Facebook: The Risk-Taking Attitude amongst Emerging Adults

Sayed Enayat Sayed Ally, Craig Blewett and Brett van Niekerk
Discipline of Information Systems and Technology
University of KwaZulu-Natal
Westville, South Africa
se.sayedally@gmail.com, blewett@ukzn.ac.za, vanniekerkb@ukzn.ac.za

***Abstract*— This study investigates students, or "Emerging Adults", in the South African tertiary environment; and their risk-taking attitudes towards Facebook. The general risk attitude and behaviour of students has been researched from various angles and even in online and social environments as well. This study however focuses on Facebook due to its popularity and widespread adoption amongst students and particularly the disclosure of Personal Identifiable Information (PII) in the South African context. Preliminary results reveal that South African students tend to divulge PII on their profiles and are therefore considered as risk-takers. Students tend to disclose various aspects of their life, and this risk attitude has also been found to be influenced by age; wherein younger students choose to disclose PII such as their phone number more easily in comparison to older students. Whilst students have adopted a risk-taker attitude on Facebook by opting to disclose PII, there is a dichotomy between this attitude and their choice of Facebook friends access privileges; this is evidence of the gap between students' risk-taking attitude and their reported behaviour.**

Keywords- Facebook, Risk-Taking Attitude, Personal Identifiable Information

I. INTRODUCTION

"Is it a good idea to set one's hair on fire?", was a question posed in a study related to risk-taking [1] wherein the participating adolescents took longer than adults to answer whether or not it was a good idea. It is no surprise that studies in the area of risk-taking have revealed that adolescents exhibit a high risk-taking attitude as compared to adults and children [2]. These high levels of risk-taking are further intensified in the company of peers for both adolescents and adults [3]. While the example above is physical risk, many of the issues with risk today occur online. Most notable amongst the online environments where risk-taking behaviour is exhibited is Facebook. This study looks at Personal Identifiable Information that is disclosed by South African students in the Facebook environment.

In June 2013 it was reported that there was an 83% increase from 2012 in South African Facebook users effectively taking the number of users up to 9,6 million [4]. According to Social Bakers [5], South Africa has a gender ratio, 49% male to 51% female, and the majority of Facebook users fall between the ages of 18 and 34. A local study [6] carried out in 2011 indicated that 93% of South African students log on to Facebook at least once a day and spend an average of 3.5 hours per day on Facebook. These findings indicate that the younger generation spends a significant amount of time on Facebook. A study in the United States reported similar high usage results wherein students have been found to use Facebook for close to 3 hours per day and the mean age of these users was age 20 [7].

The term "Emerging Adulthood" is adopted in this study to conceptualize the period of individuals' lives that span roughly from 18 till 25. Arnett [8] states that previously used classifications were more suited towards the middle of the 20th century as people of this age group were married and in jobs at the age of 20; however modern lifestyles have changed and this type of classification does not strictly hold true because of different phenomena such as Individualization [7] amongst others.

Furthermore this period of life is associated with many life changing decisions that individuals have to make, and therefore is demographically diverse because of the exploration and change that is associated in this period. It is also stated that developing economies allow for individuals in this age group to continue exploration and change especially in industrialized societies. South Africa has been identified as a country that is diverse [9] and a young industrialized country [10]. It can therefore be said that within South African society, individuals are influenced by the dynamic environment around them and in–turn these individuals impact society and their immediate environment. This study adopts the classification of Emerging Adults to describe students for the above reasons and the fact that university students satisfy the context of this classification in terms of risk-taking decision making.

