THE IMPACT OF USERS' AWARENESS AND SELF-EFFICACY OF PRIVACY CONTROL OPTIONS ON DISCLOSURE INTENTION IN ONLINE SOCIAL NETWORKS

by

Ting Li

MSc in Management, Tianjin University, 2009

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate and Postdoctoral Studies

(Business Administration)

THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)

August 2015

Abstract

Online social networks (OSN) such as Facebook have changed people's communication patterns. Along with new OSN feature development, control options in OSNs have accumulated in an unprecedented speed, yet the impact of the awareness of the abundance of control features has not been fully studied. This study addresses this research gap by proposing and validating a theoretical model that explains how awareness and two specific awareness-influencing constructs, namely perceived self-efficacy and perceived usefulness of control options, jointly affect OSN users' personalization-enabled privacy controls and their disclosure intention in the OSN environments (e.g. posting intention). Data was collected from 297 active Facebook users through an online survey, and the research model was tested using structural equation modeling (SEM). It was found that 1) OSN users only possess a medium level of awareness of available control options; 2) the impact of awareness of control options on privacy control is fully mediated by individuals' self-efficacy; 3) both self-efficacy and perceived usefulness of control options are positively associated with OSN users' perceived control over their privacy; 4) function tutorial of control options alone is effective in improving OSN users' awareness, self-efficacy and PU of the control features, while the presence of warning messages lead to no further privacy control improvement but have a mitigating impact on individuals' disclosure intention; and 5) 'too much' awareness of control options will exert a negative influence on OSN users' disclosure intention through constructs (e.g. perceived risk) other than privacy control. Theoretical and practical implications of this study are discussed at the end of the thesis.

Preface

This thesis is original, unpublished, independent work by the author, Ting Li, under the supervision of Professor Hasan Cavusoglu and Professor Izak Benbasat. Research proposal of this study is reviewed and approved by the Human Ethics Board at the University of British Columbia (BREB number: H15-01425).

Table of Contents

List of Tables

List of Figures

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my supervisors, Professor Hasan Cavusoglu and Professor Izak Benbasat. My two years at Sauder have been the most rewarding two years in my life thanks to their guidance. They have taught me the basic qualifications of a researcher through their inspiring courses, through numerous revisions of my research proposals, and through continuous modification and improvement of my work on this thesis. Their guidance, suggestions, and support encouraged me throughout the research process.

I am also grateful to my graduate colleagues, all of the Ph.D. and MSc students in MIS division, for their advice and help with my study and research.

Lastly, I want to express my gratitude towards my beloved husband, parents, and my grandfather. It was their strongest support and the deepest love that provided me with an enduring source of strength in overcoming all the obstacles I faced during the past two years.

1. Introduction

1.1 Research background

The world of online social networks (OSN) is evolving fast. One moment we were still marveled at the transnational video chats with our friends, the next moment we have already taken for granted the privilege of browsing through the updates posted by our friends, clicking likes and ridiculing with goodwill to show our concern in the virtual community. Apart from the exponential growth in membership (Acquisti & Gross, 2006; Cheung et al., 2011; Berger et al., 2014), OSNs such as Facebook and Google Plus+ have altered individuals' daily routines of communication, making the joy of sharing within the reach of one's fingertips (Ellison et al., 2007). Designed as platforms where users can create and share personal information as a result of voluntary disclosure, the trade-off between individuals' privacy needs and their sociability as well as sharing desire has remained a difficult task from the very early days of the emergence of OSN (Joinson, 2008; Tufekci, 2008; Brandtzaeg et al., 2010).

In the hope of attract new users and maintain current ones, OSN providers have exerted themselves in devising new personalization tools (e.g. customized interfaces), which serves as a key mechanism of service improvement. Thanks to the rapid accumulation of personalization features during the past decade, online individuals have been placed in a labyrinth of assorted IT artifacts through which they can fulfill activities with great diversity: one can now trace every visitor's activity on one's virtual space (e.g. Q Zone), add the exact location to one's new post with automatic positioning function (e.g. Facebook), organize an outdoor event with people sharing the same interest (e.g. Tumblr), one can even withdraw a message that has just been sent to someone on the

spur of the moment (e.g. Wechat). One sub-division of the set of personalization features is privacy control options, defined as privacy settings that allow users to maintain their state of privacy through configuration activities, such as, restricting access to future posts or personal contact information, or editing the list of blocked people (Wang et al., 2011; Donovan, 2015). Although privacy control options were considered less influential compared to pleasure features (e.g. well-designed interface, shortcut to most frequently used options, three dimensional image presentation) in generating enticement for further usage or purchasing intention, their role as privacy-enhancing technologies should be re-defined in modern OSN contexts, where privacy has been raised to a new height of significance in recent years (Tavani & Moor, 2001; Belanger et al., 2002; Hichang, 2010; Hoadley et al., 2010).

The fast accumulation of personalization functions has enabled a great diversity of activities for OSN users, yet the mental acceptance and actual utilizations of those functions are confined to the cognitive capacity of individuals (Acquisti & Gross, 2006; Hoadley et al., 2010). The simple truth is that people will not perceive any benefit or protection from available IT artifacts provided on OSN platforms unless they are knowledgeable about the features' existence. However, the prerequisite role of awareness to further option-based perceptions has not been highlighted in current IS research. As the installation of fire extinguishers in a building renders meaningless if no one is knowledgeable of the existence and hence no utility perceived; the existence of privacy control options becomes moot if the majority of users are not even aware of their availability, not to mention the skills in using them. Within the scope of this study, we aim to study the impact of individuals' awareness and self-efficacy of currently available privacy control options on their privacy related perceptions in OSN environments

specifically.

1.2 Focus of the study

Extant literature in the IS domain has laid heavy emphasis on individuals' awareness over private information handling practices conducted both at the legislation level and organizational level (Culnan, 1995; Milne & Rohm, 2000; Phelps et al., 2000; Xu et al., 2008). Only a handful of scholars got interested in individuals' actual awareness of personalization features or potential losses caused by the lack of awareness of available privacy control options in the last decade (Brandtzaeg et al., 2010). While fair information practices (FIP) conducted by organizations are identified as a key component triggering people's perceived justice and mitigating their privacy concern (Son & Kim, 2008), the availability of privacy control features has long been recognized as an important channel for individuals to exercise control over their personal information and to perceive benevolence from service providers in the online environment (Laufer et al., 1973; Schoeman, 1984). In line with this perspective, the thesis aims to explore the association between awareness of control options and individuals' perceived control over privacy, and see if this perception can lead to increased privacy and disclosure intention in OSN environments.

Apart from awareness, perceived privacy control is another construct that has been partially studied. Some scholars have identified privacy control as an antecedent or dimension of privacy, while others have equated privacy with control or the ability to control (Smith, Dinev, & Xu, 2011). Regardless of the original perspective taken, a shared core definition has been accepted by most IS scholars that it represents individuals' control over the collection, dissemination and secondary usage of personal

information (Stone & Stone, 1990; Culnan, 1993; Caudill & Murphy, 2000; Phelps et al., 2000; Zweig & Webster, 2002; Malhotra et al., 2004; Bélanger & Crossler, 2011). However, most extant research on privacy control only took a close look at the influence of real control over personal information that has been bestowed by organizations (e.g. FIP) or legislative authorities. A few studies have concentrated on personalization-enabled control, defined as a sense of control generated through available IT features, such as, privacy control options and security procedures (Dinev & Hart, 2004).

Addressing the call for more consolidated protection over online privacy (Smith et al., 2011), this study will explore the linkage from the awareness of privacy control options to individuals' privacy control enabled by privacy control features in OSN environments. To further explore the significance of awareness of control options, the associations between awareness-influencing constructs (i.e. self-efficacy and perceived usefulness of privacy control options) and perceived privacy control will also be examined. In sum, we aim to provide insights into the following four research questions:

1. Are individuals aware of the privacy control options provided by OSNs? If not, what educational mechanisms (e.g. tutorials) can be used to increase people's awareness?
2. Provided people already have enough awareness, do they have enough self-efficacy over the privacy control options? If not, how do we increase their self-efficacy level?
3. Are awareness and self-efficacy effective predictors of individuals' perceived privacy and disclosure intention?
4. Given the plenty of privacy control options, can someone be too aware and knowledgeable that he or she perceives higher privacy control yet becomes more

cautious in sharing activities than individuals with low or medium level of awareness?

In the following sections, a literature review is first conducted to summarize relevant findings in extant studies. Second, the research framework of this study is proposed, followed by a detailed description of study design. After data collection and cleaning, the proposed research model is tested and analyzed. The conclusion of this study and future research directions are presented at the end of this thesis.

2. Literature Review

2.1 The classification of awareness

Based on an extensive literature review of 89 empirical studies, Yun et al. (2014) summarized the core definition of privacy awareness as the extent to which an individual is informed about the available technology, service, or practice (e.g., privacy policy). In accordance with the findings of Yun et al., we identified two major trends of awareness study after a summarization of extant privacy literature: the first school of thought emphasizes importance of the awareness of privacy practice, and their accumulated work constitutes the mainstream of awareness-privacy study (Brecht et al., 2011). The second group of researchers (also the minority) focuses on IT artifacts and explores individuals' awareness of personalization tools. To clarify the standpoint of this study, the focus on these two trends and their corresponding statements are summarized and illustrated as following.

2.1.1 Awareness of privacy practice

Privacy practices conducted at the enterprise level and regulation effort under the supervision of government exert a direct influence on individuals' privacy concern and various other perceptions (e.g. trust). According to Culnan (1995), people's privacy concern is significantly influenced by their awareness of privacy practices conducted by organizations. Drawing on social contract theory, Malhotra at el. (2004) claim that the awareness over privacy practice represents internet users' understanding about established conditions and actual practices and serves as a key dimension formulates individuals' privacy concern. Some other scholars state that privacy awareness should be treated as a direct antecedent of the privacy concern (Smith et al., 2011). Those

above mentioned conditions and practices are normally regulated and bestowed by authorities or companies that run online businesses. A classification of studies on awareness of privacy practices can be found in Appendix A.

2.1.2 Awareness of personalization tools

Academic attention should not only be on the restraint mechanisms of FIP or regulatory guidance but also on the technological affordances. Only through the combination of these aspects should online users achieve sufficient accountability of personal data (Giannotti et al., 2012). It is claimed that apart from awareness of privacy practices conducted by organizations, the state of privacy can only be achieved co-existent with the awareness of privacy control options such as granting users with account deactivating options (Culnan, 1995; Milne & Rohm, 2000; Yeung et al., 2009). Similarly, Phelps et al. (2000) claimed that an advanced level of FIP should grant customers more control over initial data gathering and the power to restrict the sharing of their personal information with third parties. Apart from computer anxiety and some other well identified ingredients, it is suggested that individuals' awareness and attitude of privacy protection technologies exert a direct influence on people's IT adoption decision (Kumar et al., 2008). Based on the above statements, it is not enough to base investigation of privacy related awareness solely on consumers' knowledge of FIP; researchers should also lay emphasis on individuals' awareness of personalization options that are available for them to utilize and safeguard their online privacy.

The prevalent usage of privacy control tools will make individuals more knowledgeable about privacy protection mechanisms and increase their perceived control accordingly. In the long run, online users should be able to allow access to and use of their data for

their own good with the availability of privacy-preserving methods (Giannotti et al., 2012). According to Acquisti et al. (2005), lack of sufficient awareness of privacy control settings will affect OSN users' control over personal information and further influence their privacy expectation. Following this logic, when acknowledged, the existence of privacy control options should also exert influence on OSN users' perceived control. In addition, it is empirically shown that an individual's perceived benevolence of a service provider will increase when he believes that the service provider cares about him and acts in his interests (Benbasat & Wang, 2005). Accordingly, it is assumed that the development of a variety of control features will increase individuals' perceived benevolence and protection from the service provider and further increase their perceived control in OSN environments. In the context of OSNs, where users vary in their awareness and perceptions about privacy settings (Gross & Acquisti, 2005), it becomes extremely necessary to explore possible ways to improve users' awareness of privacy control options.

It was reasonable to assume that a majority of the public had potentially been exposed to opportunities to learn about personalization tools (Culnan, 1995), yet OSN users do not possess adequate understanding over the visibility of members' profiles, neither do they have enough awareness of privacy issues regarding information collection and dissemination (Acquisti & Gross, 2006). In addition, Brandtzaeg et al. (2010) empirically showed that there exists a generational gap in awareness of and ability to handle privacy settings among Facebook users: while younger people possess high level of awareness over the available privacy settings and find Facebook to be generally trustworthy, older users are not as aware of the usage and protection strategies as the younger ones and showed higher concern over privacy invasion via Facebook.

