MODELLING USERS' TRUST IN ONLINE SOCIAL NETWORKS

**Iacob Cătoiu[1*], Mihai Orzan[2], Octav-Ionuț Macovei[3]
and Claudia Iconaru[4]**
[1) 2) 4)] *The Bucharest University of Economic Studies, Romania*
[3)] *Lumina – The University of South-East Europe*

Abstract

Previous studies (McKnight, Lankton and Tripp, 2011; Liao, Lui and Chen, 2011) have shown the crucial role of trust when choosing to disclose sensitive information online. This is the case of online social networks users, who must disclose a certain amount of personal data in order to gain access to these online services. Taking into account privacy calculus model and the risk/benefit ratio, we propose a model of users' trust in online social networks with four variables. We have adapted metrics for the purpose of our study and we have assessed their reliability and validity. We use a Partial Least Squares (PLS) based structural equation modelling analysis, which validated all our initial assumptions, indicating that our three predictors (privacy concerns, perceived benefits and perceived risks) explain 48% of the variation of users' trust in online social networks, the resulting variable of our study. We also discuss the implications and further research opportunities of our study.

Keywords: social media, users trust, online privacy, structural equation modelling

JEL Classification: M31, L82

Introduction

Protection of consumers' private space is one of the foremost principles of corporate social responsibility, bringing together privacy and data protection as an intrinsic part of modern business. Consumers' privacy should be protected in compliance with all legal requirements and beyond (Dinu, 2011), in order for consumers to take full advantage of an increasingly interconnected and data-driven world. By being proactive and understanding how users think and act towards disclosing sensitive information, companies could install a trust-centric environment, where users' concerns regarding privacy and security are diminished and further interaction is encouraged (Xu, 2012).

Internet has become an ever growing presence in our daily activities (Pelău and Bena, 2010) and the amount of public information available and collected by interested entities has increased exponentially within the framework of social networking sites expansion.

---

[*] Correponding autor, **Mihai Orzan** - mihai.orzan@ase.ro

While companies and other interested parties strive to gain access to consumer data, privacy continues to be one of the main concerns of Internet users, as 62% are concerned about their online privacy (Han and Malaren, 2002).

In the particular case of social networks, slightly over half of registered users try to set their profiles to private, 48% men and 67% women (Magid, 2012). These figures show some alarming concerns regarding users' lack of knowledge in managing privacy options on social networking sites. This is a consequence of the way users perceive risks and benefits associated with information disclosure, and may indicate their privacy concerns and trust in social networking sites, which is the primary focus of our research.

Online social networks are part of social media. According to Kaplan and Haelin (2010, pp. 59-68) social media can be defined as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content".

Moreover, there are six different types of social media: collaborative projects (e.g., Wikipedia), blogs and micro blogs (e.g., WordPress, Twitter), content communities (e.g., YouTube), social networking sites (e.g., Facebook, Twitter), virtual game worlds (e.g., World of Warcraft), and virtual social worlds (e.g. Second Life). However, these delimitations among different types of social media are not always so exact (Moise, Georgescu and Zgură, 2012). One good example is Twitter, which can be considered both a micro-blogging site and a social network.

1. Development of online social media and their users

Social networks have had a rapid and progressive evolution in terms of Internet users' adoption, reaching 1.4 billion users in 2012, representing 82% of worldwide Internet users, and it is estimated that they'll reach over 1.5 billion users by the end of 2013 (eMarketer, 2012).

According to Wikipedia (2013) and eBizMBA (2013) which analyzed traffic ranks from alexa.com, the most popular social networks are Facebook, with over 950 million active accounts and 750 million monthly unique visitors, followed by Twitter (500 million accounts and 250 million visitors), Qzone (536 million active accounts, mainly from China), Google Plus+ (over 250 million registered users), LinkedIn and MySpace. In the European Union there are 347 million users of social networking sites, representing 73% of European Internet users (Insites, 2011), and the most popular social networks are Facebook, followed by Twitter, Vkontakte and LinkedIn.

The users of social networking sites can be divided by many criteria. First are the demographic ones. For example women represent the majority of Facebook and Twitter users, and men the majority of LinkedIn and Google+ (Magid, 2012). The regions with the lowest use of social networking sites are Eastern Europe and Asia (around 40%) while South America has the highest percentage of Internet users (around 95%) (Buzzom, 2012). Over 75% of teens and adolescents have a profile on a social networking site and 85% teenage children ages 13 – 17 years have a profile on a social networking site (Internet Safety, 2012). According to the same source, more than 50% of teens log on to their social network account daily and 38% of Facebook users in 2011 were under the age of 13, the minimum legal age allowed to create an account, from which over 25% are under the age of 10.