II. SOCIAL NETWORK SYSTEMS AND FACEBOOK

The popularity of social network systems (SNS) has increased significantly since the boom of Social Media and its close affinity with Web 2.0 technologies. Facebook which is used through-out the world has been at the forefront of the social network boom [7]. The fact that Web 2.0 is grounded in information sharing and collaboration, has led to the popularity of SNS's such as Facebook wherein creating social networks is encouraged [11]. Online profiles form a common part of modern culture and most online users are willing to or have already created online profiles on social networks for various reasons. The nature of online profiles are such that

they leave behind a digital trail that can be linked back to the user [33,34]. Research has indicated that users are aware of the risk that they can be identified physically using their social network profile [12]. Most users however do not fully understand the real cost of privacy associated with social networks but nevertheless place trust in social network sites. While there is no direct monetary cost associated with creating social network profiles, by sharing personal content, users are making a trade-off between their private and public life [13]. As users share their information online so they close the gap between their private and public life.

Privacy and Confidentiality are at risk from threats that affect Facebook security as described in the Security Threat Matrix (STM) by Leitch & Warren [18]. They further explain that these threats may arise from the Privacy and Confidentiality security dimension; which include the use of third-party applications that use unencrypted messages to transfer data, third-party applications recording conversations without expressed consent and also the unintentional alteration of privacy settings that release user information. These studies therefore indicate that issues of Trust, Privacy risk, Risk-Taking and Identity Disclosure exist within Internet social network systems.

Facebook is at the center of online social networks and boasts more than 1.23 billion users worldwide [14]. Facebook has grown from a campus wide project to a giant on the World Wide Web since its inception in 2004. Founder, Chairman and CEO of Facebook, Mark Zuckerburg, has successfully turned what initially was a campus project, into a successful business that connects people from around the world [14]. Boasting an active user base of more than 1.23 billion active users worldwide at December 2013 from just 1 million users in 2004, Facebook's growth has been tremendous [14]. Despite the continued efforts to increase security and security awareness [15], there are still numerous threats that arise from sharing Personal Identifiable Information (PII) online. Facebook as a result of its huge user base has been the focus of numerous trust and privacy issues which are discussed at length throughout the Internet community and in scholarly papers [15, 24].

III. Personal Identity Information

One of the main threats of the online world is poor Internet privacy control [12]. By definition, "Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences." [19]. Personal data can be broken down into two different types of data, Personal Identity Information (PII) and non-Personal Identity Information. PII is any information that can be used to identify an individual e.g. financial account numbers and medical information [20]. An example of non-PII would be information such as a visitor's behaviour on a website. PII in the wrong hands poses a threat to users' security as discussed below.

Aïmeur, Gambs and Ho [21] identified three major risks associated with privacy and social networks, namely:

- Security Risks
- Reputation and Credibility Risks and
- Profiling Risks.

Security Risks are online attacks such as identity theft, phishing and scams. These security risks arise as a result of the large amounts of data that can be found on SNS's. The damage done by criminals is extensive and lucrative, in 2009 alone 11.1 million people fell victim to Identity Theft that resulted in a $54 billion cost in the US [22].

The second risk applies to Reputation and Credibility, and is an important factor in society as it represents the social evaluation of the public view of a person [23]. The credibility of a person is judged by the information they post on SNS's, and in many cases this information has led to negative employee relations and has also impacted peoples' careers in a negative manner [21]. Smith & Kidder [24] state that young adults may not understand the gravity of the risks associated with self-disclosure on SNS's.

The third risk, profiling, refers to the recording and classification of behaviours. This is a common practice where information is collected, often without consent, to build a profile in order to sell products [21] or undertake some form of malicious phishing scheme or other forms of attack on the individual.

IV. Methods

A. Objective

The main objective of this paper is to investigate the Facebook risk-taking attitudes that South African students adopt. This will be carried out by analysing users' attitudes; or their "readiness of the psyche to act or react in a certain way" [36]. By assessing the attitudes of users to risk it is possible to profile user risk attitudes as risk-averse, risk-neutral or risk takers.