2.2 The role of control in privacy literature

When equipped with the belief that one is in control of the information he submitted online, an individual will be more willing to reveal personal information on social network sites (Acquisti & Gross, 2006; Brandtzaeg et al., 2010). When studying this multifaceted control concept, one needs to understand the relationship between privacy control and privacy itself. Focusing on the role of control in extant literature, nature of the association between control and privacy is first explored in this study. Despite the huge amount of publications discussing the relationship between privacy and individuals' perceived control, the description of their relationship is less intricate: only three classifications are identified. The first group of interpretation of this association defines the perception of control as an effective antecedent of privacy; another group holds the view that general privacy is control, per se; in the recent two decades, there are a growing number of scholars starting to treat control as a crucial dimension of privacy, which now becomes a second order construct. A summarization of the above-mentioned perspectives is found in Appendix B.

The concept of control covers many aspects of individuals' submitted information, e.g. who will be granted access to your data, who is privileged to collect and disseminate that information, and under what conditions are the information open for secondary usage (Stone & Stone, 1990; Clarke, 1999; Phelps et al., 2000; Zweig & Webster, 2002; Malhotra et al., 2004; Bélanger & Crossler, 2011). Apart from this general definition of control that depends heavily on FIP conducted at organizational level, it is also found that the sense of individual control can also be attained through IT artifacts and procedures a website provides for users to control the disclosure of their personal information (Milne & Rohm, 2000; Dinev & Hart, 2004). In the 1970s, scholars have

distinguished the concept of objective control (reflection of the reality) from individuals' subjective control (Averill, 1973), and later studies have mainly taken the subjective view and treated control as a psychological perception (Hoadley et al., 2010).

Based on the discussion above, there should be no big surprise to see that the sense of control perceived by individuals using the internet to complete transactions or establish communications bears little resemblance to the reflection of objective control bestowed by data handling organizations (Belanger et al., 2002; Hoadley et al., 2010). One may be well satisfied with the status quo of control over privacy, yet his submitted personal information might have already been passed to third parties, or even be intercepted by unknown groups under the inadequate security defense measures adopted by the company having the data (Brecht et al., 2011). Accordingly, some scholars assert that individuals' control belief equals nothing more than an 'illusion', yet this perception exerts a profound influence on individuals' behavior such as adoption and purchase (Langer, 1975; Wallston, 2001).

Individuals' subjective control can easily be manipulated by features and functions provided by online companies (Goffman, 1963; Leon et al., 2013). In the OSN environment, it is already empirically verified that individuals' control perception can be significantly influenced by the alteration of IT features (Hoadley et al., 2010; Kramer et al., 2014). E.g. Facebook introduced a novel News Feed feature in September 2006, revealing no more information than before, but resulting in immediate criticism from users. Eventually the Facebook CEO at that time had to make an official apology to quell the outcry. In addition, it is also suggested that the granular privacy settings that allow individuals to determine the impressions others form about them will increase individuals' perceived trust and benevolence from the OSN providers, and hence increase their

privacy control (Dwyer et al., 2007; Wang et al., 2011).

2.3 Self-efficacy and perceived usefulness

Across different user types and various IT usage contexts, joint research effort from both the practice and academia examining complicated constructs like self-efficacy and perceived usefulness is of great importance in accurately explaining individuals' usage activities (Segars & Grover, 1993).

2.3.1 Self-efficacy

Although the importance of awareness on privacy related issues is well identified in the IS literature, this construct alone is not sufficient in strengthening people's disclosure intention and boosting their usage activities in OSN environments. People might be well aware that there are fire extinguishers in the building but fail to locate the exact position or do not have the how-to knowledge when it comes to critical junctures. So, apart from the pure awareness of privacy control options provided by OSNs, how to utilize those functions for better privacy personalization experiences should be another key facilitator inducing OSN users' perceived privacy control. This advanced level of awareness regarding the how-to and ease of IT artifacts usage is termed as self-efficacy in this paper, and will be explored as an antecedent of perceived control.

The idea of self-efficacy is already well explored in extant literature. Individuals' self-efficacy over Internet usage, defined as the belief in one's capabilities to organize and execute certain courses of Internet actions, is claimed to be an important factor dividing experienced Internet users from novices (Bandura, 1997; Eastin & LaRose, 2000). According to Belanger et al. (2002; 2011), individuals' self-efficacy of online navigation is one of the six web site features that affect users' usage and adoption activities and worth

more concentrated study. Similarly, the perception of self-efficacy has been found to be positively associated with the diversity of individuals' online activities (Yao et al., 2007), especially their privacy protection behaviors (Chai et al., 2009; Hichang, 2010).

When it comes to the realm of social networks, self-efficacy of the whole bundle of control options and personalization tools becomes something essential to establish trust and loyalty of users (Hsu et al., 2007). It is already empirically shown that self-efficacy of internet usage is an effective predictor of users' attitude and privacy concern toward OSNs (Gangadharbatla, 2008; Mohamed & Ahmad, 2012). In addition, the impact of self-efficacy expectation on OSN users' disclosure activities is found to be mediated by the perception of behavioral control (Shih et al., 2012). Despite the importance, there is still a portion of OSN users who never use the ever-evolving privacy settings and options, indicating a introduction-usage gap between the endless control option potentials and individuals' ability to handle privacy settings (Brandtzaeg et al., 2010). As suggested by Belanger et al. in a recent review, the effect and association patterns of self-efficacy and privacy related constructs should be carefully investigated (Bélanger & Crossler, 2011).

Self-efficacy of personalization tools is not achievable without awareness of the option existence, yet awareness alone is not sufficient to dominant the efficacy perception. According to Bandura (1977), there are four sources affecting individuals' self-efficacy expectations: performance accomplishments, vicarious experience, verbal persuasion and emotional arousal. Based on this statement, the efficacy expectation can be insinuated through verbal persuasion mechanisms such as function tutorials of available control options.

2.3.2 Perceived usefulness (PU)

Another antecedent of control identified in the literature is perceived usefulness (Yun et al., 2014). In essence, privacy control options and other personalization tools offered by OSN providers are IT artifacts ready for people's adoption. In the pervasively adopted technology acceptance model (TAM), PU serves as a key factor influencing individuals' attitude towards IT features and technologies, as well as their adoption behavior (Davis et al., 1989). Subsequent research has repeatedly verified the impact of usefulness perception on individuals' behavioral intention in various contexts (Adams et al., 1992; Venkatesh & Davis, 2000; Zweig & Webster, 2002; Venkatesh & Bala, 2008; Hess et al., 2014). Especially in the OSN context, the PU of privacy control features is claimed to enable control in the content-sharing process (Brandtzaeg et al., 2010), and influence individuals' continuance intention as well (Kwon & Wen, 2010; Jung et al., 2012).

Apart from self-efficacy, PU is another construct that can only be attained and improved after awareness (Brandtzaeg et al., 2010). In an empirical study, the PU of a system which most participants never used before was analyzed and it is proposed that the awareness of privacy practices and policies is positively associated with PU of internet applications (Xu et al., 2008). Similarly, this study hypothesizes that once be aware of the option existence, people will generate usefulness perception based on their own judgement, and the PU should be higher than individuals who are not aware of the privacy control tools. Meanwhile, the existence of privacy control options will possibly insinuate the idea of privacy risks and complex consequences associated with OSN usage into people's understanding (Acquisti & Grossklags, 2005; Yun et al., 2014); hence we also proposes that when equipped with too much awareness, people will be more cautious and less willing to post personal information in OSN environments.

Although the importance of PU is widely recognized, this statement is not exempt from scholars' challenges. Yun et al. (2014) suggest that individuals' PU is not an efficient mitigator of the risk perception, but instead positively associated with individuals' privacy concerns. Especially in the context of hedonic systems such as OSN platforms, PU is said to be a less salient predictor compared with intrinsic motivations such as perceived enjoyment (Van der Heijden, 2004; Rosen & Sherman, 2006; Wu & Lu, 2013). However, when exploring the impact of privacy control features that are devised to enhance individuals' privacy perception, it is not rational to expect any enjoyment from users due to the options' original functionality. Hence, for the purpose of this study, we will only take two awareness-influencing constructs into consideration, i.e. perceived self-efficacy and PU.

2.4 Awareness-increasing techniques

As previously discussed, awareness alone is not sufficient to boost OSN users' control perception to a high level. Self-efficacy and PU of privacy control options should also be improved to safeguard privacy. In this section, the role of online function tutorials in the extant literature will be explored, as well as the impact of warning messages illustrating the potential negative consequences of not utilizing the presented control options.

2.4.1 Tutorials

The effect of tutorials in affecting individuals' psychological procedures is already well verified in the academic world. It is claimed that an individual does not need to engage personally to form his expectation of possible outcomes of an activity; he can simply adjust his estimation based on mental simulation (Acquisti & Grossklags, 2005). According to Bandura (1977), vicarious experience such as leading an individual through

the configuration procedures of certain functions will not only make people aware of the function existence but also enhance their self-efficacy perception. It is also found that usage tutorial of a software can effectively boost individuals' self-efficacy beliefs (Hartzel, 2003). Similarly, presenting individuals with functional tutorials demonstrating the usage of privacy control options is supposed to increase their self-efficacy expectation, as well as reduce the cognitive load of using those options (Silver & Nickel, 2005).

Since it is neither practical nor realistic for OSN providers to offer concrete classroom-based tutorials, online tutorials have gradually become the most pervasively adopted technique to increase individuals' awareness and self-efficacy of available IT features in the virtual world (Dewald, 1999). It is suggested that a well-developed online tutorial not only can generate same learning outcomes as in-person lecture but also is preferable to the majority of online users due to its flexibility of time, distance and location (Ng, 2007; Silver & Nickel, 2005).

2.4.2 Warning messages

Increasing only the self-efficacy of privacy control options should not be the sole purpose of functional tutorials devised by OSN providers. People might find the control options quite easy to use but still refuse to use them under recommended situations due to lack of PU. The usefulness perception, however, just like other perceptions, is subjected to the influence of psychological fluctuations such as an altered evaluation of possible outcomes (Tversky & Kahneman, 1981). This phenomenon is later termed as framing effect, a cognitive bias in which people react to a particular choice in different ways depending on how it is presented (e.g. with or without warning) (Plous, 1993). It is found that warning messages illustrating the negative consequences of online activities will

significantly influence individuals' subsequent behaviors (Cheng & Wu, 2010; Y. Wang et al., 2013; Xiao, 2010; Xiao & Benbasat, forthcoming), which is consistent with protection motivation theory (Maddux & Rogers, 1983; Pechmann et al., 2003). However, formulation of warning messages that incorporates all necessary elements is not an easy task and requires great caution with its design (Drabek, 1999).

Similarly, according to the fear appeals (arousal) theory from marketing, it is suggested that persuasive messages demonstrating the threat of impending negative consequences could be useful in arousing fear among individuals, and hence diverting their behaviors (Hoog et al., 2005; Maddux & Rogers, 1983; Ruiter et al., 2001). A vivid illustration of the fear appeal in real life is the picture of the lungs of a smoker appearing on the tobacco packs. When be warned about the possible negative outcomes of using OSNs, individuals are supposed to be more aware of the risks they are facing, hence perceive higher utility from the available control options. But warning alone is not sufficient to significantly influence OSN users' responses: its impact is moderated by other factors such as individuals' degree of involvement (Cheng & Wu, 2010). According to Chai et al. (2009), education opportunities that promote the usage of control options play an important role in positively affecting the internet users' perception as well as protective behavior regarding online privacy. Thus, it is reasonable to assume a combination of framing effects and educational techniques is effective in affecting individuals' privacy related perceptions.

2.5 Disclosure intention

The initial purpose of the Internet is to facilitate collaborative work and interaction among users (Wellman, 2001). It is especially so in the context of OSN since it is the very IT

creature that is designed to enhance people's social relationships, and to form or maintain connections between individuals (Haythornthwaite, 2005; Ellison & others, 2007; Ellison et al., 2007;). For benefits such as psychological well-being or fulfilment, OSN users disclose astonishing and varied amount of personal information (Gross & Acquisti, 2005; Tufekci, 2008), and their disclosure behaviors are strongly predicted by individuals' disclosure intention (Ajzen & Fishbein, 1977; Ajzen, 1991).

When engaging in social interactions via OSNs, there are various occasions under which individuals will disclose personal information (Gross & Acquisti, 2005). One can choose to complete personal profile on Facebook for easier searchability from acquaintances, post one's daily activities such as a family reunion, or comment on photos posted by friends with self-identifiable information such as one's workplace. According to the theory of planned behavior (TPB), people's behavioral control beliefs, defined as the perception of the availability of skills, resources, and opportunities, have a direct impact on their intention of corresponding activities, hence further influence their actual behaviors (Ajzen, 1985, 1991). Accordingly, it is proposed in the IS domain that individuals' privacy-related beliefs are correlated with their disclosure intention (Liu et al., 2005; Bélanger & Crossler, 2011).

