Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

An Empirical Investigation of Factors that Influence Individual Behavior toward Changing Social Networking Security Settings

C. Bryan Foltz[1], Henry E. Newkirk[2] and Paul H. Schwager[3]

[1] University of Tennessee at Martin, Management, Marketing, and Information Systems Department, Martin, TN, USA, foltz@utm.edu
[2] East Carolina University, Department of Management Information Systems, Greenville, NC, USA, newkirkh@ecu.edu
[3] East Carolina University, Department of Management Information Systems, Greenville, NC, USA, schwagerp@ecu.edu

Received 23 January 2014; received in revised form 30 July 2015; accepted 14 August 2015

Abstract

While the use of social networking sites continues to rise, security continues to be an important issue. This issue often results when many users do not change their social networking security settings. Such behavior leaves vast amounts of data vulnerable to criminal activities. This study utilized the Theory of Planned Behavior to examine factors that impact users' behaviors regarding changing their social networking security settings. This research found support for six of the eight hypotheses. Results showed that Attitude (H1), Subjective Norm (H2), and Perceived Behavioral Control (H3) predicted Behavioral Intention. Behavioral Intention (H4) positively influenced Behavior. Apathy (H6) negatively predicted Attitude while Perceived Behavioral Control (H7) positively influenced Social Trust. Finally, Perceived Behavioral Control did not predict Behavior (H5) and Social Trust did not impact Behavioral Intention (H8). These findings have future implications for research and practice.

Keywords: Apathy, Social trust, Social networking sites, Theory of planned behavior, Privacy, Security, Privacy, Security

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

1 Introduction

Social networking continues to grow at a phenomenal rate today. In fact, the growth rate is quite astounding. For example, Facebook, founded in February 2004, reported over 1.44 billion monthly active users as of May 2015 [21]. Twitter, created in March 2006 [12], reached 500 million accounts in June 2012 [47], and has 302 million monthly active users [53]. LinkedIn, which began in 2002, has over 364 million registered members [38]. While these statistics are impressive, it does not keep new entrants away. Platforms such as Pinterest, Instagram, Tumblr and Vimeo are changing how social networking is done while stalwarts such as MySpace are reinventing themselves in an attempt to remain competitive.

Unfortunately, security remains an issue, and all social networking users face security threats. These risks range from unexpected privacy violations to worms and viruses. In addition, concerns with privacy have been linked to social media fatigue [9]. Fortunately, most social networking sites allow users to adjust security and privacy settings to help avoid these threats. Unfortunately, many users fail to make these adjustments. A recent study notes that many users do post private (*risky*) information [54]. This study will examine individual alteration of social networking security settings (without regard to the direction or correctness of those alterations) utilizing a theoretical model of human behavior. Figure 1 shows the research model.

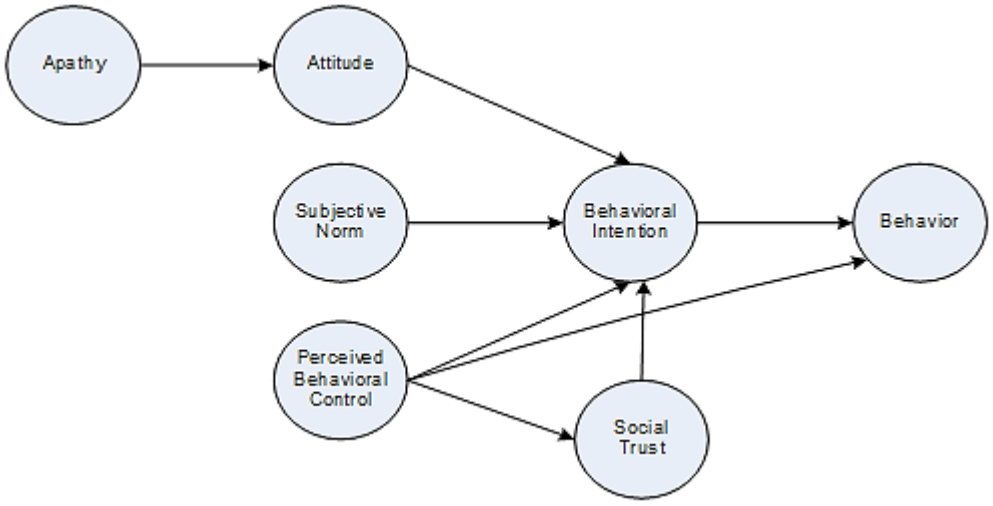


Figure 1: Research model

The structural model above contains latent variables or constructs (circles) and paths (arrows). Paths show relationships between latent variables. Latent variables are ideas that cannot be measured directly [16]. Manifest or Observable variables (not shown above) serve as measures that represent latent constructs. The model has two types of latent variables, namely endogenous and exogenous. Exogenous variables do not have paths or arrows pointing at them. On the other hands, endogenous variables have paths pointing toward them [32].

The next section of this paper discusses the relevant literature. It is followed by the research hypotheses section. The subsequent section examines the methodology used for the study. The results of the study are then presented followed by a discussion of the findings. The paper concludes with sections that discuss limitations and future research, implications for practice and conclusion.

2 Literature Review

In addressing the literature, we examine multiple research streams that are associated with this study. We first take a broad look at the Theory of Planned Behavior (TPB). From there we take a more focused look at TPB and how it specifically applies to information systems misuse. Finally, we examine the literature related to Apathy and Social Trust.

2.1 Theory of Planned Behavior

The Theory of Planned Behavior (TPB) suggests that human behavior can be explained and predicted within specific contexts based upon individual intention to commit behavior, along with individual perceptions of personal control over performing that behavior [1]-[2], [19], [42], [44]. The TPB suggests that behavior is a function of beliefs or information relevant to the specified behavior. Although individuals may have multiple beliefs, only a few salient

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

beliefs can be dealt with at any given time. These beliefs are thus the primary determinants of intentions and actions [4], [19]. These beliefs link the specified behavior with the outcomes generated by performing that behavior, as well as with any potential costs generated by performing the behavior [4], [19].

2.1.1 Intentions

Intentions, which indicate the amount of effort individuals are willing to exert to perform a given behavior [2], "are assumed to capture the motivational factors that influence a behavior" [8] p. 286. Intentions are formed from three factors: Attitude toward the Behavior, Subjective Norms, and Perceived Behavioral Control [1].

2.1.2 Attitude

Attitude toward the Behavior (A) captures an individual's positive or negative perceptions of performing the behavior- an Attitude is a disposition to respond favorably or unfavorably to an object, person, institution, or event [1]. Attitude is a latent variable formed from behavioral beliefs [4] regarding the expected outcome of the behavior and an evaluation of those outcomes [1]. Individuals with more positive perceptions of changing social networking security settings should also have higher Intentions to change those settings. Importantly, Attitudes are malleable [1]; in other words, they may change over time [1], [19], [36].