Users can be divided into passive, which have an account but access it very rarely and almost never update their information, voyeur, which access the account only to look on other users profiles, social occasions, which irregularly post information on their account, especially only for major events, and addicts, which access their account and update their profile information or status almost daily (Buzzom, 2012).

This is the first aspect of the consequences of personal information disclosure through social networks. The second aspect is related to the use of personal information for marketing purposes (Popescu, Dumitru, Veghe and Kailani, 2013). While in the first case information is voluntarily shared by users, in the second case the information is inferred by electronic means from users' online behaviours using "cookies" (Privacy Rights, 2010), click-stream analysis, data mining techniques and data-warehousing technology. This information collected especially by third-party applications from social networks like games, personal agendas, event planners, media content apps and many others, allowing them to collect cheap information and to develop customer behaviour profiles for better targeted online marketing campaigns (Rust, Kannan and Peng, 2002)

Practically, social networks have added an increased amount of personally identifiable information (PII) which can be used by third parties in order to distinguish and trace an individual's online identity (Krishnamurthy and Wills, 2009). Third-party applications can combine the information collected from online social networks, phenomenon known as "leakage", with the information about the same user collected from other regularly visited websites, which lead to increased online malware practices and abusive marketing practices. The most common frauds on social networks are identity thefts, hacks and frauds through malicious software (McCole, Ramsey and Williams, 2010).

Social networks and third-party applications on social networks often gather data from users in order to sell them to marketing data starved companies, like advertisers or software developers. More interesting is the behaviour which stands behind the social network users' intention regarding their willingness to disclose personal information and how they perceive the risks and benefits associated to this social activity, their privacy concerns and their trust level regarding personal data usage of social networks.

2. Trust in online social media

According to Meinart et al (2006) the information requested by web sites can be classified in three categories: contact information, biographical information and financial information. Also, an Internet user is more willing to provide contact information, including his or hers phone number, e-mail, name or address rather than biographical information like age, workplace, interests and hobbies. Nonetheless, users are more willing to provide biographical information rather than financial information, credit card numbers or account details. In this context, the most important elements in building consumer confidence in e-commerce are secure networks, secure access and protecting privacy (Ionescu, Lăzăroiu and Şerban, 2013).

Social networking sites request information from the first two categories, and this is a reason why they have such a great adoption rate among Internet users, because sharing these types of information apparently seems harmless. Furthermore, if the contact information is generally requested by the social networking sites, which is a common practice among all types of websites which require user accounts, the biographical information is shared voluntarily by the users, and many times this kind of information is more valuable for third parties.

Public profiles in social media amount to about 47% of their users (Magid, 2012), with about 91.3% of them creating accounts with real data (CNN, 2012). Sharing information voluntarily on this media has become a major concern and raises privacy and trust issues, as only about 70% of users provide real information about themselves on other online services (Marketing Charts, 2007), thus becoming a true bonanza for different data mining and data warehousing tools of third-party applications.

The relationship between privacy, trust and perceived risks has been analysed frequently in the marketing literature, with an emphasis on electronic commerce (Pand and Zinkhan, 2006; Eastlick, Lotz and Warrington, 2006), online monetary transactions (Liao, Liu and Chen, 2011), website users' experience and personalization (Lee and Cranage, 2011) and online marketing campaigns, especially e-mail campaigns (Cases et al, 2010).

2.1 Privacy concerns of information disclosure

Privacy can be regarded as a limited access to a user's information and weighs heavily when users decide whether to disclose their personal information and the amount of displayed information, together with the associated benefits of using social networking sites (Hart, 2006). However, users are aware of the fact that they must share an amount of information in order to benefit from using online social networking sites.

Using the interview research method, Young and Quan-Haase (2009) found that users' main concern is that their information would be used for potentially harmful purposes by other parties that would gain access to their data. The second main concern when using online social networks was the possibility that their information could and would be used, sold or appropriated without their knowledge and consent. Also, data mining and various moral prejudices from unauthorized people seeing inappropriate hidden content were stated as privacy concerns in the study of Young and Quan-Haase (2009). As a result of their privacy concerns, users tend to reduce the amount of disclosed information and they become more conscious about the type of content they display publicly (Krasnova et al, 2009).

2.2 Perceived risks of information disclosure

Users cannot take advantage of the whole range of benefits associated with online social networking websites unless they disclose a certain amount of personal information. Users may perceive that their personal information is a vulnerable target, prone to alienation to third parties for marketing purposes, unauthorized access, threats to personal identity, and misuse of personal information or malware attacks (Featherman and Pavlou, 2003).