Privacy perception is not always considered as an effective predictor of individuals' disclosure intention; it is even repeatedly found that individuals disclose huge amount of information regardless of their level of privacy concern (Awad & Krishnan, 2006; Barnes, 2006; Smith et al., 2011; Sutanto et al., 2013). In the OSN environments, it is found that individuals' privacy concerns are only a weak predictor of his ONS membership, and that individuals with high privacy awareness join the network and reveal great volume of personal information as well (Acquisti & Gross, 2006). Tufekci (2008) proposes that

there is little to no relationship between online privacy concerns and information disclosure on OSNs. Similarly, the negative correlation between personal disclosure and information control is found to be non-significant (Christofides et al., 2009). However, current research exploring the association between privacy-related constructs and people's disclosure intention has mainly focused on the control perception triggered by privacy practices conducted at the organizational or legislation level. In order to provide some insight into the impact of personalization-enabled control, this study aims to explore its impact on individuals' disclosure intention in the OSN contexts.

2.6 General privacy concern

Since studies exploring the impact of information privacy have frequently been impeded by the near impossibility of measuring privacy itself, individuals' concern over privacy has been pervasively adopted by scholars as a proxy of privacy in empirical studies to capture the cognition and perception regarding privacy (Smith et al., 1996; Smith et al., 2011; Yun et al., 2014). There are two validated instruments measuring privacy concern: concern for information privacy (CFIP) and Internet user's information privacy concerns (IUIPC) (Bélanger & Crossler, 2011). CFIP scale is composed of 15 items tapping into four privacy dimensions: the collection of data, unauthorized secondary use of data, improper access to data, and errors in data (Smith et al., 1996). Drawing on social contract theory, Malhotra et al. (2004) proposed the IUIPC instrument specifically designed for online environments that incorporate three dimensions: collection, control, and awareness. Both these two well adopted instruments are measuring individuals' general privacy concern, not taking the situational factors such as the context of a specific website into account (Li et al., 2010; Xu et al., 2011; Li, 2014). In this study, general privacy concern represents individuals' trait-based concern over privacy, and will

be measured with extant items as one control variable.. Prior research has found that personality traits have a direct influence on individuals' general privacy concerns (Xu, et al., 2012).

2.7 Propensity to share

As social creatures, human beings have an innate propensity to share (Nadkarni & Hofmann, 2012). The need for social interaction is so salient that people continue their sharing activities even after unpleasant experiences such as regretting some posted content (Wang et al., 2013). Unlike the e-commerce environments where people disclose for transactional benefits, OSN users share personal information in order to establish intimacy and express themselves (Cozby, 1973; Olivero & Lunt, 2004; Livingstone, 2008). According to Brief and Motowidlo (1986), sharing activities are forms of prosocial behaviors and are conducted to maintain the well-being and integrity of others and the self. In line with this statement, it is found that people's propensity to share, defined as a personal norm reflecting the costs and benefits of sharing, affects information disclosure activities (Constant et al., 1994; Jarvenpaa & Staples, 2000).

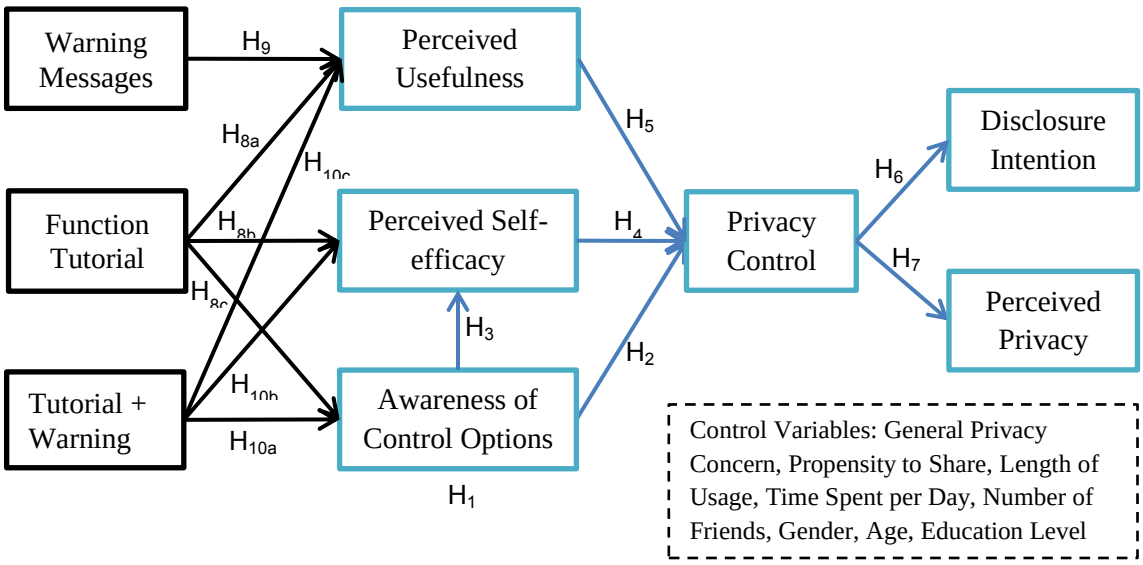
Under the 'privacy calculus' view, it is suggested that individuals will make information disclosure decisions based on rational evaluation of risk and benefit perceptions (Awad & Krishnan, 2006; Dinev & Hart, 2006; Li et al., 2010; Kehr et al., 2015). While individuals' risk perceptions are found to have a mitigating impact on their disclosure intention (Acquisti & Grossklags, 2005), the benefit of personal information disclosure is positively associated with individuals' disclosure intention, e.g. people with strong propensity to share are more likely to assign high psychological weight to the social and personal good from sharing and thus more willing to engage in sharing activities

(Jarvenpaa & Staples, 2000). Studies exploring individuals' propensity to share will possibly generate new insight into the privacy paradox phenomenon by introducing new element that has a positive impact on individuals' disclosure intention. Based on the privacy calculus view discussed in the literature review section, we believe that controlling for the risk perception, people with high degree of propensity to share will perceive greater benefit from posting activities, and thus more likely to disclose personal information in OSNs. Thus, this study proposes that the OSN users' propensity to share is positively associated with their disclosure intention.

3. Research Framework

This research aims to explore the impact of awareness, as well as self-efficacy and perceived usefulness (PU) of privacy control options on individuals' privacy perception and disclosure intention in OSN environments. It is hypothesized that individuals' perceived control over their privacy mediates the effect of awareness, self-efficacy and PU of control options on OSN users' posting intention and perceived privacy. The overarching research framework with corresponding hypotheses is summarized in Figure 3.1. In the hope of evaluating people's usage pattern of privacy control options in a feasible manner, this study aims to focus only on the OSN environments, where most of the devised IT-enabled control options are contributing to.

Figure 3.1 Research framework



3.1 The impact of awareness

Earlier research has stated that there should be substantial awareness of online features and resources due to individuals' frequent and diversified internet usage (Yao et al.,

2007). While this statement bears some merit, it has been challenged in the recent decade, particularly in the OSN context, where individual users have been overwhelmed with hundreds of IT artifacts provided by different platforms. It is found that even at the most preliminary level of option availability, 52 percent of the public, including 45 percent of those who shop by mail, are not aware of name removal procedures (Phelps et al., 2000). For the available control options this study chose, we believe the OSN users on average are aware of no more than 80 percent of the options. Thus, when term high level of awareness of control options as knowledgeable of at least 80 percent of the control options we present, this study proposes that:

H1: OSN users do not possess a high level awareness (≥ 80%) of currently available privacy control options.

From the designers' perspective, the awareness of privacy control options is expected to exert a direct influence on individuals' perceived control. In line with this assumption, perceived control over privacy has been repeatedly identified in literature as an influential factor that affects the shaping process of individuals' privacy perceptions in various domains (Xu et al., 2011; Li, 2014). Specifically in the OSN field, dozens of new IT artifacts addressing people's privacy perceptions have been devised or suggested by researchers from both the academia and practice (Tsai et al., 2011). Empirical results have shown that apart from awareness of privacy practices conducted by organizations, the state of privacy can only be achieved co-existent with the awareness of privacy control options such as granting users with account deactivating options (Culnan, 1995; Milne & Rohm, 2000; Yeung et al., 2009). However, along with the fast accumulation of control options, few academic studies have looked closely at the impact of awareness of control options on individuals' privacy control. To address this research gap, it is first

hypothesized in this study that the awareness of control option has a direct impact on individuals' privacy control.

H2: Awareness of privacy control options is positively associated with individuals' perceived privacy control.

Apart from the direct impact of awareness on individuals' privacy control, we propose that individuals' awareness of control options is assumed to be positively associated with their self-efficacy. Although there is no guarantee that the available control options, if known by users, are perceived as easy-to-use, the majority of control options provided by OSNs are designed in an intuitive way, such as, on-and-off switches and available choices in a menu. Once be acknowledged of the existence of certain control options, OSN users should be able make analogy to the control options that they are already aware of and gain a preliminary level of self-efficacy accordingly. Thus, it is hypothesized that:

H3: Awareness of privacy control options is positively associated with individuals' perceived self-efficacy of control options.

In addition, it is proposed that 'too much' awareness of control features, given the diversity and large amount of available control options, will insinuate negative perceptions (e.g. privacy risk) into OSN users' mind, thus has a mitigating effect on individuals' disclosure intention regardless of the level of privacy control they perceived. Thus, it is proposed in this study that too much awareness of available privacy control options will mitigate the influence of privacy control OSN users' disclosure intention.

3.2 Self-efficacy and perceived usefulness

Provided that people already have enough awareness of available privacy control options, it is worthwhile to explore whether they have enough self-efficacy and PU. As

discussed in the previous section, awareness alone is not sufficient for privacy control improvement. One has to possess enough knowledge to handle the usage and configuration of the privacy control options to attain personalization-enabled control. As mentioned in the previous section, the significance of self-efficacy is already well accepted by IS scholars and this construct is adopted as an important factor dividing experienced Internet users from novices (Bandura, 1997; Eastin & LaRose, 2000). Hence, we hypothesize that:

H4: Self-efficacy of using privacy control options is positively associated with individuals' perceived privacy control.

Apart from self-efficacy which is capable of increasing individuals' ease of usage, PU is another necessary factor that influence people's attitude towards privacy control options, and further affect their control perception (Davis et al., 1989; Venkatesh & Davis, 2000). As previously mentioned, researchers have repeatedly verified the impact of perceived usefulness on individuals' behavioral intention (Adams et al., 1992; Zweig & Webster, 2002; Venkatesh & Bala, 2008; Hess et al., 2014). Apart from studying the impact of awareness of control options, this study also aims to explore the influence of PU on individuals' perceived control, as well as possible techniques to improve OSN users' awareness, self-efficacy and PU. Accordingly, we hypothesize that:

H5: Perceived usefulness of privacy control options is positively associated with individuals' perceived privacy control.

3.3 Perceived privacy and posting intention

As discussed in the previous section, privacy on OSNs cannot be guaranteed solely by users' awareness of privacy practices conducted at the organizational and legislation level. The design of a sophisticated website should, rather, offer users the means and

options to determine their own level of privacy controls, and make sure that they are aware of those IT artifacts (Brandtzaeg et al., 2010). To better understand the practical outcomes of awareness, self-efficacy and PU, the subjective control perceived by individuals will be analyzed as a predictor of privacy in this research. The antecedent view is chosen because individuals' awareness of privacy control options is most likely to increase a specific dimension of control over privacy, yet its impact is not sufficient to influence every identified privacy aspects. In the analysis conducted in the following sections, disclosure intention and perceived privacy, which is defined as the amount of privacy perceived by OSN users in this study, will be analyzed as outcome variables:

H6: Individuals' perceived privacy control is positively associated with their disclosure intention.

H7: Individuals' perceived privacy control is positively associated with their perceived privacy.

3.4 Function tutorial and warning messages

If OSN users do not possess sufficient awareness or self-efficacy of privacy control options, it is necessary to utilize awareness or self-efficacy enhancing techniques to seek improvement. While a single privacy control function may not cause difficulties in understanding among users, two dozens of control options provided by a social network (e.g. Facebook ("Privacy Help Center," 2015)) may not be as intuitive to ordinary users based on the anecdotal evidence. Thus, online educational techniques that can improve OSN users' awareness, self-efficacy and PU of privacy control options should be carefully studied. According to Bandura (1977), interpretive treatments such as function tutorials will not only improve individuals' awareness of illustrated features but also change their efficacy expectations of handling the specific features and. Moreover,

individuals will mentally generate usefulness perception to the control options the moment they are acknowledged of the existence. Thus, we hypothesize that:

H8a: Function tutorial illustrating the usage of privacy control options will increase individuals' awareness of privacy control options.

H8b: Function tutorial illustrating the usage of privacy control options will increase individuals' perceived self-efficacy of privacy control options.

H8c: Function tutorial illustrating the usage of privacy control options will increase individuals' perceived usefulness of privacy control options.

The framing effect such as showing negative consequences to individuals to increase their risk perception has repeatedly been found effective in the IS domain (Plous, 1993; Cheng & Wu, 2010; Xiao, 2010; Wang et al., 2013). This finding is consistent with the fear appeal theory in marketing, which suggests that warning messages presenting privacy risk or vulnerability to the risk will arouse fear of impending danger, and hence divert individuals' relevant behavior (Maddux & Rogers, 1983; Ruiter et al., 2001; Hoog et al., 2005). Thus, this study proposes that warning messages showing people the potential negative consequences of not using or configuring certain privacy control options will increase people's PU of control options, and further influence their information disclosure behaviors. We hypothesize that:

H9: Warning messages showing the potential negative consequences of not configuring privacy control options will increase individuals' PU of those options.