2.1.3 Subjective Norms

Subjective Norms (SN) reflects the individual's impression of other's feelings about performing the behavior [1]-[2]. Subjective Norms are essentially peer pressure [19]. If an individual perceives that others who are important to them have a positive view of changing security settings, then an individual should have a higher Intention to change security settings. Subjective Norms are formed from normative beliefs, which essentially reflect the individual's beliefs regarding how important others perceive the behavior [1].

2.1.4 Perceived Behavioral Control

Perceived Behavioral Control (PBC) captures the individual's perception of their capability to perform the behavior based on past experience and anticipated issues, as well as their skills, abilities, opportunity, compulsions, and dependence upon others [1]. PBC is closely related to self-efficacy [1]-[2]. PBC extends Ajzen's original Theory of Reasoned Action to behaviors which are not completely under the individual's control [1]. These behaviors typically require skills, opportunities, or resources to perform [1]. The addition of PBC also allows the model to address more complex behaviors [17]. PBC focuses on perceptions of control, rather than actual control [1]. Perceived Behavioral Control also influences behavior directly [1]. An Individual is more likely to engage in behaviors over which they have control: within the current research, respondents who feel able to change social networking security settings should also report higher Intentions to change those settings. PBC is formed from control beliefs [4].

2.1.5 Behavior

Although the TPB was initially designed to predict behavior [2], it can also be used to target strategies for changing behavior [40], [42]. Since the TPB suggests that behavior is a function of beliefs or information, the introduction of new information about a behavior can change an individual's evaluation of that behavior [1]. Doll and Ajzen noted "The discussion of the Theory of Planned Behavior suggests that information is at the root of intentions and actions. Behavior-relevant information, represented by memory in the form of behavioral, normative, and control beliefs, results in the formation of Attitudes, Subjective Norms, and Perceptions of Behavioral Control; and new information may lead to the formation of new beliefs or may alter previously formed beliefs" [19] p. 756. Thus, the TPB can be used to explain and also to change behavior.

Appendix A-Appendix G show the survey item wordings, abbreviations, means, standard deviations, and the overall construct mean for the Attitude, Perceived Behavioral Control, Subjective Norm, Behavior Intention, and Behavior constructs.

2.2 Theory of Planned Behavior and Information Systems Misuse

The current research examines individual utilization of social networking security settings. Fortunately, the TPB has been utilized in a number of security studies in the past [24]. For example, a combination of the TPB and the Theory of General Deterrence has been utilized to examine student intentions to commit software and data misuse [18], [23]-[24]. TPB was found to explain the behavior of computer misuse. A recent study supports the use of TPB in explaining software piracy in China [14]. TPB has also been used to examine the impact of piracy on video game console adoption [30], digital piracy [56], and the sharing of media files [10].

The Theory of Planned Behavior has also been used to examine user intention and actual reading of computer usage policies. One study utilized an expanded version of the TPB, which included Social Trust and Apathy, to investigate intention and actual reading of computer usage policies [25]. Results of that study suggest that Attitudes, Social Trust, and Apathy impact Intention to read computer usage policies. A similar study utilized the TPB, Normative Belief, and Self-efficacy to examine employee attitude toward compliance with organizational information

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

security policy [11]. Findings from that study showed that Attitude, Normative Beliefs, and Self-efficacy significantly influenced intention to comply.

The Theory of Planned Behavior has also been used to examine user self-protection. In one study, TPB was used to predict the adoption of antispyware systems [35]. Specifically, the authors utilized a variety of items to capture Attitude, Subjective Norm, and Perceived Behavioral Control. Of the nine items used, six (representing all three factors) were significant and explained 83% of intention to adopt and 55% of actual adoption of antispyware systems. In another study, the authors examined individual online privacy protection strategies using the TPB [55]. This study found a strong correlation between intent to use online privacy protection strategies and the actual use of such strategies. Further, Attitude and Perceived Behavioral Control were significantly correlated with Intention, as was Self-efficacy. The TPB has also been used to examine willingness to exchange personal information for commercial benefits [33].

Extant literature has also utilized TPB to examine usage of social networking. For example, researchers examined adolescent use of social networking sites based upon an extended version of TPB [6]. They concluded that Attitude and PBC did influence use of social networking sites; however, they also noted the importance of a new factor, labeled Group Norm.

Unfortunately, recent research suggests that the simple addition of information may be insufficient to change behavior: “It is usually argued that, in addition to having the required knowledge, people must also be motivated to perform the behavior in question” [3] p. 102. However, this argument focuses on knowledge, rather than information. In addition, the TPB suggests that information (beliefs) is the ultimate determinant of intentions and behaviors but does not address the accuracy of that information [3]. Motivation may indeed be a factor involved in changing behavior. Extant research suggests that apathy (a lack of motivation) may be a factor in understanding human behavior in terms of information systems security [26].

Recently, a number of studies have compared users’ desired security settings to their actual security settings on Facebook. Liu et al. [39] noted that intentions and actual settings only matched 37% of the time, while Madejski et al. [41] found that every respondent had a mismatch between intended and actual settings.

Liu et al. [39] examined the mismatch between intended and actual privacy settings for photographs using a sample of 200 Facebook users. The authors found that 36% of uploaded content was shared with default settings, and thus visible to all Facebook users. In addition, users had assigned their desired security settings to photos only 37% of the time. The study also noted that users who did bother modifying privacy settings for photos frequently selected settings that did not match their actual intentions.

Madejski et al. [41] examined the correctness of social networking security settings by comparing user intentions and actual settings using a Facebook application. The results of this study were quite concerning: all but three respondents felt their settings matched their intentions; however, every participant had a mismatch between their intended security settings and what they actually set within Facebook. The authors noted that most of the respondents were either unable or unwilling to correct their errors. They also noted that understanding security settings depended greatly upon what the individual user intended-the settings should reflect the intention of the user. Each of these studies focused on intentions and behavior-two key portions of the TPB. However, neither study examined the formation of these intentions. The TPB does.

Shin [48] utilized the Theory of Reasoned Action, an earlier version of the TPB, to investigate user acceptance of online social networking. This research examined the formation of Attitudes from perceived security (defined *as the ability to protect data against unauthorized access*), perceived privacy (defined “as the ability of an individual to manage information about themselves and thereby reveal themselves selectively” [48] p. 430), and trust (defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” [48] p. 430. The author concluded that perceived privacy, perceived security, and trust all combine to influence Attitudes, which in turn influence intention.

