ASEAN countries live in a collectivist culture and it has been suggested that people from collectivist cultures are more comfortable with sharing their personal information and life experiences with their friends.

A limitation to this study is that the researchers designed questionnaires and worked with a conceptual research model in which each antecedent was expected to correlate with the other. Respondents, however, might have responded to survey questions as independent variables. Moreover, this research has only been based on quantitative results. In addition, the questionnaire was translated from English into local languages, thus word meanings might have been slightly misinterpreted. For stronger confirmation and insight into ASEAN country users’ perceived privacy and security concerns, and trust towards the intention to participate in OSNs, it is recommended that focus groups be conducted in order to better understand possible links among those variables, so that it is more understandable in how one factor might affect the others or have any influence on the decision to use OSNs.
ASEAN users’ privacy concerns and security in using online social networks

Acknowledgements

This work was supported by RMIT 2013 Internal Grant Scheme No. 16.

References


Paul Budde Communication Pty Ltd. (2012) *East Timor (Timor Leste) – Telecoms, Mobile and Internet*. 