2.3 Perceived benefits of using online social networks

Users are perceived as trading their personal data for benefits derived from using such social media platforms. According to motivation theory, perceived benefits of using online social networks derive from a combination of both usefulness and enjoyment (Kuan-Yu and His-Peng, 2011). Users do not only enjoy spending time on social networking sites, but they believe that these sites could enhance their personal and professional standings.

According to Collin et al (2011), online social networks offer a variety of benefits, from delivering educational outcomes to facilitating supportive relationships and identity formation. Online social networks are perceived to be able to strengthen interpersonal relationships, especially when the online and offline worlds converge, but also supports the development of new interpersonal relationships. Identity formation and self-expression comes from the facility of individual customization of personal page and its content.

Nonetheless, online social networks are able to provide a sense of belonging and to boost one's self-esteem. Content sharing plays a major role in developing the sense of belonging within an online social group and forming a collective identity due to being part of a small-scale community (Colin et al, 2011).

2.4 Users' perceived trust in online social networks

Trust could be regarded as the foundation of online interactions, since users of online social networks reveal a lot of sensitive information, willingly or unwillingly. Trust is a multi-dimensioned concept, having both a macro and a micro dimension. According to Lai and Turban (2008), users must trust the technology they are using and those who designed it. They must also trust other users of the same platform. Micro level trust can be controlled by high level privacy settings. Macro level trust could be regarded as an institution-based trust, which is associated to the users' perceptions that the organizational structure is trustworthy (McKnight and Chervany, 2002).

Technology features, as well as a rational calculus of the costs and benefits of using a social networking sites interfere with initial trust building, followed by an user personal interaction with the site where judgements regarding trust are knowledge or experienced-based. (Grabner-Krauter and Bitter, 2013). An user who is comfortable with the Internet is more likely to trust the online social network security, control and confidentiality mechanisms, which exists to protect him from losing his privacy, identity or financials (Grabner-Krauter and Bitter, 2013)

3. Research model and hypotheses

The main objective of this study is to offer an explanation as to online social networks' trust formation, when considering a privacy calculus which takes into consideration both the benefits of using online social networks and various risks to which users are subjected. Thus, we propose the following research model in Figure 1.
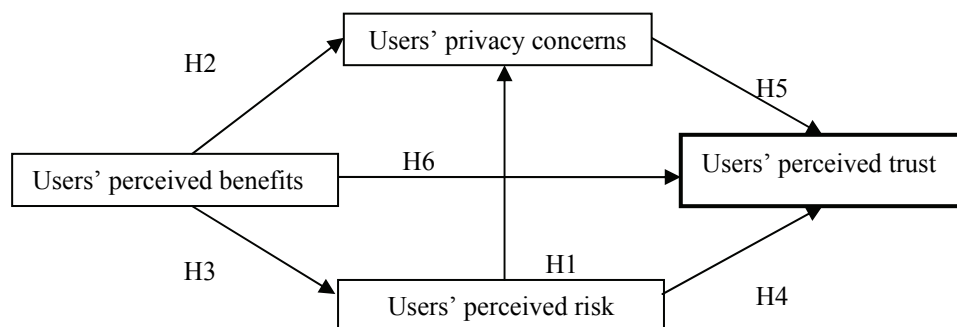

Figure no. 1: Proposed model of users' perceived trust in online social networks

There are many risks associated with the disclosure of personal information, as discussed in previous section of theoretical background and are assumed to have a positive impact on users' concerns regarding the privacy of their personal information. For example, if a user perceives the risk of personal data access by third parties, he or she is prone to having

concerns regarding who has access to his or her personal information, by which means and how third parties are going to use their personal information.

Users' perceived risk has been validated as a strong predictor of users' privacy concerns in previous researches (Grant, 2005; Liao, Liu and Chen, 2011; Youn, 2009), thus we assume the first hypothesis of the model:

H1: There is a direct and positive relationship between users' perceived risks and users' concerns regarding the privacy of their information.

Drawing from Dinev and Hart (2006) privacy calculus model, the risk/benefit ratio is taken in consideration when predicting users' intention to disclose personal information. Thus, the variable „Perceived Benefits" was created for the purpose of this study, predicting its ability to decrease both perceived concerns and perceived risks.

H2: There is a direct and negative relationship between users' perceived benefits of using online social networks and their concerns regarding the privacy of their information.

H3: There is a direct and negative relationship between users' perceived benefits of using online social networks and their perceived risks associated with the use of online social networks.

When trying to predict users' trust in online social network at macro level, variables like perceived risks and users' privacy concerns are highly correlated, as validated in previous empirical studies.