Another recent study conducted by Lewis et al. [37] investigated the importance of peers upon individual privacy decisions within a social network. This study found that users were significantly more likely to utilize a private profile (the focus of their study) if their friends and especially roommates did so, thus supporting the importance of peers in privacy decisions related to online social networks. The TPB captures the concept of peer group with the Subjective Norm factor.

Lewis et al. [37] also examined and confirmed the relationship between usage and the use of a private profile. The authors concluded that individuals who used an online social network, such as Facebook, were more likely to be aware of using private profiles. This suggested that a greater familiarity with a network could increase the use of private profiles. The TPB concept of PBC does measure an individuals’ perception of their ability to perform a behavior. While not an exact match, the [37] study does suggest that greater use results in more awareness and use of private profiles.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

Taken together, the existing research provides support for the use of TPB.

2.3 Apathy

Apathy is another possible determinant of intention and behavior regarding changing social networking security policies and settings. Apathy is a lack of motivation, interest, and emotion [46]. An individual may be aware of social networking security settings but may have no interest in changing the settings or may simply feel no need to modify the default settings [25]. Appendix F shows the survey item wordings, abbreviations, means, standard deviations, and the overall construct mean for the Apathy construct.

As defined earlier, Attitude captures an individual's positive or negative perceptions of performing the behavior [1]-[2]. However, a recent call for research suggested the inclusion of apathy. Madejski et al. [41] examined online social network security settings established by college students, as well as violations or errors in these settings. The authors found that subjects reported simply not caring about settings more often than expected. As a result, [41] recommended the incorporation of an apathetic option in future research. Although Apathy appears similar to Attitude (or a lack of Attitude), this research will include Apathy as an additional factor within the Theory of Planned Behavior in an attempt to determine if Apathy and Attitude are different factors. If the two are actually different factors, this research will also allow us to evaluate the significance of Apathy upon Intentions.

2.4 Social Trust

Apathy reflects a lack of motivation to perform a behavior. However, some individuals may simply assume that the service provider is better equipped to make decisions relating to security settings. This type of assumption is reflected in the construct Social Trust. Social Trust reflects a willingness to allow others to make decisions, especially in areas where the individual may lack interest, time, abilities, or other resources to reach decisions personally [51]. Some individuals may substitute Social Trust for an understanding of risks associated with technology [20]. Within the current context, social networking users could simply assume that service providers automatically adjust the security settings in optimal ways, given that the social networking security providers have presumably greater knowledge of the systems. Appendix G displays the survey item wordings, abbreviations, means, standard deviations, and the overall construct mean for the Social Trust construct.

3 Hypotheses

Existing research has utilized the TPB in a wide variety of settings, including information systems security. Thus the current research examines the standard TPB hypothesis within a new setting: utilization of security settings in social networking. For example, the TPB suggests that Behavior is influenced by Intention and that Intention is influenced by Attitude, Subjective Norm, and Perceived Behavioral Control. Each of these theoretical links will be examined separately. Further, TPB suggests that Perceived Behavioral Control also has a direct impact on Behavior. This also will be examined.

H1: Attitude is correlated with Intention

H2: Subjective Norm is correlated with Intention

H3: Perceived Behavioral Control is correlated with Intention

H4: Intention is correlated with Behavior

H5: Perceived Behavioral Control is correlated with Behavior

As discussed above, the extant literature suggests that motivation also plays a part in the formation of intention and behavior. This research will investigate the impact of Apathy (the lack of motivation) upon user's intention and actual modification of security settings.

H6: Apathy is correlated with Attitude

Extant literature also suggests that individuals may elect simply to trust others to make decisions about items such as security settings. This study will also examine the impact that Perceived Behavioral Control has on Social Trust.

H7: Perceived Behavioral Control is positively correlated with Social Trust.

H8: Social Trust is correlated with Behavioral Intention.

Figure 2 shows the relationships among the constructs with the related hypotheses.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile
This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

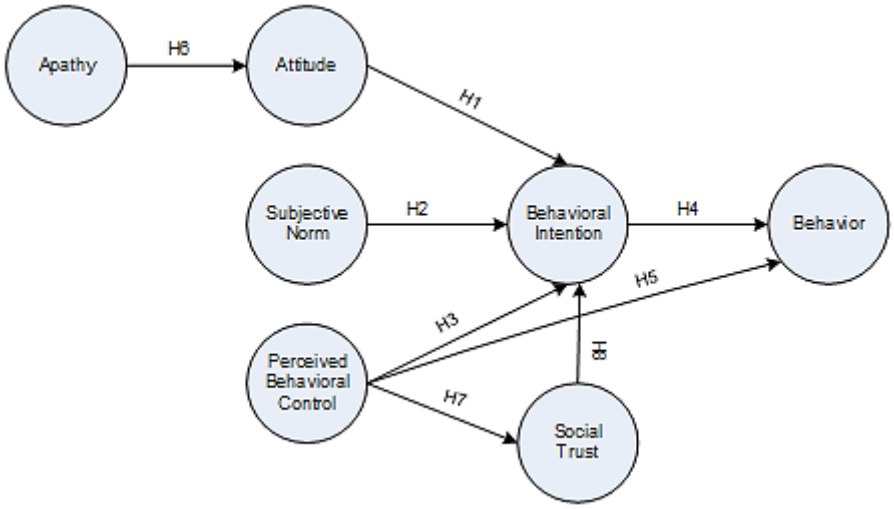


Figure 2: Research model hypotheses

4 Methodology

This study utilized a web-based survey of students enrolled in a flexible Master of Business Administration (MBA) program at a large university in the southeast United States. The survey items were modified from existing studies [4], [29] for use within the social networking security environment. The initial survey design was piloted amongst a small group of graduate assistants. The authors integrated the comments and suggestions into the survey before it was made available to all students enrolled in the program. An initial invitation to participate was sent from the general business advising email account, and an additional follow up request was sent two weeks later.

4.1 Data Collection and Demographics

A total of 70 respondents returned useable surveys. One concern surrounding this sample was its size. A review of the Structural Equation Modeling (SEM) literature showed that this sample size was adequate for the research. The criteria for determining minimum sample size were (a) ten times the largest number of formative indicators in a construct or (b) ten times the largest number of structural paths pointing toward a latent construct [32]. Since the model did not include formative indicators, the number of structural paths were used to determine minimum sample size. The model showed that the largest number of paths directed at a latent construct was three. Thus, the minimum sample size required for this study was 30, indicating that the actual sample of 70 is adequate.