Function tutorials illustrating the usage of privacy control options are supposed to boost OSN users' awareness, as well as their perceived self-efficacy and PU. But the PU improved by function tutorials is simulated by the unaware→ aware process of control option acknowledgement, while warning messages are supposed to improve individuals' PU by increasing their perceived vulnerability when not configuring certain privacy

control options (Rogers, 1975). There is no clear evidence demonstrating how the awareness-triggered PU is affected by framing effect such as warning messages. This study will explore whether the impact of function tutorial and warning messages on individuals' PU and privacy control are additive. Deriving from the protection motivation theory (Maddux & Rogers, 1983; Pechmann et al., 2003), we expect that function tutorials incorporating warning messages are effective to improve OSN users' awareness, self-efficacy and PU of available privacy control options in the sense that warning messages will increase OSN users' PU, yet have no predicable negative influence on their awareness and self-efficacy of control options.

H10a: Function tutorial incorporating warning messages will increase individuals' awareness of privacy control options.

H10b: Function tutorial incorporating warning messages will increase individuals' perceived self-efficacy of privacy control options.

H10c: Function tutorial incorporating warning messages will increase individuals' PU of privacy control options.

4. Study Design

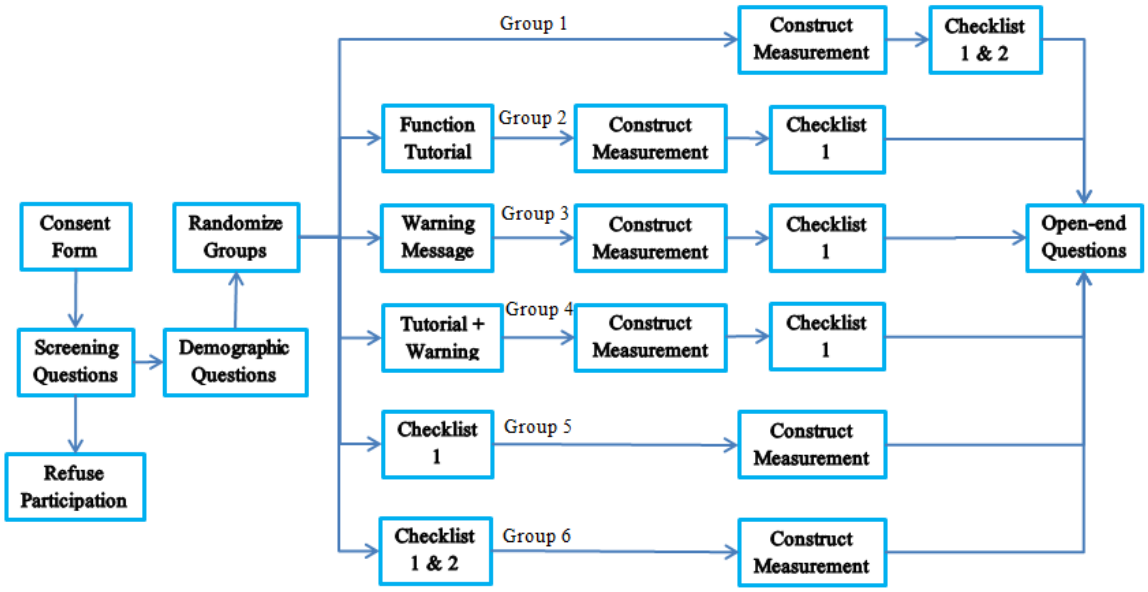
The hypothesized associations described in the previous section were tested via an online survey. The survey instrument was devised to capture individual's privacy related perceptions based on different awareness-increasing mechanisms (e.g. tutorials). Among current OSN platforms, Facebook was chosen for this study. Long been recognized as the worldwide market leader, Facebook reported more than 1.4 billion active user accounts as of March 2015 ("Social networks," 2015). We believe that by choosing this most prevalent OSN platform, the greater generalizability of this study can be attained. In addition, there are more than 40 available privacy control options on Facebook ("Privacy Help Center," 2015), and the abundance of privacy settings offers this study convenience to explore the impact of awareness, as well as too much awareness of privacy control options. Moreover, there are hundreds of function tutorials available online, making it easier for the authors to devise treatment tutorials that accurately and faithfully reflect privacy control functions on Facebook.

The online survey used to test the proposed research model was designed using the 'Qualtrics Survey' platform. As for data collection, Amazon Mechanical Turk (AMT) was used to recruit subjects and administer the survey and. We require a study participant to be at least 19 years of age and be capable of providing consent on his own behalf. In addition, each subject should be able to identify the icon of Facebook among icons of four other OSNs, and login to Facebook at least on weekly basis. These requirements are checked through screening questions. This is to ensure that all the subjects are knowledgeable of basic Facebook usage, and will not be bewildered by the option checklists or function tutorials presented later in the survey.

As to the design of online function tutorials, it is suggested that tutorials utilizing graphical representations are more effective in affecting individuals' learning outcomes than the text-based ones (Lim & Benbasat, 2000), e.g. an interface demonstration showing where to find a specific function is easier for individuals to understand than a text only instruction. Developers should also keep in mind that the tutorial devised should neither be too lengthy that can give rise to boredom (Cheung et al., 2003), nor should it be too complicated or demanding in terms of decision-making and visual processing (DeStefano & LeFevre, 2007). The utmost goal of tutorial development is to improve individuals' confidence and self-efficacy of target activities using multimedia instruction that cost minimal cognitive load (Oud, 2009). Following the guidance above, function tutorials combining text-based introduction and graphical demonstrations are developed for this study, as shown in Appendix E.

If a subject decides to participate in this study, he will be invited to fill out the online survey we devised. First, he will be presented with screening questions previously described. If qualified, he will be asked to answer some basic demographic questions and also some questions measuring their general privacy concern and propensity to share. Basic demographic questions of the survey can be found in Appendix A. After completing demographic questions, recruited participants will be randomly assigned to one of the six treatment groups. Survey procedures for each treatment group are illustrated in Figure 4.1.

Figure 4.1 Procedure diagram for each treatment groups



- Demographic questions: general demographic questions, general privacy concern and propensity to Share
- Checklist 1: control options for Timeline and Tagging Management
- Checklist 2: control options for Security, Privacy, Apps and Ads Management
- Key construct measurement: perceived self-efficacy, PU, perceived control, perceived privacy and disclosure intention

As shown in Figure 4.1, subjects in each of the six treatment groups will be asked to identify their awareness of available privacy control options. The instrument used in this study to capture individuals' awareness is two checklists of privacy control options provided by Facebook. Checklist 1 contains the names and function introduction of eight privacy control features specifically classified as 'Timeline and Tagging Management' options on Facebook. Checklist 2 introduces 16 other privacy control options covering three major privacy control dimensions on Facebook: Security Management, Basic Privacy Management, Apps and Ads management. In addition, key constructs of this study will be measured using extant or newly devised items. At the end of the survey, each subject will be invited to offer any feedback to us via two open-ended questions.

Detailed presentation order of key components of the survey for each treatment groups can be found in Appendix C. A detailed development procedure of survey components (e.g. tutorials) can be found in Appendix D. Demographic questions, two control option checklists, measurement items of key constructs and treatment tutorials developed for this study can be found in Appendix E.

5. Data Analysis

5.1 Study sample

Altogether 364 AMT workers have completed our online survey. After removing duplicate attempts in answering the survey and subjects unqualified for the analysis (e.g. failed attention check), 297 active Facebook users constituted the final analysis sample. Detailed data cleaning procedure can be found in Appendix F.

In the final sample, 78 percent of the participants were under 40 years of age; over 99 percent had received high school or higher level education, and 168 of them were males. All of the participants have more than one year usage experience of Facebook, and 61 percent of them on average spent no less than 30 minutes a day on Facebook, while only 13 percent of the participants use Facebook less than 10 minutes per day. In addition, 29 percent of the participants have less than 100 friends on Facebook, 49 percent of them have less than 400 and 22 percent have no less than 400 Facebook friends. Moreover, 96 percent of the participants had chosen browsing through new posts by their friends as their most regular activities on Facebook; 72% considered Facebook as an important channel to chat with their friends; and 65 percent used Facebook as a platform to share their thought and pictures via new posts. More comprehensive sample demographics and group distribution are summarized in Appendix G. No significant differences were found among the six treatments groups in terms of the participants' general demographics, general privacy concern and propensity to share.

Among the three items measuring awareness of control options in this study, the first item is calculated as the number of control options that a participant has specified 'yes, I

am aware of' in checklist 1, representing an objective reflection of the participant's awareness of control options. For group 1, 5 and 6, participants' original level of awareness of control options without the influence of tutorials were measured and compared. No statistically significant difference in objective awareness (the first item) regarding the eight control options in checklist 1 were found among group 1, 5 and 6 (tested via one-way ANOVA, p = 0.43); and no statistically significant difference in objective awareness regarding the 16 control options in checklist 2 were found between group 1 and 6 (tested via independent t–test, p = 0.62). Given the fact that participants are randomly assigned into different groups to answer the online survey, it is assumed that participants in group 2, 3 and 4 should have possessed the same level of objective awareness of control options at the beginning of the study.

5.2 Awareness of privacy control options

There were 8 options presented in checklist 1 and 16 options listed in checklist 2. The descriptive statistics of group 1, 5 and 6 show that Facebook users have, on average, only a medium level of awareness of available privacy control options on Facebook, as shown in Table 5.1. Comparing with the 80% threshold (6.4 for checklist 1, 12.8 for checklist 2), OSN users do not possess high level awareness of control options listed in both checklists (p < 0.001). This finding supported H1, which proposes that OSN users do not have a high level of awareness (≥ 80%) of control options.

Table 5.1 Awareness level summary

Awareness level of checklist 1 (group 1, 5, 6)

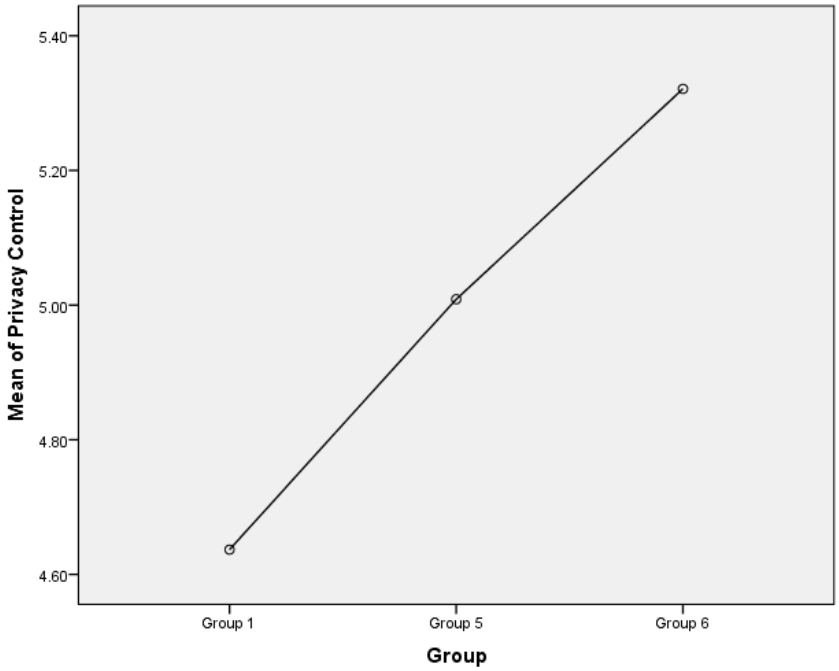
N	Minimum	Maximum	Mean	Std. Deviation	Sig.
152	0	8	5.46	2.02	<0.001

Awareness level of checklist 2 (group 1, 6)

N	Minimum	Maximum	Mean	Std. Deviation	
103	0	16	8.27	3.70	<0.001

The impact of awareness on individuals' privacy control was first explored through the mean comparison of privacy control among group 1, 5 and 6. The latent factor score for privacy control used for one-way ANOVA comparison was calculated using SmartPLS 2.0 (Ringle et al., 2005). The result suggested that there was a significant difference on participants perceived privacy control among group1, 5 and 6, F (2, 149) = 4.85, p < 0.01. Post hoc comparisons using the Bonferroni test indicated that the mean score for privacy control in group 6 (M = 5.32, SD = 0.79) was significantly higher than the mean score for the control group (M = 4.64, SD = 1.28). However, the mean score for privacy control in group 5 (M = 5.01, SD = 1.23), did not significantly differ from group1 and group 6. Despite the non-significant difference, it can be seen from the mean comparison that participants' privacy control has increased correspondingly with the presentation of checklists. This finding is consistent with H2 that awareness of control options is positively associated with perceived privacy control. The mean plot of privacy control of group 1, 5, 6 is shown in Figure 5.1.