A direct and negative relationship between users' perceived risk and users' perceived trust was found in Liao, Lui and Chen (2011), which studied online monetary transactions, Jarvenpaa, Knoll and Leidner (1998) studied in the same context global virtual teams, whilst Josang and Presti (2004) and Jarvenpaa, Tractinsky and Vitale (2000) studied e-commerce and, more recently, McKnight, Lankton and Tripp (2011) studied social networking trust at micro level. In the light of previous empirical research, we formulated the following hypothesis:

H4: There is a direct and negative relationship between users' perceived risks of using online social networks and their perceived trust in online social networks.

H5: There is a direct and negative relationship between users' concerns regarding the privacy of their information and their perceived trust in online social networks.

Furthermore, since the new variable „Perceived Benefits" was added to the research model and taking in consideration Dinev and Hart (2006) privacy calculus model, we postulate that the higher users perceive benefits from using online social networks, the higher is their level of trust in the online social networks.

H6: There is a direct and positive relationship between users' perceived benefits of using online social networks and their trust in online social networks.

4. Methodology

For hypotheses testing, the measures of our four conceptual variables were defined and a survey was employed in order to collect the primary data. The questionnaire has three parts: general questions related to Internet and online social media usage, items corresponding to

our research model constructs, respectively a series of demographic question, such as age, sex, studies, occupation and social networks used (registered). All questions were translated back and forth from English to Romanian by an authorized translator.

4.1 Measurements

Constructs from existing literature were employed in order to measure our three predictive variables: users' privacy concerns, users' perceived risks and users' perceived trust. The variable „perceived benefits" is original for our study, taking into account the major benefits of using online social networks as reported by previous literature. The sources of measurements development is represented in the table below (table 1).

Table no. 1: Source of construct variables

Construct	Code	Items	Source
Privacy concerns (of information disclosure on SNS)	**PC**	4	Liao, Liu and Chen (2011) Dinev and Hart (2006)
Trust (in SNS)	**TR**	3	McKnight and Chervany (2001) Dinev and Hart (2006)
Perceived risks (of information disclosure on SNS)	**PR**	3	Liao, Liu and Chen (2011) Dinev et al (2006)
Perceived benefits (of information disclosure on SNS)	**PB**	3	Self developed

The construct's items corresponding to the research model were measured using a 5-point Likert scale, with the following values: 1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree and 5 – Strongly agree.

4.2 Data collection

The final survey was administered to a large sample of individuals in Romania, consisting of faculty, master and PhD students from the Bucharest University of Economic Studies, high school students from the "Virgil Madgearu" Economic College and employees from series of companies from IT&C, media production and economic fields, receiving 454 questionnaires, from which 421 were valid.

The survey instrument was administered both in classic paper and electronic format. Paper-questionnaires were personally handed by authors after or before class, finally being collected a number a total of 338.

5. Data analysis

The structural equation modelling was conducted with IBM SPSS Statistics Package and Warp PLS 3.0. The database was also checked with IBM SPSS for duplicates, but no such case was found. The database was also check with IBM SPSS Amos for multivariate outliers, which were detected using the Mahalanobis D-Squared distance test for a $p<0.01$. 23 multivariate outliers were found for a $p<0.01$, but were not removed from the database, remaining to decide later about that problem, according to the results of the PLS analysis.

Data analysis and results section comprises: measures reliability and validity, the PLS-based SEM analysis and model fit.

5.1 Measures Reliability

Following Bagozzi and Yi (1988) approach, measures were tested for internal consistency by computing and interpreting Cronbach Alpha coefficients, composite reliability coefficients and average extracted variance (AVE). Nunally (1978) suggests that all CR coefficients should be above the value of 0.7 and Hair et al (1998) suggest that all Cronbach Alpha coefficients should be above the critical value of 0.5 in order to yield internal consistency.

Table 2 shows that all the Cronbach's Alpha and composite reliability values are over 0.7, this meaning that the measuring instrument is reliable and all the items associated to each variable are understood in the same way by different respondents. Also each set of items has internal consistency and each item describe accurately the underlying construct variable.

Table no. 2: Measures Reliability (Internal Consistency)

Construct	Composite reliability (CR)	Cronbach Alpha Coefficients	Average extracted variance (AVE)
PC	0.934	0.893	0.824
TR	0.871	0.777	0.692
PR	0.887	0.807	0.723
PB	0.927	0.881	0.808

5.2 Measures Validity

The validity of the measures were tested with both convergent and discriminant validity. The combined loadings and cross-loadings were employed in order to assess the convergent validity of the constructs, following Jewell approach: indicators among constructs should have high and similar loadings (Jewell, 2011).