The respondents represented a diverse group that had similar attributes to the general MBA population as well as similarities to traditional social network users. They were 44% male and 56% female, ranging in age from 20 to 59. When respondents were asked if they would classify themselves as business professionals or students, 57% indicated business professional. A recent survey conducted by the Pew Research Center [43] provided similar results to those in the current study. That survey examined the level of educational achievement for all Internet users 18+. Of the respondents who were categorized in the *some college* and *college+* groups, 59% were identified as having achieved the *college+* level of education. Table 1 shows the respondents' age, gender and primary orientation.

Table 1: Respondents' age, gender, and primary orientation

Age	**Count**	**%**	**Gender**	**Count**	**%**
20-24	17	24.29%	Male	31	44.29%
24-29	23	32.86%	Female	39	55.71%
30-39	20	28.57%			
40-49	7	10.00%	**Primary Orientation**	**Count**	**%**
50-59	3	4.29%	Business Professional	40	57.14%
>60	0	0.00%	College Student	30	42.86%
Total	70	100.00%			

Respondents were employed in a cross-section of industries with a strong representation from healthcare. They also represented varying levels of work experience, with an average of almost 10 years. Respondents also indicated that

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

they had a reasonable level of computer literacy with 60% classifying themselves as being very to extremely knowledgeable. Tables 2, 3 and 4 show respondents' industry and years of industry and computer experience.

Table 2: Respondents' industry

Business Industry	**Count**	**%**
Agriculture	2	6.25%
Durable Manufacturing	2	6.25%
Finance	4	12.50%
Food Service	0	0.00%
Government	4	12.50%
Health Care	9	28.13%
Information Systems	3	9.38%
Nondurable Manufacturing	1	3.13%
Services	4	12.50%
Trade/Retail	2	6.25%
Transportation & Public	1	3.13%
Other	0	0.00%

Table 3: Respondents' industry experience

	Years in Industry
Min	1
Max	31
Mean	9.84375

Table 4: Respondents' computer knowledge level and experience

Knowledge Level	Count	%	Years Computer Experience	Count	%
Very Little	0	0.00%	<1	0	0.00%
Somewhat Knowledgeable	7	10.00%	1-3	0	0.00%
Knowledgeable	20	28.57%	3-5	0	0.00%
Very Knowledgeable	30	42.86%	5-10	3	4.29%
Extremely Knowledgeable	13	18.57%	>10	67	95.71%

Although the use of a convenience sample of students does present weaknesses, such a sample is adequate for the current study. Students are generally considered to be quite familiar with Facebook and to possess reasonable technological skills, thus suggesting that students may be more familiar than most with managing privacy settings. Further, individuals preparing to enter the job market may be more aware of the need to focus on those privacy settings. In addition, college students are more likely than older users to post sensitive information online [41]. In addition, [48] suggests that the demographics of college students between the ages of 18 and 30 are similar to those of social networking site users. Hargittai [34] further suggests that college students are similar to SNS users.

4.2 Overview of Statistical Analysis

SmartPLS, a Structural Equation Modeling (SEM) tool that uses a variance-based approach to estimating parameters, was used to validate the measurement model and to test the hypotheses [45]. It utilizes a least-squares estimation procedure that places minimal demands on measurement scales, distributional assumptions, and sample size [15], [22], [27]. Other SEM tools, such as Analysis of a Moment Structures (AMOS) and Linear Structural Relationship Analysis (LISREL), employ a covariance-based approach to estimate parameters. They use a maximum likelihood function to obtain estimates and make greater demands on the scales, assumptions, and sample size. If the demands of the covariance based approach cannot be met, the preferred method is the variance-based approach [32]. When results are compared using structural equation models with good measurement properties, both approaches generally achieve comparable results [32].

The authors used the variance-based approach because the data did not meet the covariance-based approach assumptions exactly. The small sample size and the non-normal distribution of the data violated those assumptions. When such assumptions are violated, the preferred alternative is the variance-based approach that provides comparable results [32].

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile
This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

4.3 Assessment of the Measurement Model

The authors examined the psychometric properties of the measurement model to assess internal consistency reliability (ICR), convergent validity, and discriminant validity [15]. ICR, also known as composite reliability, is analogous to Cronbach's Alpha. Results showed that the loadings ranged from .85 to .96. These values exceed the recommended cutoff of .70 [27]. The results supported ICR. See Table 5.

Table 5: Internal consistency reliability, convergent validity, and discriminant validity

	ICR	AVE	AP	AT	B	BI	PBC	SN	ST
AP	0.93	0.77	**0.88**						
AT	0.92	0.85	-0.50	**0.92**					
B	0.93	0.87	-0.52	0.61	**0.93**				
BI	0.85	0.58	-0.78	0.56	0.46	**0.76**			
PBC	0.93	0.78	-0.38	0.27	0.25	0.44	**0.88**		
SN	0.85	0.65	-0.31	0.22	0.40	0.39	0.44	**0.81**	
ST	0.96	0.92	0.11	-0.07	-0.06	-0.05	0.28	0.15	**0.96**

Internal consistency reliabilities (in ICR column), average variance extracted (in AVE column), average variance extracted square roots (on diagonal) and correlations (below diagonal).
Apathy=AP, Attitude=AT, Behavior=B, Behavioral Intention=BI, Perceived Behavioral Control=PBC, Subjective Norm=SN, and Social Trust=ST

Table 6: Factor loadings

	AP	AT	B	BI	PBC	SN	ST
AP1	**0.86***	-0.41	-0.53	-0.66	-0.30	-0.31	-0.01
AP2	**0.86***	-0.46	-0.38	-0.70	-0.29	-0.19	0.25
AP3	**0.92***	-0.48	-0.46	-0.78	-0.34	-0.27	0.05
AP4	**0.86***	-0.38	-0.44	-0.59	-0.41	-0.34	0.09
AT1	-0.43	**0.91***	0.57	0.47	0.27	0.25	-0.02
AT2	-0.49	**0.94***	0.57	0.57	0.24	0.18	-0.10
B1	-0.57	0.61	**0.96***	0.50	0.27	0.39	0.05
B2 R	-0.36	0.53	**0.91***	0.34	0.19	0.35	-0.21
BI1	-0.55	0.59	0.45	**0.78***	0.25	0.22	-0.10
BI2 R	-0.63	0.36	0.30	**0.74***	0.33	0.29	-0.10
BI3 R	-0.75	0.40	0.31	**0.83***	0.44	0.37	-0.04
BI4	-0.46	0.33	0.32	**0.70***	0.32	0.32	0.11
PBC1	-0.34	0.25	0.24	0.37	**0.92***	0.31	0.26
PBC2	-0.47	0.36	0.28	0.52	**0.85***	0.51	0.16
PBC3	-0.24	0.15	0.21	0.32	**0.87***	0.32	0.29
PBC4	-0.24	0.18	0.15	0.29	**0.89***	0.38	0.29
SN2	-0.41	0.27	0.42	0.39	0.44	**0.88***	0.12
SN3	-0.17	0.17	0.30	0.31	0.38	**0.82***	0.08
SN4	-0.07	0.04	0.16	0.16	0.13	**0.72***	0.20
ST1	0.10	-0.10	-0.08	-0.05	0.29	0.14	**0.96***
ST2	0.11	-0.03	-0.03	-0.06	0.23	0.15	**0.95***