B. Respondents and Procedures

The chosen population for this study is the University of KwaZulu Natal (UKZN) -Westville campus student population. The majority of university students fall into the 18 to 30 age category. This chosen population is in line with similar studies in this area of risk-taking wherein students form the primary source of data [25]. Students were handed surveys at the convenience of the researcher and they participated voluntarily; a quantitative approach was chosen for this study and the data was collected in a single time period. Surveys were printed and handed out in campus computer labs and also in lecture venues. A total number of 330 surveys were collected of which 8 were found to be unfit for statistical analysis. Therefore our sample data consisted of 322 surveys.

C. Measures

The constructs used in the survey are broken up into two sections and are described as follows. The First Section used in the survey comprises of nine Yes/No questions. These questions ask students whether or not they share certain types of information on their Facebook profile. The more "Yes"

answers chosen indicate a higher risk profile of the respondent. Some of the questions posed under this section enquire as to whether students share information such as their home address and images of themselves on their profile. The age demographic was cross analysed to these nine questions for any correlations that exist by means of chi-square tests.

The second section seeks to answer how much of viewing access a student allows to their family friends and strangers. This set of questions basically asks if a student is OK with certain people accessing their profile. The controls used to configure these permissions aren't easily setup and have varying configurations for different levels of privacy; therefore students' attitude in answering these questions will vary because of the above mentioned reasoning [12].

V. Discussion of Results

A. *Demographics*

Our sample consisted of various students attending University of KwaZulu Natal Westville campus and as such, the age demographic is reflected below.

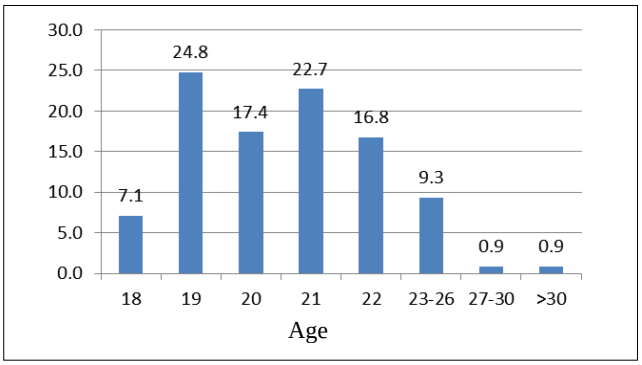

Figure 1. Age Demographics

Fig. 1 (Age Demographics) reveals that more than 70% of students that participated in this study fall within ages of 19 and 22. This result is not surprising as the majority of students attend university after leaving school, and this places them well within the above age group. As mentioned previously on the topic of Emerging Adults, the previous classification systems used to describe adults and adolescents in the late 1900's reported that individuals entered the working class at the age of 20 and were married at this age. The above ages depict a group that portrays attributes of Emerging Adults in modern society; furthermore, the fact that these respondents are furthering their education is testament to the fact that they value their future careers. This is also an attribute of Emerging Adults wherein they choose to enhance their career prospects by means of tertiary education.

B. *Facebook PII Disclosure*

The amount of PII that students disclose and also whether students are classified as low, medium or high risk takers is analysed in this section. There were nine questions about what types of information students share on their Facebook profile and are as follows:

Q1 – Do you allow anyone to view your complete profile?
Q2 – Do you include an image of yourself on your profile or is your profile image a picture of yourself?
Q3 – Do you include your email address on your profile?
Q4 – Do you include your Blackberry Messenger pin or other IM details on your profile?
Q5 – Do you include your phone number on your profile?
Q6 – Do you include your home address on your profile?
Q7 – Do you include information about your interests on your profile?
Q8 – Do you write on other peoples profile pages?
Q9 – Do you use your real name on Facebook?

Figure 2. Section One Survey Questions

The system developed to classify students is as explained hereafter. A student may answer Yes or No to any of the above questions. The distribution of "Yes" responses chosen by students is then calculated and grouped according to the number of "Yes" options selected. Therefore when we look at the following table (Table I) it shows that 26 respondents in this study have answered "Yes" to sharing 3 types of Personal Identifiable Information on their profile (Lower Risk).

TABLE I.