Figure 5.1 Mean plot of privacy control



5.3 Manipulation check

Before structural equation modeling (SEM) technique was used to test the proposed research model, manipulation checks are conducted to see if the warning messages and tutorials have served the desired purposes. ANOVA tests were performed in terms of three manipulated variables: awareness, self-efficacy and PU of privacy control options. Items measuring these three constructs can be found in Appendix E. Group classification for each manipulated variable is listed in Table 5.2. It is found that tutorials developed for this study were effective in increasing individuals' awareness, self-efficacy, and PU of control options, and warning messages successfully improved participants' PU of control options, as shown in Table 5.3. Moreover, MANOVA comparing awareness, self-efficacy and PU between group 1, 2, 3 and 4 indicates that participants in group 2 and group 4 (groups with tutorial) showed significantly higher awareness ($p_{group2} < 0.01$, $p_{group4} < 0.01$) and self-efficacy ($p_{group2} = 0.01$, $p_{group4} < 0.01$) of control options than those in

group 1, while group 3 was not significantly different from the control group in terms of awareness or self-efficacy, as shown via Bonferroni post-hoc tests. The results of Bonferroni post-hoc test among groups 1 to 4 also show that participants in group 2 and group 3 perceived significantly higher PU ($p_{group2} < 0.05$, $p_{group3} < 0.05$) than group 1, while group 4 was not significantly different from the control group regarding the level of PU ($p = 0.16$). MANOVA results can be found in Table 5.4. H8, H9, H10a and H10b are all supported accordingly.

Table 5.2 Manipulated variables and corresponding groups

Level / Variable	High	Low
Awareness	Group 2, 4	Group 1, 3
PSE	Group 2, 4	Group 1, 3
PU	Group 2, 3, 4	Group 1

Table 5.3 Manipulation check

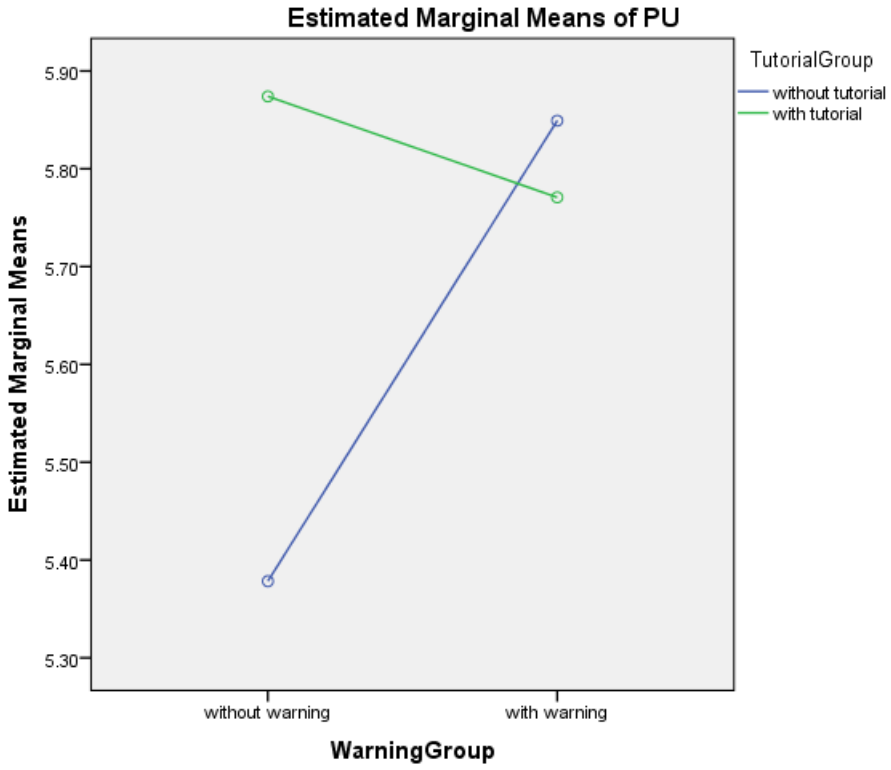
Source	Mean	Sum of Squares	df	Mean Square	F	Sig.
Awareness	Low: 4.82	Between Groups: 13.68	1	13.68	9.13	.003
	High: 5.35	Within Groups: 289.13	193	1.50		
		Total: 302.81	194			
PSE	Low: 5.77	Between Groups: 6.18	1	6.18	8.78	.003
	High: 6.13	Within Groups: 135.75	193	0.70		
		Total: 141.93	194			
PU	Low: 5.38	Between Groups: 7.64	1	7.64	10.26	.002
	High: 5.83	Within Groups: 143.63	193	0.74		
		Total: 151.27	194			

Table 5.4 MANOVA results

Source		Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	Awareness	137.282	3	45.761	22.897	.000
	PSE	11.058	3	3.686	5.379	.001
	PU	7.919	3	2.640	3.517	.016
Intercept	Awareness	8007.458	1	8007.458	4006.738	.000
	PSE	6906.309	1	6906.309	10079.537	.000
	PU	6373.964	1	6373.964	8492.596	.000
Tutorial Group	Awareness	136.827	1	136.827	68.465	.000
	PSE	6.038	1	6.038	8.812	.003
	PU	2.121	1	2.121	2.826	.094
Warning Group	Awareness	.226	1	.226	.113	.737
	PSE	3.431	1	3.431	5.008	.026
	PU	1.647	1	1.647	2.194	.140
Tutorial Group * Warning Group	Awareness	.125	1	.125	.062	.803
	PSE	1.428	1	1.428	2.084	.151
	PU	4.015	1	4.015	5.349	.022

Furthermore, 2 (with or without tutorials) by 2 (with or without warning messages) ANOVAs were conducted to see if there are interactions regarding the presence of function tutorials and warning messages. It is found that although the two techniques are supposed to improve individuals' PU of control options though different tracks, their PU-increasing effect are not exerted in an additive manner. A statistically significant interaction between function tutorials and warning messages regarding the level of PU is found (p =0.02), suggesting that for groups without tutorials, PU will rise significantly when presented with warning messages; while in the tutorial groups PU remains at a high level regardless of the presence of warning messages (Figure 5.2). No significant interaction between function tutorials and warning messages was found regarding awareness (p = 0.52) or self-efficacy (p = 0.15) of control options.

Figure 5.2 Interaction plot of PU



5.4 Measurement validation of the research model

SEM technique was used to test the measurement model of the proposed research framework. Barclay et al. (Barclay et al., 1995) suggest that for the purpose of measurement model assessments, reliability of individual measurement items, internal consistency and discriminant validity of latent variables should all be calculated and checked. According to Chin (1998), the loadings of each measurement item on its intended construct should exceed the recommended tolerance of 0.7 to demonstrate good item reliability. Only the first four treatment groups are included in the SEM analysis because the key constructs (e.g. privacy control) of group 5 and group 6 are measured after the serving of checklists. Hence, the key constructs measured in these groups are based on the improved awareness while the awareness level recorded at the

beginning of the survey is no longer valid.

Except the first item measuring awareness of control options, all other indicators loaded most highly on their own theoretically assigned construct, and at a minimum threshold of 0.78, as shown in Table 5.5 and Table 5.6. The first item of awareness has highest loading on awareness with a marginally significant loading (0.68). Given the fact that the first item is purely objective (number of aware options) and serves as a key indicator of awareness of control options, it is kept for future analysis.

Table 5.5 Loadings of measurement items

Item	Dimensions/Questions	Mean	STD	Loading
	Awareness			
Awareness1	Number of aware options in checklist 1	4.76	1.45	0.678
Awareness2	Overall usage experience of the functions presented in checklist 1, based on a scale from 1 to 7	6.41	1.64	0.882
Awareness3	Overall familiarity of the functions presented in checklist 1, based on a scale from 1 to 7	4.55	1.40	0.930
	Perceived self-efficacy			
PSE1	I am capable of using control options on Facebook to control my timeline.	6.06	0.86	0.907
PSE2	I am confident of using control options to manage my tags on Facebook.	5.79	1.06	0.924
PSE3	I am capable of using control options on Facebook to control my photos.	5.96	0.92	0.898
	PU			
PU1	I find the control options provided by Facebook useful to protect my privacy.	5.56	1.08	0.865
PU2	I find the control options provided by Facebook help me to keep my personal information and posts from the unwanted audience.	5.52	1.17	0.878
PU3	The control options provided by Facebook help me to manage my timeline and my posts.	5.86	0.95	0.875
PU4	The control options provided by Facebook help me to manage my photos and tags.	5.86	0.90	0.867
	Privacy Concerns			
PC1	I am concerned that too much information about me and my online activities has been purposely collected.	5.08	1.48	0.927
PC2	I am concerned about my privacy when I am browsing through websites.	5.20	1.45	0.930

Item	Dimensions/Questions	Mean	STD	Loading
PC3	I am concerned that the personal information I disclosed online could be misused.	5.34	1.44	0.932
PC4	I am concerned that the personal information I disclosed online could be accessed by unknown parties.	5.48	1.42	0.950
	Propensity to share			
PTS1	I feel happy to share my thoughts and pictures with my friends through online social networks such as Facebook.	5.25	1.19	0.899
PTS2	Sharing my thoughts and pictures on social networks such as Facebook is a pleasure to me.	5.09	1.19	0.913
PTS3	It feels natural for me to share my thoughts and pictures on social networks such as Facebook.	4.95	1.36	0.877
PTS4	I find sharing my thoughts and pictures on social networks such as Facebook is fun and interesting.	5.26	1.23	0.931
	Perceived privacy control			
PCtrl1	I feel I have control over who can get access to my shared content such as posts and photos on Facebook.	5.06	1.41	0.904
PCtrl2	I have control over what personal information I disclosed could be accessed by other people on Facebook.	5.08	1.31	0.910
PCtrl3	I believe I have control over what activities other people can perform (e.g. comment or tag a photo) with my shared personal information on Facebook.	5.11	1.36	0.788
	Perceived privacy			
PP1	I feel I have enough privacy when I use Facebook.	4.39	1.59	0.953
PP2	I am comfortable with the amount of privacy I have on Facebook.	4.47	1.60	0.961
PP3	I think my privacy is preserved when I use Facebook.	4.17	1.59	0.932
PP4	I am satisfied with my state of privacy when I use FB.	4.41	1.59	0.963
	Disclosure intention			
DI1	I am willing to disclose my personal information (e.g. post daily activities) on Facebook in the future.	4.61	1.60	0.933
DI2	It is probable for me to disclose my personal information to Facebook for daily social activities and other relevant usages.	4.65	1.54	0.911
DI3	It is possible for me to disclose my personal information to Facebook in the future to get connected with my friends	5.05	1.34	0.879
DI4	Given the need, I am willing to provide my personal information to Facebook in order to get the benefit of using it.	4.73	1.52	0.879

PCtrl: privacy control; PSE: perceived self-efficacy; PU: perceived usefulness; DI: disclosure intention; PP: perceived privacy; GPC: general privacy control; PTS: propensity to share

Table 5.6 Cross-loadings of measurement items

	Awareness	PSE	PU	GPC	PTS	PCtrl	PP	DI
Awareness1	0.678	0.224	0.143	-0.003	-0.017	0.155	0.077	0.023
Awareness2	0.882	0.241	0.048	-0.050	0.048	0.044	-0.001	-0.132
Awareness3	0.930	0.343	0.186	-0.056	0.178	0.140	0.102	0.027
PSE1	0.279	0.907	0.520	0.007	0.202	0.415	0.208	0.219
PSE2	0.330	0.924	0.517	-0.054	0.218	0.442	0.221	0.225
PSE3	0.294	0.898	0.469	-0.002	0.149	0.394	0.161	0.172
PU1	0.143	0.413	0.865	-0.103	0.444	0.472	0.542	0.436
PU2	0.129	0.451	0.878	-0.084	0.377	0.508	0.523	0.434
PU3	0.164	0.535	0.875	-0.080	0.323	0.494	0.389	0.303
PU4	0.124	0.528	0.867	0.031	0.331	0.456	0.310	0.258
PC1	-0.064	-0.048	-0.082	0.927	-0.200	-0.273	-0.458	-0.264
PC2	-0.007	-0.042	-0.088	0.930	-0.118	-0.293	-0.457	-0.276
PC3	-0.047	0.041	-0.025	0.932	-0.153	-0.234	-0.416	-0.192
PC4	-0.054	-0.013	-0.058	0.950	-0.126	-0.308	-0.433	-0.190
PTS1	0.166	0.252	0.430	-0.124	0.899	0.238	0.410	0.474
PTS2	0.074	0.197	0.400	-0.093	0.913	0.212	0.361	0.454
PTS3	0.068	0.170	0.371	-0.184	0.877	0.254	0.431	0.469
PTS4	0.054	0.146	0.339	-0.167	0.931	0.269	0.447	0.534
PCtrl1	0.115	0.364	0.487	-0.297	0.228	0.904	0.676	0.412
PCtrl2	0.080	0.353	0.469	-0.302	0.235	0.910	0.690	0.417
PCtrl3	0.185	0.504	0.498	-0.168	0.244	0.788	0.465	0.349
PP1	0.027	0.185	0.485	-0.433	0.436	0.686	0.953	0.578
PP2	0.044	0.173	0.464	-0.463	0.409	0.689	0.961	0.598
PP3	0.138	0.207	0.469	-0.445	0.440	0.665	0.932	0.587
PP4	0.093	0.262	0.518	-0.458	0.455	0.682	0.963	0.628
DI1	-0.014	0.174	0.397	-0.242	0.478	0.406	0.587	0.933
DI2	-0.017	0.207	0.343	-0.244	0.500	0.379	0.575	0.911
DI3	-0.056	0.209	0.335	-0.172	0.490	0.380	0.485	0.879
DI4	0.012	0.226	0.410	-0.231	0.460	0.467	0.612	0.879

PCtrl: privacy control; PSE: perceived self-efficacy; PU: perceived usefulness; DI: disclosure intention; PP: perceived privacy; GPC: general privacy control; PTS: propensity to share

It is suggested that the loading of a measurement item on its assigned latent variable should be an order of magnitude larger than any other loading with other latent variables (Gefen & Straub, 2005). This study took an iterative approach in assessing the cross-

loadings shown in Table 5.6 and found that all the items have loadings on the assigned latent variables at least 0.10 higher than the correspondingly second highest loading, suggesting good discriminant validity among latent variables in this study.