* p<.001

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

Apathy=AP, Attitude=AT, Behavior=B, Behavioral Intention=BI, Perceived Behavioral Control=PBC, Subjective Norm=SN, and Social Trust=ST

Convergent validity was assessed by observing factor loadings, ICR and average variance extracted (AVE) from the constructs [31]. Each factor loading should load significantly on its respective construct, and each loading should generally exceed .707 [13]. Factor loadings are presented in Table 6. ICR values for the constructs ranged from .85 to .96. The values exceeded the cutoff of .70 suggested by [28]. Values for AVE ranged from .58 to .92, which exceeded the cutoff of .50. Table 5 shows that ICR and AVE values used to measure convergent validity met or exceeded their thresholds. Thus, the analysis supported convergent validity.

Discriminant validity of the scales was assessed by comparing the square root of the AVE with the correlation among the constructs and examining the factor loadings and cross-loadings of the construct items. For the first measure, the square root of the AVE should be at least .707 (i.e., AVE>.50) and should exceed the correlation between pairs of constructs [28]. In terms of the second measure, items should load higher on their respective construct than on others [29]. Tables 5 and 6 show that the criteria used to measure discriminant validity met or exceeded their thresholds. Thus, discriminant validity is supported.

5 Results

Structural Equation Modeling (SEM) using SmartPLS was used to test the relationships among the constructs [45]. Results showed that six of the eight hypotheses were supported. Attitude (H1), Subjective Norm (H2), and Perceived Behavioral Control (H3) positively influenced Behavioral Intentions. Behavioral Intentions (H4) positively predicted actual Behavior. Apathy (H6) had a significant but negative impact on Attitude while Perceived Behavioral Control (H7) exhibited a positive influence on Social Trust. Perceived Behavioral Control (H5) did not impact Behavior and Social Trust did not predict Behavioral Intention (H8). Table 7 shows the results of the hypotheses testing. Figure 3 shows the results and their level of significance.

Table 7: Path coefficients and t-statistics

	Path Coeff.	t-Statistics
H1: Attitude -> Behavioral Intention	0.45	3.89**
H2: Social Norm -> Behavioral Intention	0.19	2.06*
H3: Perceived Behavioral Control -> Behavioral Intention	0.27	2.27*
H4: Behavioral Intention -> Behavior	0.43	3.76**
H5: Perceived Behavioral Control -> Behavior	0.06	0.47
H6: Apathy -> Attitude	-0.50	5.36**
H7: Perceived Behavioral Control -> Social Trust	0.28	2.31*
H8: Social Trust -> Behavioral Intention	-0.12	1.07

* p<.05; ** p<.001

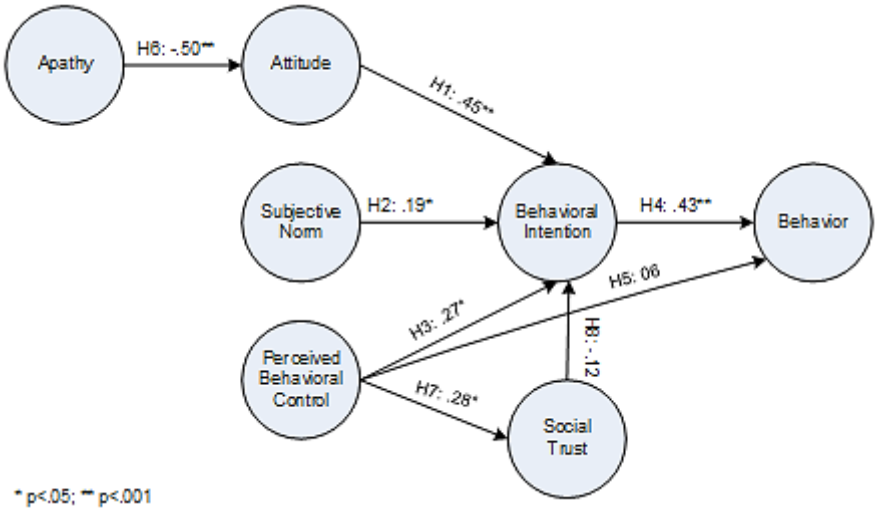


Figure 3: Research model results

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

6 Results

This study used TPB as its conceptual framework to investigate the factors that influenced users' behavior toward changing their social networking privacy and security settings. Results showed that the behavior associated with changing such settings was impacted by six of the eight constructs. In other words, Attitude (H1), Subjective Norm (H2) and Perceived Behavioral Control (H3) positively influenced users' Behavioral Intention. Behavioral Intention (4) positively predicted users' Behavior toward changing social networking privacy and security settings. Apathy (H6) negatively influenced Attitude and Perceived Behavioral Control (H7) positively predicted Social Trust. Perceived Behavioral Control (H5), however, did not predict Behavior and Social Trust did not impact Behavioral Intention (H8).

TPB suggests that Behavior is influenced by Intention, and Intention is influenced by Attitude, Subjective Norm, and Perceived Behavioral Control [1]. The results provided support for the hypothesis that Attitude predicted Behavioral Intention (H1). This support is consistent with the expectation that the Attitude toward the Behavior affects users' feelings about performing the behavior. In other words, users believed that it was important to understand and check social networking privacy and security settings. These feelings toward social networking privacy and security settings positively influenced users' Intentions to change the settings.

The results provided support for the hypothesis that Subjective Norm predicted Behavioral Intention (H2). The support is consistent with the expectation that people and authorities who are important to users can influence their behavior; e.g., users' friends and family or their superiors at college/companies think they should change privacy and security settings. This perceived social pressure positively influenced users' behavior intentions toward changing social networking privacy and security settings.

Results revealed support for the hypothesis that Perceived Behavioral Control (H3) positively predicted Behavioral Intention. This support is consistent with the expectation that users perceive that they have the abilities to perform the behavior based on past experience and anticipated issues, as well as their skills, opportunity, compulsions, and dependence upon others [1]. In other words, users believed that they have the knowledge and resources necessary to change social networking privacy and security settings. They also believed that changing those settings was easy. Such perceptions can be expected to have a positive influence on users' behavioral intention toward changing social networking privacy and security settings.