Number of "Yes" options	Frequency Distribution	Risk
1 Yes	2	Low Risk
2 Yes's	10	
3 Yes's	26	
4 Yes's	58	
5 Yes's	100	
6 Yes's	64	
7 Yes's	32	
8 Yes's	28	
9 Yes's	2	High Risk

Once the distribution of the sum of Yes choices is determined, the calculation of the average score was carried out. The result mean value was 5.2236 and this is considered higher than average and is equivalent to a medium to high degree in terms of risk score; and in this case the 5.2236 score is akin to medium to high risk-taking attitude.

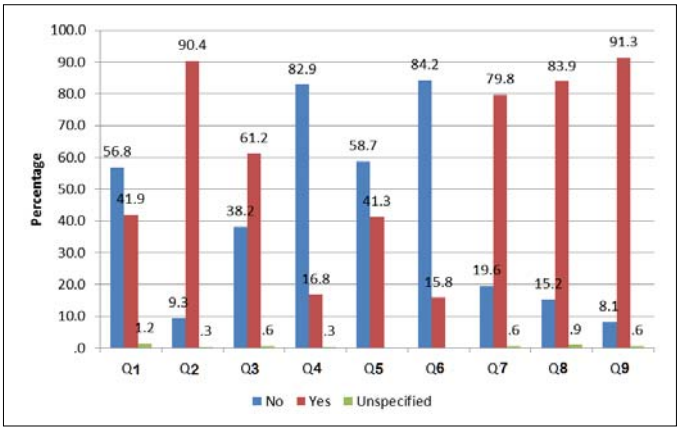

Figure 3. Section One Frequency Distribution

Figure 3 (Section One Frequency Distribution) depicts the results of both the Yes and No questions posed to students on their attitude towards sharing their Personal Identifiable Information on their Facebook profile. The results depict the areas in which students are more comfortable in taking risks on Facebook.

Questions 2, 3, 7, 8 and 9 show the resounding Yes option selected, with more than 61% choosing Yes for each question. These questions about PII on their own are difficult, but not impossible, to actually use to create a profile on a person. In this study however more than one item of PII is displayed over students' Facebook profiles. By attaching an image, a name and participating in posting content on different walls, a user leaves oneself at risk of profiling by attackers. As a result of the above choices in PII disclosure, UKZN students are considered to be taking a medium to high degree of risk in their Facebook demeanor. However it should be noted that this result has been observed amongst students in other studies as well, wherein students opt to disclose their personal details whilst applying very little caution [25, 31, 32].

According to a study that investigates risk and social network sites, age was found to be a contributing factor towards risk, more especially between the ages of 18 and 24 [12]. The reasons found in that study explain that risk behaviour on social networks is as a result of poor levels of privacy risks and also complacency in sharing their profile information. The analysis of age as an impacting variable has indicated that age does influence some of the decisions to disclose certain PII in this study. For instance in the question asking whether or not students disclose their phone number on Facebook, 19 year old students were found to have said yes as compared to 22 year old students that indicated no they did not. This display of maturity is further enforced by the fact that students between the ages of 23 and 26 opt to share their interests as opposed to 19 year olds who opt not to share this information. It can therefore be said that younger students are more inclined towards revealing PII on their Facebook profile that promotes communication with them. This attitude can be percieved as risky if all users can view this information and if attackers use it to their advantage.

41.9% of students reported in question one (see Figure 3) that they allow anyone to view their complete profile which is considered highly risky. Moreover, students were disinclined towards allowing their profile to be viewed by anyone and this result shows greater than 50% students opted to choose No. This result indicates for some reason that they are not comfortable with just anyone viewing their profile. This result also does not fit the attributed Risk-Taker attitude found in the above Facebook Risk-Taking attitude score.