The composite reliability and Cronbach's alpha were calculated for each latent variable in order to validate the internal consistency of the constructs, as shown in Table 5.7. All key constructs of this study have met the recommended tolerance (0.70) level suggested by Fornell and Larcker (1981). In addition, Harman's one-factor test was used to examine the presence of Common Method Bias (CMB) in this study. According to Podsakoff and Organ (1986), CMB is considered a problem if 1) items tend to load on a single general factor (i.e., only one single factor emerges from the factor analysis), or 2) one of the variables contributes more than 50 percent of the total variance. All the measurement items in the research model are placed into a principle component analysis (PCA) and 5 factors with eigenvalues greater than 1 are extracted. The first factor accounted for less than 40 percent of the variance and the 5 factors together accounted for 78 percent of the total variance. The data collected for this study is unlikely to have a considerable amount of CMB.

Table 5.7 Internal consistency of constructs

	CA	Aware	DI	GPC	PCtrl	PP	PSE	PTS	PU
Aware	0.78	1							
DI	0.92	-0.021	1						
GPC	0.95	-0.046	-0.247	1					
PCtrl	0.84	0.141	0.454	-0.299	1				
PP	0.97	0.079	0.628	-0.473	0.715	1			
PSE	0.90	0.332	0.227	-0.019	0.459	0.217	1		
PTS	0.93	0.099	0.535	-0.158	0.270	0.457	0.210	1	
PU	0.89	0.161	0.412	-0.070	0.555	0.508	0.552	0.423	1

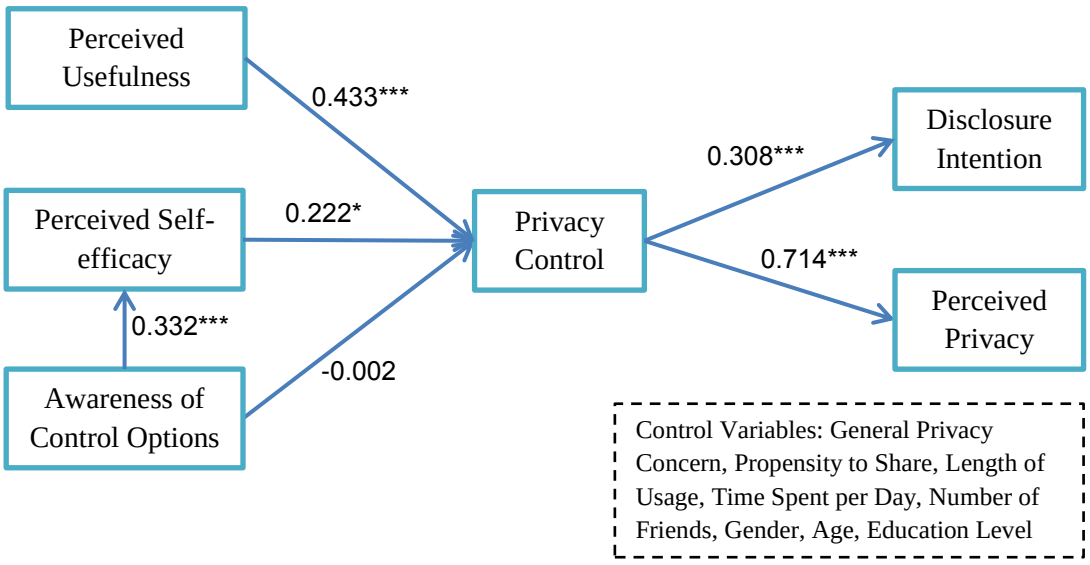
CA: Cronbach's alpha; PCtrl: privacy control; PSE: perceived self-efficacy; DI: disclosure intention; PP: perceived privacy; GPC: general privacy control; PTS: propensity to share

5.5 Test of the research model

5.5.1 Structural equation modeling

SmartPLS 2.0 was used to test the structural model, as shown in Figure 5.3. Coefficients and corresponding significance of hypothesized associations are summarized in Table 5.8. Instead of a direct impact on privacy control, awareness exerts its impact through self-efficacy of control options. All other hypothesized relationships are supported. Perceived self-efficacy, PU, and general privacy concern jointly explained 41 percent of the variance in privacy control, while the propensity to share and privacy control have jointly explained 39 percent of the variance in disclosure intention.

Figure 5.3 Testing result of the structural model



***p<0.001, **p<0.01, *p<0.05

Table 5.8 Test of study hypotheses

Hypothesis	Path	Path Coefficient	t-Statistic	Sig. Level	Validation Result
H2	Awareness → PCtrl	-0.002	0.03	N/A	Not supported
H3	Awareness → PSE	0.332	4.69	0.001	Supported
H4	PSE→ PCtrl	0.222	2.04	0.05	Supported
H5	PU → PCtrl	0.433	4.89	0.001	Supported
H6	PCtrl → DI	0.308	4.32	0.001	Supported
H7	PCtrl → PP	0.714	18.88	0.001	Supported

PCtrl: privacy control; PSE: perceived self-efficacy; PU: perceived usefulness; DI: disclosure intention; PP: perceived privacy; GPC: general privacy control; PTS: propensity to share

All control variables are also entered into the SEM calculation and apart from propensity to share (path coefficient = 0.437, $p < 0.001$), all other control variables are not significantly influencing individuals' disclosure intention. Although OSN users' general privacy concern is not significantly associated with their disclosure intention, it is found that there is a significant negative association between individuals' general privacy concern and perceived privacy control (path coefficient = -0.267, $p < 0.001$). There has not been enough emphasis on how privacy concerns influence users' disclosure intention in OSN environments; even less attention has been paid to the functioning mechanism of privacy concern on available personalization tools such as privacy control options (Acquisti & Gross, 2006; Dwyer et al., 2007). This finding helps to understand the impact of individuals' privacy concern in OSN environments, further studies is suggested to explore the impact pattern of general privacy concern on individuals' perceived privacy control.

5.5.2 Regression analyses

Furthermore, hierarchical regression (HR) was used to explore the antecedents of privacy control. All latent variable scores used in the analysis are calculated in the previous step via SmartPLS.2.0. In HR, independent variables are entered cumulatively

according to the purpose of the study (Cohen, Cohen, West, & Aiken, 2013). Six general demographic variables were first introduced in the mode (Model 1) to test their initial impact on privacy control. Second, general privacy concern was entered as a new antecedent in addition to the first block of predictors and named as Model 2. Third, awareness, self-efficacy, and PU are added to Model 3. Table 5.9 showcases all the models and HR results (coefficients and corresponding significance). It is found that none of gender, age, education level, length of Facebook usage, the number of friends, or average usage time per day is an effective predictor of privacy control. While general privacy concern has a significant impact on privacy control (β=-0.255, p<0.001), its impact is less significant than the effect of perceived self-efficacy and PU of control options. Partialling out the effect of other variables, perceived self-efficacy, and PU jointly explained 32 percent of the variance in privacy control.

Table 5.9 Regression result

	Model 1		**Model 2**		**Model 3:**	
	Coefficient	**Sig.**	**Coefficient**	**Sig.**	**Coefficient**	**Sig.**
(Constant)	5.407***	.000	6.711***	.000	1.705*	.016
Gender	-.170	.345	-.091	.599	-.073	.608
Age	-.097	.262	-.108	.191	-.081	.246
Education	-.107	.245	-.073	.411	-.039	.592
Length of usage	.164	.390	.165	.368	.132	.381
Number of friends	.015	.760	-.025	.604	-.039	.327
Time per day	.065	.379	.065	.360	.034	.555
GPC			-.255***	.000	-.237***	.000
PSE					.311**	.002
PU					.555**	.000
Aware					-.023	.713
R^2	.031		.111		.426	
Adjusted R^2	.000		.078		.394	
ΔR^2	.031		.080		.315	

***p<0.001, **p<0.01, *p<0.05

5.6 Mediation test

The mediation role of privacy control and self-efficacy are also explored in this study. To assess whether the impacts of self-efficacy and PU on disclosure intention were fully or partially mediated by privacy control, the four-step approach suggested by Baron & Kenny (1986) were performed. First, the effects of independent variable on mediating variable were tested (Path a); second, the effects of mediating variable on dependent variable were tested (Path b); in the third step, the effects of independent variable on dependent variable were tested (Path c); finally the effects of both independent variable and mediating variable on dependent variable were tested simultaneously (Path d). Results show that the impact of self-efficacy on individuals' disclosure intention is fully mediated by privacy control, while the impact of PU is only partially mediated by privacy, as shown in Table 5.9. According to TAM, PU of control options should also has a significant impact on individuals' attitude towards those IT features and further influence individuals' usage intention, as well as their disclosure intention (Mathieson, 1991). Thus, this study offers new insight into the role of PU by showing that apart from affecting users' attitude of control options, PU also exerts its influence on people's behavioral intention via perceived privacy control.

Table 5.10 Mediation test of privacy control

PSE→ DI

		Path d (PSE, PCtrl -> DI)
Path a (PSE -> PCtrl)	0.461***	
Path b (PCtrl -> DI)	0.452***	0.442***
Path c (PSE -> DI)	0.226**	0.022

PU → DI

		Path d (PU, PCtrl -> DI)
Path a (PU -> PCtrl)	0.555***	
Path b (PCtrl -> DI)	0.452***	0.324***
Path c (PU -> DI)	0.410***	0.230**

***p<0.001, **p<0.01, *p<0.05

This study also found that the impact of awareness of control options on privacy control is fully mediated by perceived self-efficacy. This finding is also making sense for the following two reasons: 1) one can hardly claim oneself to be in a state of control if he has no confidence utilizing available control tools; 1) most of the control options provided by OSNs are quite intuitive and clear to use, making self-efficacy easy to achieve once new options are introduced. The impacts of self-efficacy and PU on OSN users' perceived privacy are partially mediated by privacy control, as shown in Appendix H.

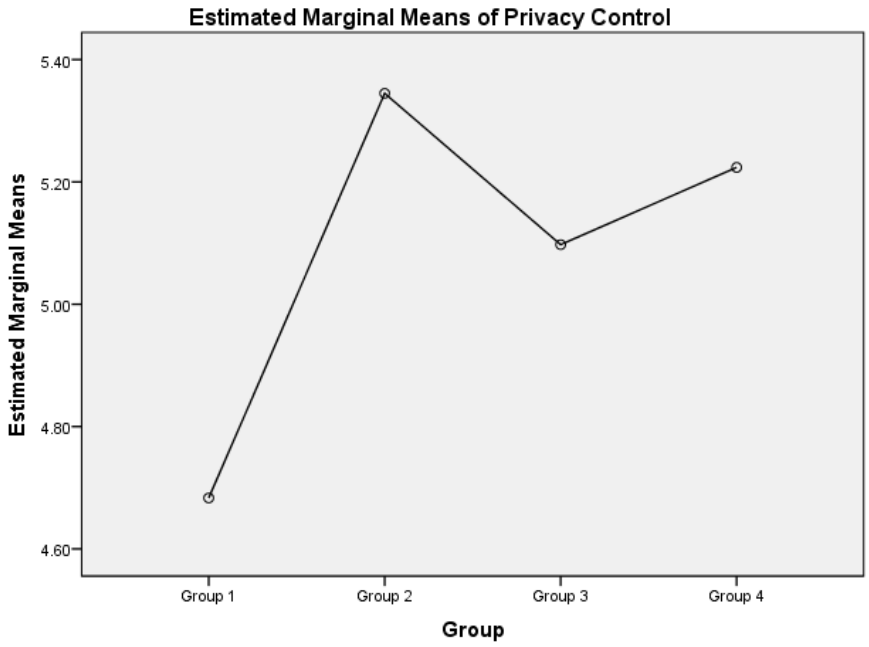
6. Supplementary Analysis

6.1 The effect discussion of tutorials and warning messages

It is already empirically shown in section 5.3 that function tutorials are effective in improving OSN users' awareness, perceived self-efficacy and PU of control options, and that warning messages are effective in increasing PU. Although both function tutorials and warning messages can independently increase OSN users' PU, it is found that their impacts on PU are not additive. In this section, the impact of tutorials and warning messages on OSN users' privacy control and disclosure intention are explored.