The results also supported the hypothesis that Behavioral Intention (H4) positively influenced Behavior. This finding is consistent with the expectation that Behavior can be predicted by investigating users' Intentions to perform the behaviors [1]. In other words, users' intentions to take time to check and change social networking privacy and security settings predicted their actual behavior toward changing such settings.

The study results showed negative support for the hypothesis that Apathy predicted Attitude (H6). This support was consistent with the expectation that users who do not feel motivated, interested or emotional about changing their social networking privacy and security settings will assume that such changes are unimportant and that failing to change those settings will have no consequences. Thus, Apathy had a negative effect on users' Attitudes toward changing their social networking settings.

Results showed support for the hypothesis that Perceived Behavioral Control influences Social Trust (H7). This finding is consistent with the expectation that users who feel unable to make changes to security settings due to a lack of interest, time, abilities, or other resources may prefer to let service providers adjust security settings for them [37]. On the other hand, users who understand how to adjust security settings but lack the time, interest, or opportunity to do so may rely on service providers to make the changes.

However, no statistical support is found for the impact of Social Trust on Behavioral Intention (H8). This unexpected result suggests that trusting or not trusting the service provider to make decisions has no real impact on user intention. While unexpected, this could simply reflect a lack of overall understanding of security settings. Alternatively, Social Trust may be reflected somewhat in Perceived Behavioral Control measurements. For example, Perceived Behavioral Control represents user perceptions of ability to perform a behavior. If users perceive that they can change settings but elect to use the default settings established by the service provider, one could assume that the users are expressing trust in the existing settings—thus there would be no intention to make changes. Future research could help clarify this.

Despite expectations, the relationship between PBC and Behavior (H5) is not significant in the current study. However, this is not unexpected from a theoretical perspective. Armitage and Conner [5] noted that in situations where the behavior in question is under volitional control, PBC logically should not have any impact on the relationship between intention and behavior. In short, these authors suggest that PBC will only be important when subjects feel they lack control over a behavior. Barua [7] offers support for this position, noting that *the actual role of PBC varies according to the situational factors* (p. 57). Within the current study, the users may feel they have significant control over the alteration of privacy settings on social networks, thus negating the impact of PBC on behavior itself.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

7 Study Limitations and Future Research

This research examined the Theory of Planned Behavior as applied to user modification of social networking privacy settings. Although the applicability of TPB to security-related behaviors has been examined in the past, this research is the first to confirm that the TPB stands within the area of social networking privacy.

In addition, this research extends the TPB by adding two factors: Apathy and Social Trust. Although both factors have been examined in the extant security and privacy literature, this is the first time the two factors have been examined together as part of the TPB in an examination of social networking privacy. Both of the new factors, Apathy and Social Trust, were found significant. These factors helped explain the formation of Attitude and how Perceived Behavioral Control influence Social Trust and added another possible way to examine the underlying causes of Behavior.

This study also provides a foundation for future research regarding user modification of social networking security settings. For instance, future work could examine variation in subject characteristics such as age or past experiences with security breaches. Furthermore, other factors such as group norm from [5] should be included and examined as well. In addition, Apathy and Social Trust could be employed in future research utilizing TPB, Technology Acceptance Model (TAM), or other related models.

The limitations of this study offer opportunities for researchers to make meaningful contributions to the security and privacy literature. One limitation was that environmental and economic factors were not investigated. These factors could impact Intentions toward performing a behavior. Future researchers could examine how these factors might impact users' Intentions toward changing their social networking privacy settings. Another limitation was that the direction and correctness of users' changes to their social networking settings were not examined in details. Although some research has been done in this area [39], [41], the literature review provided sparse findings. Researchers could use this lack of findings to fill the gap in our understanding of the accuracy of how users' make changes to their social networking setting. A final limitation of the study was that it did not explore a longitudinal study. Future researchers could use TPB in the context of a longitudinal study to examine how, if any, changes in users' social networking settings vary over time.

8 Implications for Practice

Although this study was limited by the use of a convenience sample of MBA students, a number of implications for practice should be noted. First, the results of this study suggested that respondents do not consider changing privacy settings to be difficult; however, those settings are still often not changed. This suggests a need to focus on why users elect not to change privacy settings.

Fortunately, the study does suggest why users elect not to change settings: Apathy. Although the other TPB constructs, including Attitude and Subjective Norm, were associated with the behavior of changing constructs, Apathy also plays a part. Results suggest that social network users simply do not understand or see a need to change their privacy settings. As a result, those settings are typically not modified.

This result provides insight for practitioners, social networking organizations, and organizations in general. Additional education and training should be provided frequently to help users understand the importance of privacy settings and to help them make good decisions regarding their settings. Users need to be continually reminded of the importance of privacy settings and not simply to trust others (Social Trust) to handle it for them.

9 Conclusion

This research examined social network user Intention to change privacy and security settings. As predicted by the TPB, Attitude, Subjective Norm, and Perceived Behavioral Control, all influenced intention to change settings. In addition, intention to modify privacy and security settings predicted the actual behavior of changing those privacy and security settings. In contrast to the TPB, PBC was not correlated with Behavior.

In addition, to examining the TPB constructs within the social networking privacy and security setting, this research also examined the impact of Apathy and Social Trust. As expected, Apathy negatively influenced Attitude, suggesting that individuals who simply don't care are unlikely to change their privacy and security settings. The current research also investigated the impact of PBC upon Social Trust; a positive relationship was found.