Loadings are the Pearson correlations between variables and indicators. The pattern matrix was obtained through an oblique rotation, which is recommended in the case of PLS-based structural equations modelling analysis (Kock, 2012).

Following results from table 3, we can state that measurements have good convergent validity, indicators of each construct loading more inside the construct than cross-loading with the indicators from the rest of the constructs.

Table no. 3: Combined loadings and cross-loadings

	PR	PB	PC	TR	SE	P value
PR1	**0.805**	0.019	0.068	0.069	0.045	<0.001
PR2	**0.868**	-0.035	-0.049	0.014	0.032	<0.001
PR3	**0.876**	0.017	-0.014	-0.078	0.030	<0.001
PB1	-0.039	**0.893**	0.074	-0.014	0.042	<0.001
PB2	-0.024	**0.898**	0.006	0.038	0.038	<0.001
PB3	0.062	**0.905**	-0.079	-0.023	0.042	<0.001
PC1	0.019	-0.038	**0.924**	0.029	0.032	<0.001
PC2	-0.008	-0.033	**0.904**	0.024	0.028	<0.001
PC3	-0.011	0.073	**0.895**	-0.053	0.035	<0.001
TR1	0.165	-0.029	0.154	**0.810**	0.041	<0.001
TR2	-0.135	0.011	-0.066	**0.821**	0.047	<0.001
TR3	-0.026	0.017	-0.082	**0.863**	0.031	<0.001

Note: P values < 0.05 are desirable for reflective indicators.

Measurements' divergent validity was assessed through a confirmatory factor analysis, following Fornell and Larcker (1981) approach, which implies testing the square roots of AVE of each variable of the model with the other correlations which imply testing if the square root of AVE is greater. These values can be seen in Table 4, on the diagonal being the square roots of AVE which are higher than any of the corresponding row or column values.

Table no. 4: Variables correlations and square root of AVE

	PR	PB	PC	TR
PR	**0.850**	-0.189	0.393	-0.547
PB	-0.189	**0.899**	-0.293	0.399
PC	0.393	-0.293	**0.908**	-0.497
TR	-0.547	0.399	-0.497	**0.832**

5.3 Structural Equation Modelling

The structural research model was analysed with WarpPLS 3.0 which is able to analyse nonlinear relationships between variables (Kock, 2011; Kock, 2012), like U-curve or S-curve relationships, using the variance-based or PLS-based method. PLS methods also allow users to estimate parameters of both formative and reflective constructs, which is the case of our study, while covariance based methods only estimates parameters of reflective constructs.

Relationships between variables in economics and psychology are in majority non-linear, and the fact that our study uses both formative and reflective variables made WarpPLS 3.0 software the best choice for the analysis of the proposed structural model (Figure 2).

The estimates of the structural model analysed with WarpPLS are showed in Fig. No. 2 and include the results for the whole sample of 463 respondents using as resampling method bootstrapping with a number of 100 resamples and the Warp3 PLS regression algorithm, the most recommended for non-linear relationships between variables.

Fig. no.2 shows the path or β (Beta) coefficients between the model's constructs, which show the strength of the relationships between variables, their associated p-values, which shows that the relationships are significant for a $p<0.05$, and the R^2 (R squared coefficient of determination), which shows the percentage of variance of a criterion variable explained by its predictors or dependent variables.

All the hypotheses and their corresponding relationships between variables have p-values associated to the beta coefficients under .01, being statistically significant.

Perceived risks has the strongest influence on privacy concerns, with a β of 0.36 for a p under .01, thus the first hypothesis of the study (H1) being validated. Perceived benefits negatively correlated with privacy concerns, having a β of -0.21, supporting the second hypothesis (H2) and showing that the variable developed for this study, perceived benefits, was a good choice to be introduced in modeling users' perceived trust in online social networks. Perceived risks also negatively influenced perceived benefits, as it was hypothesized in the third hypothesis (H3), for a β of -0.24 and a p under .01.