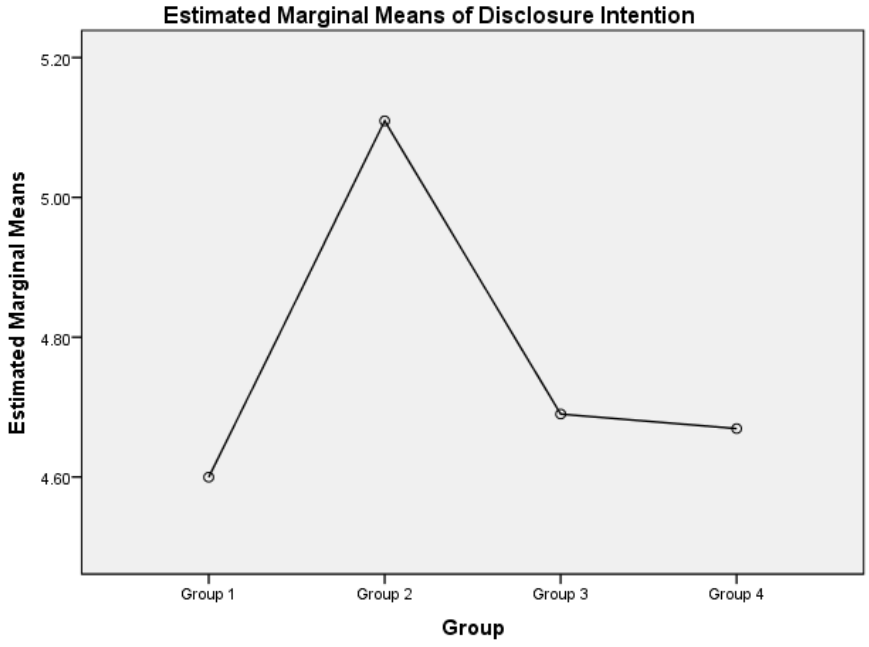
It is found that subjects in all treatment groups perceived higher privacy control than subjects in the control group (t = 3.17, p < 0.01) while there is no statistically significant difference among the three treatment groups, see figure 6.1. It is also found that when compared with the other three groups, subjects in group 2 (function tutorial group) show higher posting intention when using Facebook (t = 1.91, p = 0.06). When warning messages are presented, however, no statistically significant difference is found among group 1, 3 and 4 (F = 1.69, p = 0.19), as shown in Figure 6.2. The mean plot of privacy control is shown in Figure 6.1. Based on the privacy calculus perspective, it can be explained as the sense of risk triggered by warning messages has a mitigating effect on individuals' disclosure intention. When warning messages are presented (group 3 and group 4), OSN users' disclosure intention is not as high as the tutorial alone group (group 2). More details of the manipulation comparison can be found in Appendix I.

Figure 6.1 Privacy control among group 1, 2, 3, 4



Covariates appearing in the model are evaluated at the following values: GPC = 5.2778

Figure 6.2 Mean plot of disclosure intention

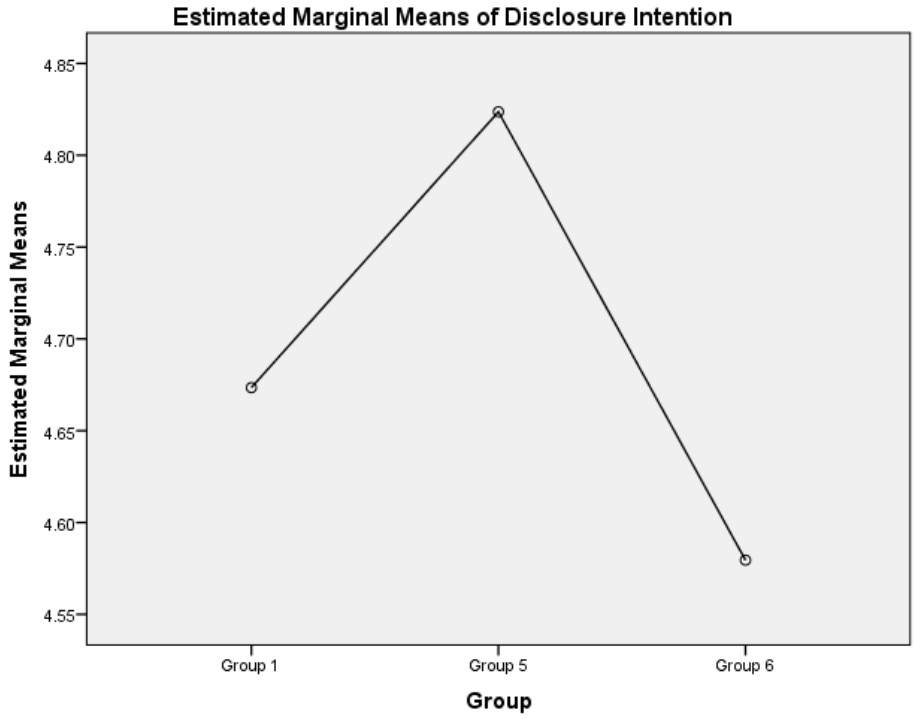


Covariates appearing in the model are evaluated at the following values: PTS = 5.1441

6.2 The impact of 'too much' awareness

The potential impact of too much awareness is explored through the comparison of group 1, 5, and 6, in which different amount of available control options on Facebook are introduced via checklists. It is found that although participants in group 6 have perceived significantly higher privacy control than group 1 ($p < 0.01$), the disclosure intention did not rise accordingly, as shown in Figure 6.3. Although the result of a one-way ANOVA shows that there was no statistically significant difference ($F = 0.42$, $p = 0.66$), the average disclosure intention of group 6 is lower than group 1 and group 5, in which participants do not possess as much awareness of control options. This is probably because the sudden acknowledgment of many control options will increase the amount of privacy risk perceived by OSN users and hence exerts a mitigating effect on individuals' disclosure intention.

Figure 6.3 Disclosure intention of group 1, 5 and 6



6.3 Privacy control and perceived privacy

In the broader research model, the positive association between privacy control and perceived privacy is already tested and supported. As a supplementary analysis, the relationship between privacy control and perceived privacy is further explored. In the literature review, it is identified that there are three available perspectives: the antecedent view, the dimension view, and the control is privacy view. Items measuring privacy control and perceived privacy are analyzed using the factor analysis technique. When free loading are allowed for the privacy control and perceived privacy measurement items, only one factor is extracted using maximum likelihood estimation, explaining 72.9 % of the variance. While two factors are extracted, 85% variance can be explained. When substituting perceived control with perceived privacy in the proposed research model, H2 was no longer supported. This finding is supportive of the antecedent view we took, which can both explain the high-level communality and the discriminative role of the two constructs. More details of this analysis are in Appendix J.

6.4 Open-ended questions

Participants' opinion regarding the amount of available control options are collected via an open-ended question and summarized in Table 6.1. It is found that the majority of Facebook users are satisfied with the amount of control options they are aware of.

Table 6.1 Opinion of control options on Facebook

Opinion	Frequency	Percent
Too much control options	33	11.1
Just the right amount	193	65.0
Not enough control options	34	11.4
Unspecified	37	12.5
Total	297	100.0

7. Conclusion and Future Directions

This study aims to offer some insight into the impact of awareness of control options on individuals' privacy related perceptions. It is found that the users' awareness of available control options is positively associated with individuals' privacy control, and its impact is fully mediated by perceived self-efficacy in the OSN environments. Both perceived self-efficacy and PU of control options are found to be effective predictors of individuals' perceived control over privacy, which has a further influence on their disclosure intention.

While it is shown in the study that Facebook users on average only have a medium level of awareness of available control options, the majority of users are satisfied with the amount of control options provided by Facebook. However, although individuals' perceived control over privacy will increase when be acknowledged with previously unknown control features, their disclosure intention will not rise accordingly in a linear manner. In fact, their disclosure intention demonstrated a decreased tendency when 'too much' awareness was attained via checklists of control options.

In terms of awareness-increasing techniques, it is found that the function tutorial is effective in improving OSN users' awareness, self-efficacy and PU of available control features. While warning messages alone are effective in improving individuals PU of control options, its impact on PU is no longer significant in the presence of function tutorials. Moreover, when presented with tutorials incorporating warning messages, individuals' disclosure intention is found to be lower than the tutorial alone group, suggesting a mitigating impact of warning messages on disclosure intention.

The findings of this study are of great practical value. First, it empirically shows that the effort to devise novel control options is a two-edged sword, in the sense that the

accumulated awareness will not only increase OSN users' perceived privacy control but increase their perceived risk and exerts a mitigating effect on disclosure intention. OSN providers should be cautious in introducing new control features and carefully examine the available options to make sure they are not exceeding the optimized amount. Second, control options in OSN environments should be easy to use and as intuitive as possible, in that individuals' self-efficacy of control options is positively associated with their perceived privacy control. Third, when introducing new control features, function tutorials are recommended instead of tutorials incorporating warning messages, which will not only increase OSN users' privacy control but mitigate their online disclosure intention as well.

Apart from the contribution, several limitations exist in this study which would worth further exploration. First, the control options selected as key manipulations in this study are under the tag of Timeline and Tagging Management on Facebook, which have already attained a medium level of awareness among users. It will be interesting to see whether our findings apply to other control options that are less knowledgeable to OSN users in future research. Second, a potential ceiling effect exists in this study in terms of latent variable measurement. Even in the control group, participants show a high level of latent variable scores on a 7 point Likert scale, e.g. average privacy control equals 4.6, average general privacy control equals 5.5. More valid and reliable measurement of the latent variables used in this study should be devised or modified based on extant research findings. Third, this study only examined the impact of 'too much' awareness of control options on a superficial level, more comprehensive and thorough exploration should be addressed to explore the impact of abundance of control options. Lastly, it is found the personalization-enabled privacy control only partially mediated the impact of

self-efficacy and PU on individuals' perceived privacy, the relationship between privacy control and privacy itself needs further research in the IS field.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies* (pp. 36–58). Springer.

Acquisti, A., & Gross, R. (2111). Imagined communities: Awareness, information sharing, and privacy on the facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies* (Vol. 4258, pp. 36–58).

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: a replication. *MIS Quarterly*, 227–247.

Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior*. Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*, *84*(5), 888.

Altman, I. (1976). Privacy: A Conceptual Analysis. *Environment and Behavior*, *8*(1), 7–29.

Averill, J. R. (1973). Personal control over aversive stimuli and its relationship to stress. *Psychological Bulletin*, *80*(4), 286.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13–28.

Bakker, C. B., & Bakker-Rabdau, M. K. (1973). *No trespassing!: Explorations in human territoriality*. Chandler & Sharp Pub.

Bandura, A. (1977). Self-Efficacy - Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 191–215.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Macmillan.

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies*, *2*(2), 285–309.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First*

Monday, *11*(9).

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1042.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3), 245–270.

Benassi, P. (1999). TRUSTe: an online privacy seal program. *Communications of the ACM*, *42*(2), 56–59.

Benbasat, I., & Wang, W. (2005). Trust in and adoption of online recommendation agents. Journal of the Association for Information Systems, 6(3), 4.

Berger, K., Klier, J., Klier, M., & Probst, F. (2014). A Review of Information Systems Research on Online Social Networks. Communications of the Association for Information Systems, 35(1), 8.

Brandtzaeg, P. B., Lueders, M., & Skjetne, J. H. (2010). Too Many Facebook “Friends”? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction*, *26*(11-12), 1006–1030.

Brecht, F., Fabian, B., Kunz, S., & Mueller, S. (2011). Are you willing to wait longer for internet privacy? In *ECIS*.

Brief, A. P., & Motowidlo, S. J. (1986). Prosocial organizational behaviors. *Academy of Management Review*, *11*(4), 710–725.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, *19*(1), 7–19.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *Professional Communication, IEEE Transactions on*, *52*(2), 167–182.

Cheng, F.-F., & Wu, C.-S. (2010). Debiasing the framing effect: The effect of warning and involvement. *Decision Support Systems*, *49*(3), 328–334.

Cheung, W., Li, E. Y., & Yee, L. W. (2003). Multimedia learning system and its effect on self-efficacy in database modeling and design: an exploratory study. *Computers & Education*, *41*(3), 249–270.

Cheung, C. M., Chiu, P.-Y., & Lee, M. K. (2011). Online social networks: why do students use Facebook? Computers in Human Behavior, 27(4), 1337–1343.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295–336.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyberpsychology & Behavior*, *12*(3), 341–345.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences*. Routledge.

Constant, D., Kiesler, S., & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research*, *5*(4), 400–421.

Cozby, P. C. (1973). Self-disclosure: a literature review. *Psychological Bulletin*, *79*(2), 73.