However students were questioned about their knowledge and usage of privacy controls, and only 13% (40 students) reported to have known what privacy controls are and even fewer students 4% (12 students) reported to actually using them. Whilst the information of students is shared on their own Facebook wall, there exists a risk that students face in that they do not actively use privacy controls; even whilst they are aware of them. In this case it is possible that not only do their trusted friends have access to their information, but also any person with a Facebook account. Furthermore, a related study [38] in the dynamics of Facebook befriending has reported that students also add Facebook friends despite not having met them physically. Herein lies a risk of information being disclosed to strangers which is also coupled with the risk of "friends-of-friends" viewing a person's information, even though students answered that they do not allow complete viewing rights to anyone.

It is not certain then as to whether this contradictory risk-averse attitude for this question can be linked to risk-taking at all, and whether this result is such because of some other reason. The first possible explanation to this may actually exist in the profile types that students assign to their Facebook contacts; for instance, one has the ability to restrict the information that every contact on their list actually sees. In this case the contacts of students may not be limited to just their friends, but also to strangers as contacts and these contacts may be limited in their viewing privileges. The following graph (Figure 4 – Profile Access) provides data to substantiate this theory, wherein students are asked as to who they are "OK" with accessing their profile. It can be seen that when asked whether it is OK that friends and family can access their profile, greater than 50% of students agree. In contrast, when the same question is asked with strangers in place of family or friends, there is a resounding disagreement of greater than 70% students opting in the negative.

Therefore, whilst this study looks into the factors that affect the risk of students, there are other socio-emotive factors that seem to be at work in the Facebook friendship dynamics of students. It is well known that students follow social normative behaviour especially in a campus environment. Aronson, Wilson and Akert [31] state that in order to be liked and accepted by others, we are influenced by them and conform.

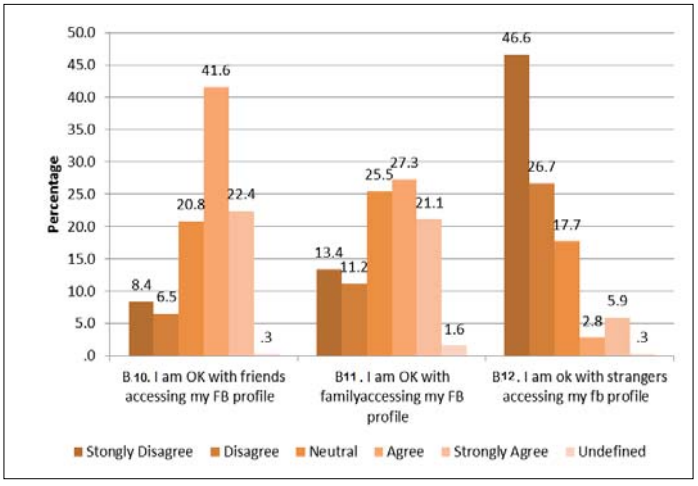

Figure 4. Profile Access

The second possible and more plausible explanation could be that students' perceptions of their behaviour and their actual actions differ because of the mental conditioning from various influences such as social networks. Whilst students may be aware of the dangers of revealing PII and are in this case are disinclined to allow access to strangers, their actual conduct

on Facebook is to reveal PII. Therefore students perceive that they are safe and this is evident in their choices in the survey results, however in reality their PII disclosure choices leave them at risk.

The medium-to-high risk-attitude that UKZN Westville students have adopted is inline with results of similar studies in this area [26,27,28]; Studies have reported that university students are heavy users of Facebook and tend to reveal a great deal of their PII on social networks. Moreover, whilst students display risky attitudes towards sharing their information online, research inline with this study reveal that students don't draw a link between sharing their personal information on their social profiles and their privacy concerns; they actually rely on restricted viewing mechanisms as a solution to maintaining their profile [29].

Whilst this may be effective in warding off unwanted strangers accessing their profile, it still means that students' personal information is stored online. It has been reported that individuals also choose to accept friendship invitations from unknown profiles [37,38]; apart from the fact that a person leaves their profiles open to scrutiny from would be attackers, it just highlights the risk-taking behaviour that this study focuses on. What may seem to be a friendly invitation to an unwary person may just turn out to be an attacker attempting to access an individual's information. Furthermore, there are reports of attackers falsifying accounts of individuals and befriending people on Facebook, all in an attempt to carry out various attacks on users [30].