Trust is significantly influenced by privacy concerns, validating the fifth hypothesis (H5) with a β of -0.27, and a p under .01. Perceived risks also has a strong negative correlation

with trust, as it was found in numerous empirical studies, confirming once again this relationship and validating our fourth hypothesis (H4). The newly introduced variable for the case of online social networks, perceived benefits, positively and significantly influences trust, with a β of 0.25, thus supporting our last hypothesis (H6). The cumulative effects of the three predictors: privacy concerns, perceived risks and perceived benefits explain in a proportion of 46% the users' trust in social network, trust having an R^2 of 0.46.
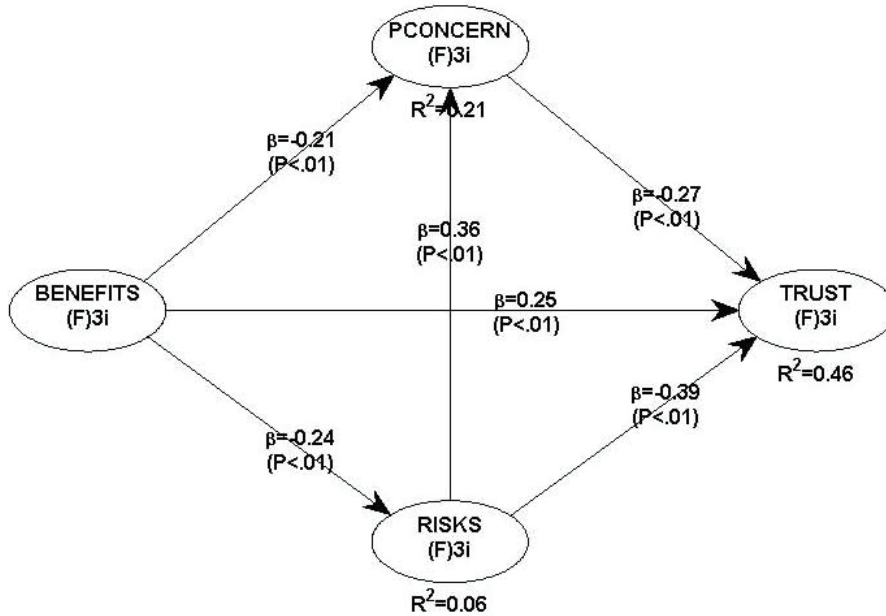

Figure no. 2: A Results of the PLS Analysis

5.4 Model fit

The proposed structural research model is also validated, having good model fit indices, the ARS index being 0.286 for a p<0.001, the most important measure of model fit, the AVIF being 1.139, much under the higher accepted limit of 5 (Kock, 2011), and the APC being 0.286 for a p<0.001. These three model fit indexes are another great advantage of WarpPLS, because unlike in covariance based SEM analysis, where there are a broad variety of model fit indices, in variance based SEM analysis methods usually these can't be provided (table 5).

Table no. 5: Model fit

APC=0.223, P<0.001	Good if p< 0.05
ARS=0.450, P<0.001	Good if p< 0.05
AVIF=1.858	Good if AVIF < 5

Conclusions

When modelling online trust, as a multi-dimensional construct that influences every aspect of interpersonal relationships, previous empirical researches were focused mainly on e-commerce issues related to the disclosure of information for buying online goods and services.

However, online trust should also take into consideration other types of websites, such as the growing trend of online social networks. Not only that these sites require information for registration, but they also encourage disclosure of personal and sensitive information, such as age, date of birth, place of living, major life events, information about work and education or professional skills.

As to disclose such sensitive information, users must trust online social networks at a both micro and macro level, as discussed in previous theoretical background section. But trust in online social networks is a complex construct, being influenced by many variables, among which we have studied the influence of only three predictors: perceived risks of using an online social network, perceived concerns regarding the use of an online social network and perceived benefits of using online social networks. As a result of the structural equation modelling, these three variables only account for a 46% variation in users' trust in online social networks, concluding that there are many other influences there to study in future research on the same topic.

Even though there are many other influences to be taken into account for increasing R^2 of trust in a structural equation model, the three variables chosen for the purpose of this study has proven to have a great influence on trust in online social networks.

The results of our study could be useful for both marketers and social media managers. The former should take into account privacy concerns and perceived benefits of social networking websites users and weight these against the quality of the data they gather online, which can affect their targeting and segmentation objectives in integrated marketing communication campaigns. Social media managers should take into account the delicate balance between privacy concerns and trust, which can greatly impact the success of their online services.

References

Bagozzi, R.P. and Yi Y., 1988. On the evaluation of structural equation model. *Journal of the Academy of Marketing Science,* 16(1), pp. 74-94.

Buzzom, 2012. *Social media users count reaches 940 Million.* [online] Available at: <www.buzzom.com/2010/03/social-media-users-count-reaches-940-million> [Accessed 10 July 2013]

Cases, A. S., Fournier, C., Dubois, P.-L. and Tanner, J. F. Jr, 201. Web Site spill over to email campaigns: The role of privacy, trust and shoppers attitudes. *Journal of Business Research*, 63, pp. 993-999.