This research contributes by adding to our understanding of how and why individuals are willing to modify the privacy and security settings of their social networking accounts. Apathy appears to be a huge factor negatively influencing such changes; however, Apathy can be overcome.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

References

[1] I. Ajzen, Attitudes, Personality, and Behavior. Chicago, IL: The Dorsey Press, 1988.
[2] I. Ajzen, The theory of planned behavior, Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179-211, 1991.
[3] I. Ajzen, N. Joyce, S. Sheikh, and N. Cote, Knowledge and the prediction of behavior: The role of information accuracy in the theory of planned behavior, Basic and Applied Social Psychology, vol. 33 no. 2, pp. 101-117, 2011.
[4] I. Ajzen and T.J. Madden, Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control, Journal of Experimental Social Psychology, vol. 22, no.6, pp. 453-474, 1986.
[5] C.J. Armitage and M. Conner, Efficacy of the theory of planned behavior: A meta-analytic review, British Journal of Social Psychology, vol. 40, no. 4, pp. 471-499, 2001.
[6] R.K. Baker and K.M. White, Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective, Computers in Human Behavior, vol. 26, no. 6, pp. 1591-1597, 2010.
[7] P. Barua, The moderating role of perceived behavioral control: The literature criticism and methodological considerations, International Journal of Business and Social Science, vol. 4 no. 10, pp. 57-59, 2013.
[8] L. Beck and I. Ajzen, Predicting dishonest actions using the theory of planned behavior, Journal of Research in Personality, vol. 25, no. 3, pp. 285-301, 1991.
[9] L. F. Bright, S. B. Kleiser and S. L. Grau. Too much Facebook? An exploratory examination of social media fatigue, Computers in Human Behavior, vol. 44, pp. 148-155, 2015.
[10] R.H. Blake and E. S. Kyper, An investigation of the intention to share media files over peer-to-peer networks, Behavior & Information Technology, vol. 32, no. 4, pp. 410-422, 2013.
[11] B. Bulgurcu, H. Cavusoglu and I. Benbasat, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, MIS Quarterly, vol. 34, no. 3, pp. 523-548, 2010.
[12] N. Carlson. (2011, April) The real history of Twitter. Business Insider. [Online]. Available: http://www.businessinsider.com/how-twitter-was-founded-2011-4.
[13] E.G. Carmines and R.A. Zeller, Reliability and Validity Assessment. Beverly Hills, CA: Sage Publications, 1979.
[14] R. Y.K. Chan, K. H.Y. Ma and Y.H. Wong, The software piracy decision-making process of Chinese computer users, The Information Society, vol. 29, no. 4, pp. 203-218, 2013.
[15] W.W. Chin, The partial least squares approach to structural equation modeling, in Modern Methods for Business Research (G.A. Marcoulides, Ed.). Mahway, NJ: Lawrence Erlbaum, 1998, pp. 295-336.
[16] W.W. Chin, B.L. Marcolin and P.R. Newsted, A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Marti Carlo simulation study and an electronic-mail emotion/adoption study, Information Systems Research, vol. 14, no. 2, pp. 189-217, 2003.
[17] M. Conner and C.J. Armitage, Extending the theory of planned behavior: A review and avenues for further research, Journal of Applied Social Psychology, vol. 28, no. 15, pp. 1429-1464, 1998.
[18] T.P. Cronan, C. Foltz and T.W. Jones, Piracy, computer crime, and IS misuse at the university, Communications of the ACM, vol. 49, no. 6, pp 84-90, 2006.
[19] J. Doll and I. Ajzen, Accessibility and stability of predictors in the theory of planned behavior, Journal of Personality and Social Psychology, vol. 63, no. 5, pp. 754-764, 1992.
[20] T. Earle and G. Cvetkovich, Social Trust: Toward a Cosmopolitan Society, Westport, CT: Praeger, 1995.
[21] Facebook Newsroom. (2015, June) Key Facts. Newsroom. [Online]. Available: http://newsroom.fb.com/Key-Facts.
[22] R. Falk, F. Miller and N.B. Miller, A Primer for Soft Modeling. Akron, OH: University of Akron Press, 1992.
[23] C.B. Foltz, The impact of deterrent countermeasures upon individual intent to commit misuse: A behavioral approach, Ph.D. dissertation, Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR, 2000.
[24] C. Foltz, P.T. Cronan and T. Jones, Human behavior as a factor in the control of information systems misuse and computer crime, in Proceedings of the Decision Sciences Institute, Atlanta, GA, 2002, pp. 1246-1251.
[25] C.B. Foltz and P.H. Schwager, Social network privacy: Expectation vs. reality, in Proceedings of the Southern Association for Information Systems Conference. Americas Conference on Information Systems, Charleston, SC, 2009, pp. 165-168.
[26] C. Foltz, P.H. Schwager and J.E. Anderson, Why users (fail to) read computer usage policies, Industrial Management & Data Systems, vol. 108, no. 6, pp. 701-712, 2008.
[27] C. Fornell and F.L. Bookstein, Two structural equation models: LISREL and PLS applied to consumer exit-voice theory, Journal of Marketing Research, vol. 19 no. 4, pp. 440-452, 1982.
[28] C. Fornell and D.F. Larcker, Evaluating structural equations models with unobservable variables and measurement error, Journal of Marketing Research, vol. 18, no. 1, pp. 39-50, 1981.
[29] D. Gefen and D. Straub, A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example, Communications of the AIS, vol. 16, no. 5, pp. 91-109. 2005.
[30] S. Goode and A. Kartas, Exploring software piracy as a factor of video game console adoption, Behavior & Information Technology, vol. 31, no. 6, pp. 547-563, 2012.
[31] J.F. Hair, R.E. Anderson, Jr., R.L. Tatham, and W.C. Black, Multivariate Data Analysis with Readings, 5th ed., Englewood Cliffs, NJ: Prentice Hall, 1998.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