VI. Conclusion

As modern psychology continues to investigate the risk-attitudes, it is evident that South African students in this study fit into this classification of Emerging Adults. The societal normative values surrounding university graduates include finding a job and progressing in their career. These students portray the risk-taking attitude found in other studies and conform to the image generally associated with risky adolescent individuals.

The immediate concern with this attitude is that students at tertiary level are transitioning into the workforce, and therefore bring with them a risky attitude into the workplace; furthermore the fact that many students choose to not utilize privacy controls increases the risk associated with PII disclosure. The disclosure of PII via Facebook is an avenue that attackers seek to exploit in order to conduct attacks. This exposes emerging adults, and potentially even the firms they will be employed at, to the risks associated with this risky attitude. The age of students also impacts the types of information that students tend to disclose; with younger age groups opting to disclose revealing Information such as their phone number in comparison to older students that opt to disclose PII that may not so easily be manipulated by attackers.

The perceived safety awareness of students therefore does not translate into their actual conduct on Facebook. Students believe that they are cautious when in reality their actions are actually putting them potentially at risk to attacks. Thus the attitude of students with regards to risk is not inline with their reported behaviour.

In further research the continuation of this study would delve into factors that seek to explain students' risk attitude. One of the factors that merits analysis is the effect of gender in risk attitudes, as gender has been shown to be a significant factor in similar studies [17,25]. Furthermore a qualitative study would aid in revealing the reasoning of students and their attitude adoption.

References

[1] Baird. A, Fugelsang. J, and Craig. M. "What were you thinking"?: An fMRI study of adolescent decision making. Department of Psychological and Brain Sciences. Hanover: Dartmouth College, 2005.

[2] Steinberg, L. Risk Taking in Adolescence. Association for Psychological Science, 2007, pp.55-59

[3] Gardner, M., & Steinberg, L. Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study. Developmental Psychology, 2005, pp.625-635.

[4] Gillian Meier. Social Media Briefing Conference South Africa. http://www.bluemagnet.co.za/blog/the-state-of-social-media-in-south-africa-2013. 2013. Accessed 29 April 2014

[5] Social Bakers. South Africa Facebook Statistics. http://www.socialbakers.com/facebook-statistics/south-africa 2012. Accessed 2012

[6] Shambare. R, Rugimbana. R, & Sithole, N. The Facebook Phenomenon: Social Networking among South African Students. 13th IAABD Conference Proceedings. Edmonton, Canada. 2011

[7] Ellison, N, Steinfeld, C, and Lampe, C. The Benefits of Facebook "Friends:" Social Capital and College Students' use of Online Social Network Sites. Computer Mediated Communication. 2007

[8] Arnett, Jeffrey Jensen. Emerging Adulthood: What Is It, and What Is It Good For? Society for Research in Child Development, 1(2), 2007. pp. 68-73.

[9] John HE Maré, Economic Diversification in Africa - A Review of Selected Countries, NEPAD 2010

[10] What is Industrialisation?, South African History Online. http://www.sahistory.org.za/archive/what-industrialisation. N.D. Accessed 2014

[11] Mcafee, A. Enterprise 2.0: New Collaborative Tools for your organisations toughest challenges. Harvard Business Edition. 2009

[12] Lane, M., & Shrestha , A. An empirical analysis of SNS users and their privacy and security awareness of risks associated with sharing sns profiles (online identities). The 11th International Conference on Electronic Business. Bangkok, Thailand. 2011

[13] Rosenblum, D. The Privacy Risks of Social Networking Sites. IEEE Security & Privacy. IEEE Computer Society.2007 pp. 40-49

[14] Facebook.com, http://newsroom.fb.com/. N.D Access Date 2012

[15] Maximilien, E., Grandison, T., Liu, K., Sun, T., Richardson, D., & Guo, S. Enabling Privacy As a Fundamental Construct for Social Networks. International Conference on Computational Science and Engineering. IEEE Computer Society 2009

[16] Burt, B. Definitions of risk. Journal of Dental Education. 2001;65:1007–1008.