CNN, 2012. *83 million Facebook accounts are fakes and dupes.* [online] Available at: <articles.cnn.com/2012-08-02/tech/tech_social-media_facebook-fake-accounts_1_facebook-accounts-facebook-profiles-facebook-estimates> [Accessed 09 July 2013].

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C., 2006. Privacy calculus model in e-commerce: a study of Italy and the United States. *European Journal of Information Systems*, 15(4), pp. 389-402.

Dinev, T. and Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), pp. 61-80.

Dinu, V., 2011. Corporate social responsibility – opportunity for reconciliation between economical interests and social and environmental interests. *Amfiteatru Economic*, XIII(29), pp. 6-7.

Eastlick, M. A., Lotz, S. L. and Warrington, P., 2006. Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust and Commitment. *Journal of Business Research*, 59, pp. 877-886.

eBizMBA, 2013. *Top 15 most popular social networking sites*. [online] Available at: <www.eBizMBA.com/articles/social-networking-websites> [Accessed 10 July 2013].

eMarketer, 2012. *Where in the World Are the Hottest Social Networking Countries?* [online] Available at: <http://www.emarketer.com/Article/Where-World-Hottest-Social-Networking-Countries/1008870> [Accessed 10 July 2013].

Featherman, M.S. and Pavlou, P.A., 2005. Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), pp. 451-474.

Fornell, C. and Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 48, pp. 39-50.

Grabner-Krauter, S. and Bitter, S., 2013. Trust in online social networks: A multifaced perspective. Forum for social Economics. [online] Available at: <http://www.tandfonline.com/doi/full/10.1080/07360932.2013.781517#.UmBf1_k71U Y> [Accessed 12 July 2013].

Grant, I.C., 2005. Young peoples' relationships with online marketing practices: an intrusion too far?. *Journal of Marketing Management*, 21(5), pp. 607-623.

Hair, J.F., Anderson, R.E., Tatham, R.L. and Black W.C., 1998. *Multivariate Data Analysis*, 5th edition. New Jersey: Prentice Hall.

Han, P. and Malaren, A., 2002. Do consumers really care about online privacy? *Marketing Management*, 11(1), pp. 35-38.

HTTP State Management Mechanism, 2011. [online] Available at: <http://tools.ietf.org/html/rfc6265#section-3> [Accessed 09 July 2013].

Insites, 2011. *347 million Europeans use social networks (results of our global social media study)*. [online] Available at: <http://Blog.insites.eu/2011/09/14/347-million-europeans-use-social-networks-results-of-a-global-social-media-study > [Accessed 10 July 2013].

InternetSafety101, 2012. Social Networking Stats. [online] Available at <www.internetsafety101.org/Socialnetworkingstats.htm> [Accessed 08 July 2013].

Ionescu, L., Lăzăroiu, G. and Şerban, S., 2013. A Theory of the Availability and Level of Consumer Protection in Online and Mobile Payments for Public Economic Services. *Amfiteatru Economic*, XVI(34), pp. 1-16.

Jarvenpaa, S.L., Knoll, K. and Leidner, D.E., 1998. Is anybody out there? Antecedents of trust in global virtual teams. *Journal of Management Information Systems*, 14(4), pp. 29-64.

Jarvenpaa, S.L., Tractinsky, N. and Vitale, M., 2000. Consumer trust in an Internet store. *Information Technology and Management*, 1(1/2), pp. 45-71.

Jewell, D.V., 2011. *Guide to evidence-based physical therapist practice.* 2ⁿᵈ edition. Ontario: Jones & Bartlett Learning.

Josang, A. and Lo Presti, S., 2004. Analyzing the relationship between Risk and Trust. *Lecture Notes in Computer Science*, 2995, pp. 135-145.

Kaplan, A.M. and Haenlein, M., 2010. *Users of the world, unite! The challenges and opportunities of Social Media.* Business Horizons, 53(1), pp. 59-68.

Kenyon, H.S., 2010. Cybercriminals find new ways to exploit vulnerabilities. *Armed Forces Communication and Electronics Association*, pp. 23-27.

Kock, N., 2011. Using WarpPLS in e-Collaboration studies: Descriptive statistics, settings, and key analysis results. *International Journal of e-Collaboration*, 7(2), pp. 1-18.

Kock, N., 2012.WarpPLS 3.0 User Manual. Laredo, Texas: ScriptWarp Systems.

Krasnova H., Gunther O., Spiekermann S. and Koroleva K., 2009. Privacy Concerns and Identity in online social networks. *Journal of Identity in the Information Society*, 2(1), pp. 39-63.