[32] J.F. Hair, C.M. Ringle and M. Sarstedt, PLS-SEM: Indeed a silver bullet, Journal of Marketing Theory and Practice, vol. 19, no. 2, pp. 139-151, 2011.
[33] W. Hairman, M. Walrave and K. Ponnet, Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior, Cyberpsychology, Behavior, and Social Networking, vol. 16, no. 2, pp. 81-87, 2013.
[34] E. Hargittai, Whose space? Differences among users and non-users of social network sites, Journal of Computer-Mediated Communication, vol. 13, no. 1, pp. 276-297, 2007.
[35] Y. Lee and K.A. Kozar, Investigating factors affecting adoption of anti-spyware systems, Communications of the ACM, vol. 48, no. 8, pp. 72-77, 2005.
[36] L.N.K. Leonard and T.P. Cronan, Attitude toward ethical behavior in computer use: a shifting model, Industrial Management & Data Systems, vol. 105, no. 9, pp. 1150-1171, 2005.
[37] K. Lewis, J. Kaufman and N. Christakis, The taste for privacy: An analysis of college student privacy settings in an online social network, Journal of Computer-Mediated Communication, vol. 14, no. 1, pp. 79-100, 2008.
[38] LinkedIn Press Center. (2013, July) About linkedIn: Company information. LinkedIn. [Online]. Available: http://press.linkedin.com/about.
[39] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing Facebook privacy settings: User expectations vs. reality, in Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, Berlin, Germany, 2011, pp. 61-70.
[40] T.J. Madden, P.S. Ellen and I. Ajzen, A comparison of the theory of planned behavior and the theory of reasoned action, Personality and Social Psychology Bulletin, vol. 18, no. 1, pp. 3-9, 1992.
[41] M. Madejski, M. Johnson and S.M. Bellovin, The failure of online social network privacy settings, Columbia University, New York, Technical Report CUCS-010-11, 2011.
[42] J. D. Newton, M.T. Ewing, S. Burney, and M. Hay, Resolving the theory of planned behavior's 'expectancy-value muddle' using dimensional salience, Psychology and Health, vol. 27, no. 5, pp. 588-602, 2012.
[43] Pew Research Center. (2013, December) Social networking fact sheet. Pew Research Internet Project. [Online]. Available: http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/.
[44] S. Rao and I. Troshani, A conceptual framework and propositions for the acceptance of mobile services, Journal of Theoretical and Applied Electronic Commerce Research, vol. 2, no. 2, pp. 61-73, 2007.
[45] C.M. Ringle, S. Wende and A. Will. (2005) SmartPLS 2.0 (M3) Beta. SmartPLS. [Online]. Available: http://www.smartpls.de/.
[46] P.H. Robert, S. Clairet, M. Benoit, J. Koutaich, C. Bertogliati, O. Tible, H. Caci, M. Borg, P. Brocker, and P. Bedoucha, The apathy inventory: Assessment of apathy and awareness in alzheimer's disease, parkinson's disease and mild cognitive impairment, International Journal of Geriatric Psychiatry, vol. 17, no. 12, pp. 1099-1105, 2002.
[47] Semiocast. (2012, July) Twitter reaches half a billion accounts: More than 140 million in the U.S. Semiocast. [Online]. Available: http://semiocast.com/en/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US.
[48] D. Shin, The effects of trust, security, and privacy in social networking: A security-based approach to understand the pattern of adoption, Interacting with Computers, vol. 22, no. 5, pp. 428-438, 2010.
[49] M. Siegrist, The influence of trust and perceptions of risks and benefits on the acceptance of gene technology, Risk Analysis, vol. 20, no. 2, pp. 195-203, 2000.
[50] M. Siegrist and G. Cvetkovich, Perception of hazards: The role of social trust and knowledge, Risk Analysis, vol. 20, no. 5, pp. 713-719, 2000.
[51] M. Siegrist, G. Cvetkovich and C. Roth, Salient value similarity, social trust, and risk/benefit perception, Risk Analysis, vol. 20, no. 3, pp. 353-62, 2000.
[52] S. Taylor and P.A. Todd, Understanding information technology usage: A test of competing models, Information Systems Research, vol. 6, no. 2, pp. 144-176, 1995.
[53] Twitter: About Twitter. (2015) About Twitter. Twitter. [Online]. Available: https://about.twitter.com/company.
[54] E. Vanderhoven, T. Schellens, M. Valcke, and A. Raes. (2014, August) How safe do teenagers behave on facebook? An observational study. PLoS ONE. [Online] Available: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0104036.
[55] M.Z. Yao and D.G. Linz, Predicting self-protections of online privacy, CyberPsychology & Behavior, vol. 11, no. 5, pp. 615-617, 2008.
[56] C. Yoon, Digital piracy intentions: A comparison of theoretical models, Behavior & Information Technology, vol. 31, no. 6, pp. 565-579, 2012.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

Appendix A: Attitude Construct Items, Means, and Standard Deviations

Items Adapted from [52]	Survey Item Abbreviation	Mean	SD
I believe it is important to check social networking privacy and security settings.	AT1	4.63	.59
I believe it is important to understand social networking privacy and security settings.	AT2	4.50	.65
Changing the privacy and security settings of social networking sites is unpleasant.	AT3	3.10	1.00
Construct Mean		3.91	.52

Appendix B: Perceived Behavioral Control Construct Items, Means, and Standard Deviations

Items Adapted from [52]	Survey Item Abbreviation	Mean	SD
Overall, I believe that social networking privacy and security settings are easy to change.	PBC1	3.80	.83
I have the resources necessary to change my social networking privacy and security settings.	PBC2	4.03	.76
I would find it easy to change my social networking privacy and security settings.	PBC3	3.81	.82
I have the knowledge necessary to change my privacy and security settings on social networking sites.	PBC4	3.70	.86
Construct Mean		3.83	.72

Appendix C: Subjective Norm Construct Items, Means, and Standard Deviations

Items Adapted from [52]	Survey Item Abbreviation	Mean	SD
People who influence my behavior think that I should change the privacy and security settings of social networking sites.	SN1	3.10	.95
The administration and staff of my company/college think that I should change the privacy and security settings of social networking sites.	SN2	3.56	.91
People who are important to me think that I should change my social networking privacy and security settings.	SN3	3.40	.92
My superiors think that I should change the privacy and security settings of my social networking sites.	SN4	3.20	1.05
Construct Mean		3.31	.75

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 2 / MAY 2016 / 1-15
© 2016 Universidad de Talca - Chile
This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000200002

Appendix D: Behavioral Intention Construct Items, Means, and Standard Deviations

Items Adapted from [8], [40]	Survey Item Abbreviation	Mean	SD
I always take time to check social networking privacy and security settings.	BI1	4.03	.78
I definitely do not intend to change my social networking privacy and security settings.	BI2	4.14	.82
I would never change my social networking privacy and security settings.	BI3	4.31	.75
I definitely will try to change my social networking privacy and security settings.	BI4	3.79	.83
Construct Mean		4.06	.61

Appendix E: Behavioral Construct Items, Means, and Standard Deviations

Items Adapted from [26]	Survey Item Abbreviation	Mean	SD
What percentage of the social networking privacy and security settings do you:			
Change	B1	6.90	3.21
Keep the Defaults	B2	7.81	2.87
Construct Mean		7.36	2.80

Appendix F: Apathy Construct Items, Means, and Standard Deviations

Items Adapted from [46]	Survey Item Abbreviation	Mean	SD
I don't care if I change my social networking privacy and security settings.	AP1	1.90	.89
Changing social networking privacy and security setting is of no consequence.	AP2	1.90	.85
Changing social networking privacy and security settings is unimportant.	AP3	1.81	.79
It doesn't matter if I change my social networking privacy and security settings.	AP4	1.97	.92
Construct Mean		1.89	.75

Appendix G: Social Trust Construct Items, Means, and Standard Deviations

Items Adapted from [49]-[51]	Survey Item Abbreviation	Mean	SD
I trust that the organizational administration is conscious of their responsibilities in creating, implementing, and enforcing social networking and security policies.	ST1	4.55	2.32
In general, I have confidence in the organizational administrational personnel in charge of creating, implementing, and enforcing social networking and security policies.	ST2	4.28	2.42
Construct Mean		4.41	2.18