[17] Nicole L. Muscanell, Rosanna E. Guadagno. Make new friends or keep the old: Gender and personality differences in social networking use.Computers in Human Behavior, 28(1), January 2012, Pages 107–112

[18] Leitch, S., & Warren, M. Security Issues Challenging Facebook. Australian Information Security Management Conference. Perth. 2009

[19] Techopedia. (N.D). Internet Privacy. http://www.techopedia.com/definition/24954/internet-privacy. Accessed 2014

[20] PII. (N.D). Personal Identifiable Information. The University of California. Accessed 2014

[21] Aïmeur, E., Gambs, S., & Ho, A. Towards a Privacy-enhanced Social Networking Site. International Conference on Availability, Reliability and Security. IEEE. 2010

[22] Vamosi, R., Monahan, M., & Kim, R. 2010 Identity Fraud Survey Report. 2010

[23] Dingledine, R., Mathewson, N., & Syverson, P. Reputation in Privacy Enhancing Technologies. 2002

[24] Smith, W., & Kidder, D. You've been tagged! (Then again, maybe not):Employer s and Facebook. Elsevier. 2010

[25] Fogel, Joshua, & Nehmad, Elham. Internet Social Network Communities: Risk Taking, Trust and Privacy Concerns. *Computers in Human Behaviour, 25,* 2009. pp.153-160.

[26] Acquisti, Alessandro, & Gross, Ralph. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Paper presented at the Privacy Enhancing Technologies Workshop (PET). 2006

[27] Gerrard, Meg, Gibbons, Frederick X, Houlihan, Amy E, Stock, Michelle L, & Pomery, Elizabeth A. A dual-process approach to health risk decision making: The prototype willingness model. Developmental Review, 28(1), 2008. pp.29-61.

[28] Sunstein, C.S. Adolescent risk-taking and social meaning: a commentary. 2008

[29] Tufekci, Zeynep. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society, 28(1), 2008. Pp.20-36.

[30] Jacoby, David. Fake or hijacked Facebook accounts used in scams to steal money are on the rise. https://www.securelist.com/en/blog/208193413/Fake_or_hijacked_Facebook_accounts_used_in_scams_to_steal_money_are_on_the_rise. 2012. Accessed 2014

[31] Aronson, E, Wilson, T. D, & Akert, R. M. Social Psychology (5th ed.). Upper Saddle River, NJ: Prentice Hall. 2005

[32] Christofides, Emily, Muise, Amy, & Desmarais, Serge. Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? Cyberpsychology & Behavior, 12(3), 2009. pp.341-345.

[33] Taraszow, Tatjana, Aristodemou, Elena, Shitta, Georgina, Laouris, Yiannis, & Arsoy, Aysu. Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook™ profiles as an example. International Journal of Media and Cultural Politics, 6(1), 2010. pp.81-102.

[34] Mary Maden. Privacy management on social media sites. Pew Research Center's Internet & American Life Project. 2012

[35] Anshu Malhotra, Luam Totti, Wagner Meira Jr., Ponnurangam Kumaraguru, Virg´ılio Almeida. Studying User Footprints in Different Online Social Networks. 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. 2012.

[36] Carl Jung. Psychologische Typen. Gesammelte Werke. Olten u.a. 1971

[37] SOPHOS. Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. 2014, from http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx 2007. Accessed 2014

[38] Jesse P. Mendez, John Curry, Mwarumba Mwavita, Kathleen Kennedy, Kathryn Weinland, Katie Bainbridge. To Friend or Not to Friend: Academic Interaction on Facebook. International Journal of Instructional Technology & Distance Learning, 6(9), 2009.