Krishnamurthy, B. and Wills, C.E., 2009. On the Leakage of Personally Identifiable Information via Online Social Networks. In: *2ⁿᵈ ACM Workshop on Online Social Networks*, Barcelona, August 17, pp. 7-12.

Kuan-Yu, L. and Hsi-Peng, L., 2011. Why peope use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior*, 27(3), pp. 1152-1161.

Lai, L.S. and Turban, E., 2008. Groups' formation and operations in the Web 2.0 environment and social networks. *Group Decision and Negotiation*, 17(5), pp. 387-402.

Lee, C.H. and Cranage, D.A., 2011. Personalization-privacy paradox: The Effects of Personalization and Privacy Assurance on Customer Responses to Travel Web sites. *Tourism Management*, 32, pp. 987-994.

Liao, C., Liu, C.-C. and Chen, K., 2011. Examining the Impact of Privacy, Trust and Risk Perceptions beyond Monetary Transactions: An Integrated Model. *Electronic Commerce Research and Applications*, 10, pp. 702-715.

Magid, L., 2012. Facebook Users Becoming privacy Savvy. *Forbes Magazine.* [online] Available at: <www.forbes.com/sites/larrymagid/2012/02/24/facebook-users-becoming-more-privacy-savvy > [Accessed 10 July 2013].

Marketing Charts, 2007. Social Network Users Enter False Personal Info to protect identity. [online] Available at <www.marketingcharts.com/interactive/most-social-network-users-enter-false-personal-info-to-protect-identity-1691> [Accessed 09 July 2013].

McCole, P., Ramsey, E. and Williams, J., 2010. Trust Considerations on Attitudes towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns. *Journal of Business Research*, 63(9-10), pp. 1018-1024.

McKnight, D.H. and Chervany, N.L., 2002. What trust means in e-commer customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6(2), pp. 35-59.

McKnight, D.H., Cummings, L.L. and Chervany, N.L., 1998. Initial trust formation in new organizational relationships. *The Academy of Management Review*, 23(3), pp. 473-490.

McKnight, D. H., Lankton, N. and Tripp, J., 2011. Social networking information disclosure and continuance intention: A disconnect. In: IEEE Computer Society, *System Sciences (HICSS) 44th Hawaii International Conference,* Koloa, Kauai, 4-7 January 2011.

Meinart, D. B., Peterson, D. K., Criswell, J. R. and Crossland, M. D., 2006. Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce Organization*, 4(1), pp. 1-17.

Moise, D., Georgescu, B. and Zgură, D., 2012. Strategies for Interactive Communication, with External and Internal Stakeholders, in Events' Marketing. *Procedia - Social and Behavioral Sciences*, 46, pp. 5361-5365.

Nunally, J.C. 1978. *Psychometric Theory*. 2nd edition. New York: McGraw Hill.

Palmer, D.E., 2005. Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis Significance of Internet Marketing Practices. *Journal of Business Ethics*, 58, pp. 271-280.

Pan, Y. and Zinkhan, G.M., 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, 82(4), pp. 331-338.

Pelău, C. and Bena, I., 2010. The risk perception for consumer segments in e-commerce and its implication for the marketing strategy. *Amfiteatru Economic*, XII(28), pp. 373-387.

Popescu, I.C., Dumitru, I., Vegheş, C. and Kailani, C., 2013. Marketing Communication as a Vector of the Romanian Small Businesses Sustainable Development. Amfiteatru Economic, XV(Special Issue 7), pp. 671-686.

Privacy Rights, 2010. *Fact Sheet 35: Social Networking Privacy: How to be safe, secure and social*. [online] Available at: <www.privacyrights.org/social-networking-privacy> [Accessed 08 July 2013].

Rust, R. T., Kannan, P. K. and Peng, N., 2002. The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30, pp. 455-464.

The Economist, 2011. *Europe's social media hotspots. Where networking works*. [online] Available at <www.economist.com/blogs/dailychart/2011/07/europe%E2%80%99s-social-media-hotspots > [Accessed 08 July 2013].

Wikipedia, 2013. *List of social networking sites*. [online] Available at <en.Wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_users> [Accessed 10 July 2013].

Youn, S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), pp. 389-418.

Young, A.L. and Quan-Haase, A., 2009. Information Revelation and Internet Privacy Concerns on Social Network Sites: A case Study of Facebook. C&T'09, June 25-27, 2009, University Park, Pennsylvania, USA, pp. 265-273. [pdf] Available online at: <http://sozio-informatik.net/fileadmin/IISI/upload/2009/p265.pdf> [Accessed 08 July 2013].

Xu, C., 2012. Internet of things in service innovation. *Amfiteatru Economic,* XIV(Special No.6), pp. 698-719.