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *Mis Quarterly*, 341–363.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*(2), 10–19.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing*, *19*(1), 20–26.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

De Hoog, N., Stroebe, W., & de Wit, J. B. (2005). The impact of fear appeals on processing and acceptance of action recommendations. *Personality and Social Psychology Bulletin*, *31*(1), 24–33.

DeStefano, D., & LeFevre, J.-A. (2007). Cognitive load in hypertext reading: A review. *Computers in Human Behavior*, *23*(3), 1616–1641.

Dewald, N. H. (1999). Transporting good library instruction practices into the web

environment: an analysis of online tutorials. *The Journal of Academic Librarianship*, *25*(1), 26–31.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422.

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

Dinev, T., & Hart, P. (2006b). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7–29.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316.

Donovan, J. (2015). How to set Facebook privacy settings. Retrieved June 7, 2015, from http://www.digitaltrends.com/social-media/how-to-set-facebook-privacy-settings/

Drabek, T. E. (1999). Understanding disaster warning responses. *The Social Science Journal*, *36*(3), 515–523.

Durndell, A., & Haag, Z. (2002). Computer self efficacy, computer anxiety, attitudes towards the Internet and reported experience with the Internet, by gender, in an East European sample. *Computers in Human Behavior*, *18*(5), 521–535.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 Proceedings*, 339.

Eastin, M. S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of Computer-Mediated Communication*, *6*(1), 0–0.

Ellison, N. B., & others. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends:” Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168.

Facebook 101 Tutorial. (2015). Retrieved June 23, 2015, from http://www.gcflearnfree.org/facebook101

Facebook Video Courses and Tutorials from. (2015). Retrieved June 23, 2015, from /Facebook-training-tutorials/197-0.html

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39–50.

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, 106–119.

Gangadharbatla, H. (2008). Facebook me: Collective self-esteem, need to belong, and internet self-efficacy as predictors of the iGeneration's attitudes toward social networking sites. *Journal of Interactive Advertising*, *8*(2), 5–15.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 5.

Giannotti, F., Pedreschi, D., Pentland, A., Lukowicz, P., Kossmann, D., Crowley, J., & Helbing, D. (2012). A planetary nervous system for social mining and collective awareness. *European Physical Journal-Special Topics*, *214*(1), 49.

Gilliland, S. W. (1993). The perceived fairness of selection systems: An organizational justice perspective. *Academy of Management Review*, *18*(4), 694–734.

Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity*. Englewood Cliffs, NJ: Prentice-Hall.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 149–166.

Gross, H. (1971). Privacy and autonomy. *Nomos XIII: Privacy*, *169*, 81.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71–80). ACM.

Hartzel, K. (2003). How self-efficacy and gender issues affect software adoption and use. *Communications of the ACM*, *46*(9), 167–171.

Haythornthwaite, C. (2005). Social networks and Internet connectivity effects. *Information, Community & Society*, *8*(2), 125–147.

Hess, T. J., McNab, A. L., & Basoglu, K. A. (2014). Reliability generalization of perceived ease of use, perceived usefulness, and behavioral intentions. *Mis Quarterly*, *38*(1), 1–28.

Hichang, C. (2010). Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self-Protection Strategies. *Journal of Information Privacy and Security*, *6*(1), 3–

27.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80–85.

Hsu, M.-H., Ju, T. L., Yen, C.-H., & Chang, C.-M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies*, *65*(2), 153–169.

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: an exploratory study of determinants. *The Journal of Strategic Information Systems*, *9*(2), 129–154.

Johnson, C. A. (1974). PRIVACY AS PERSONAL CONTROL (1). In *EDRA; Proceedings of the Annual Environmental Design Research Association Conference* (p. 83).

Joinson, A. N. (2008). Looking at, looking up or keeping up with people?: motives and use of facebook. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 1027–1036). ACM.

Jonassen, D. H., & Hernandez-Serrano, J. (2002). Case-based reasoning and instructional design: Using stories to support problem solving. *Educational Technology Research and Development*, *50*(2), 65–77.

Jung, E. J., Lankton, N., McKnight, H., & Jung, E. (2012). Three Processes that Form Online Social Networking Post-Adoptive Use Intention.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Thinking Styles and Privacy Decisions: Need for Cognition, Faith into Intuition, and the Privacy Calculus.

Kolodner, J. (2014). *Case-based reasoning*. Morgan Kaufmann.

Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788–8790.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, *46*(1), 254–264.

Kwon, O., & Wen, Y. (2010). An empirical study of the factors affecting social network service use. *Computers in Human Behavior*, *26*(2), 254–263.

Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology*, *32*(2), 311.

Laufer, R. S., Proshansky, H. M., & Wolfe, M. (1973). Some analytic dimensions of privacy. In *Third International Architectural Psychology Conference, Lund, Sweden*.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, *14*(1), 79.

Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, *10*(6), 702–715.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62.

Lim, K. H., & Benbasat, I. (2000). The effect of multimedia on perceived equivocality and perceived usefulness of information systems. *MIS Quarterly*, 449–471.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289–304.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393–411.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Magat, W. A., Viscusi, W. K., & Huber, J. (1988). Consumer processing of hazard warning information. *Journal of Risk and Uncertainty*, *1*(2), 201–232.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): Tthe construct, the scale, and a causal model. *Information*

Systems Research, *15*(4), 336–355.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5–21.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, *2*(3), 173–191.

Milne, G. R. (1997). Consumer participation in mailing lists: A field experiment. *Journal of Public Policy & Marketing*, 298–309.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 206–215.

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing*, *19*(2), 238–249.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, *19*(1), 54–61.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375.

Nadkarni, A., & Hofmann, S. G. (2012). Why do people use Facebook? *Personality and Individual Differences*, *52*(3), 243–249.

Ng, K. C. (2007). Replacing face-to-face tutorials by synchronous online technologies: Challenges and pedagogical implications. *The International Review of Research in Open and Distributed Learning*, *8*(1).

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when “privacy” matters. *Journal of Direct Marketing*, *9*(3), 46–60.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262.

Oud, J. (2009). Guidelines for effective online instruction using multimedia screencasts. *Reference Services Review*, *37*(2), 164–177.

Parker, R. B. (1973). Definition of privacy, a. *Rutgers L. Rev.*, *27*, 275.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41.

Plous, S. (1993). *The psychology of judgment and decision making.* Mcgraw-Hill Book Company.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544.

Polyviou, P. G. (1982). *Search & seizure: constitutional and common law*. Duckbacks.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. B. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, *7*(1), 24–47.

Privacy Help Center. (2015). Retrieved June 22, 2015, from https://www.facebook.com/help/437430672945092/

Raab, C. D. (1998). The distribution of privacy risks: Who needs protection? *The Information Society*, *14*(4), 263–274.

Rapoport, A. (1972). *Some perspectives on human use and organization of space*. A. Rapoport.

Reidenberg, J. R. (1994). Setting standards for fair information practice in the US private sector. *Iowa L. Rev.*, *80*, 497.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS (Release 2.0 M3) http://www. smartpls. de. University of Hamburg. *Hamburg: Germany*.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114.

Rosen, P., & Sherman, P. (2006). Hedonic information systems: acceptance of social networking websites. *AMCIS 2006 Proceedings*, 162.

Ruiter, R. A., Abraham, C., & Kok, G. (2001). Scary warnings and rational precautions: A review of the psychology of fear appeals. *Psychology and Health*, *16*(6), 613–630.

Schoeman, F. (1984). Privacy: philosophical dimensions. *American Philosophical Quarterly*, 199–213.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2005). Privacy, fair information practices and the fortune 500: the virtual reality of compliance. *ACM SIGMIS Database*, *36*(1), 49–63.

Segars, A. H., & Grover, V. (1993). Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Quarterly*, 517–525.

Shih, D.-H., Hsu, S.-F., Yen, D. C., & Lin, C.-C. (2012). Exploring the Individual's Behavior on Self-Disclosure Online. *International Journal of Human-Computer Interaction*, *28*(10), 627–645.

Silver, S. L., & Nickel, L. T. (2005). Are online tutorials effective? A comparison of online and classroom library instruction methods. *Research Strategies*, *20*(4), 389–396.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 980–A27.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196.

Social networks: global sites ranked by users 2015 | Statistic. (2015). Retrieved June 22, 2015, from http://www.statista.com/statistics/

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *Mis Quarterly*, 503–529.

Sovern, J. (1999). Opting in, opting out, or no options at all: The fight for control of personal information. *Wash. L. Rev.*, *74*, 1033.

Stewart, D. W., & Martin, I. M. (1994). Intended and unintended consequences of warning messages: A review and synthesis of empirical research. *Journal of Public Policy & Marketing*, 1–19.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, *68*(3), 459.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, *8*(3), 349–411.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *Mis Quarterly*, *37*(4), 1141–1164.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society*, *31*(1), 6–11.

Torkzadeh, G., & Koufteros, X. (1994). Factorial validity of a computer self-efficacy scale and the impact of computer training. *Educational and Psychological*

Measurement, *54*(3), 813–821.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254–268.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36.

Turn, R. (1985). Privacy protection. *Annual Review of Information Science and Technology*, *20*, 27–50.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458.

Van der Heijden, H. (2004). User acceptance of hedonic information systems. *MIS Quarterly*, 695–704.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204.

Viswanath, B., Mislove, A., Cha, M., & Gummadi, K. P. (2009). On the evolution of user interaction in facebook. In *Proceedings of the 2nd ACM workshop on Online social networks* (pp. 37–42). ACM.

Wallston, K. A. (2001). Conceptualization and operationalization of perceived control. *Handbook of Health Psychology*, 49–58.

Wang, N., Xu, H., & Grossklags, J. (2011). Third-party apps on Facebook: privacy and the illusion of control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology* (p. 4). ACM.

Wang, Y., Leon, P. G., Chen, X., & Komanduri, S. (2013). From Facebook Regrets to Facebook Privacy Nudges. *Ohio St. LJ*, *74*, 1307.

Wellman, B. (2001). Computer networks as social networks. *Science*, *293*(5537), 2031–2034.

Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.

Wu, J., & Lu, X. (2013). Effects of extrinsic and intrinsic motivators on using utilitarian, hedonic, and dual-purposed information systems: A meta-analysis. *Journal of the Association for Information Systems*, *14*(3), 153–191.

Xiao, B. (2010). Product-Related Deceptive Information Practices in B2c E-Commerce: Formation, Outcomes, and Detection, *UBC*.

Xiao, B. & Benbasat, I. Forthcoming. Designing warning messages for detecting biased online product recommendations: an empirical investigation. *Information System Research*.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: toward an integrative view. *ICIS 2008 Proceedings*, 6.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). Research Note-Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research*, *23*(4), 1342–1363.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722.

Yeung, C. A., Liccardi, I., Lu, K., Seneviratne, O., & Berners-Lee, T. (2009). Decentralization: The future of online social networking. In *W3C Workshop on the Future of Social Networking Position Papers* (Vol. 2, pp. 2–7).

Yun, H., LEE, G., & Kim, D. (2014). A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators. *ICIS 2014 Proceedings*.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure Intention of Location-Related Information in Location-Based Social Network Services. *International Journal of Electronic Commerce*, *16*(4), 53–89.

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behavior*, *23*(5), 605–633.

Appendices

Appendix Index

Appendix A: Literature Review on Awareness of Privacy Practices

Organizational data handling behaviors that harbor potential negative consequences, although still pervasively existent, have met accordant censure from both the academia and practice (Schwaig et al., 2005; Posey et al., 2011). It is found that internet users always feel shocked to realize that their personal data could be collected without individuals' awareness (Sovern, 1999; Bélanger & Crossler, 2011), and their threat perceptions can easily lead to individuals' privacy-protective reactions (Lewis et al., 2008). For fear of the negative consequences incurred by privacy outcries, FIP has long been recognized as a default contract assumed from the consumer perspective when transact with online companies (Reidenberg, 1994; Culnan & Armstrong, 1999). This contract is considered breached if 1) data is collected without consumers' awareness; 2) submitted data is rented to a third party; or 3) consumers are not provided with opt-out options (Milne & Rohm, 2000; Phelps et al., 2000). Two levels of privacy practices that aim to safeguard individuals' online privacy are summarized as following:

1. Privacy practice conducted at the organizational level

Individuals' awareness over privacy is most commonly analyzed as the extent to which a user is informed about privacy practices and policies, more specifically, through the impact of FIP (Culnan, 1995; Milne & Rohm, 2000; Phelps et al., 2000; Xu et al., 2008). There is basic agreement among scholars that online users should not only be acknowledged of what personal information has been collected by a certain entity, but also be aware of the possibility that their submitted information may be shared with third parties (Phelps et al., 2000).

Consumers' awareness on information collection at the organizational level is widely taken

as the basis of defining consumer privacy (Goodwin, 1991; Foxman & Kilcoyne, 1993; Nowak & Phelps, 1995; Milne & Rohm, 2000). It is also proposed that an individual will tend to exercise process control and influence changes in organizational policies if they are found to be objectionable (Gilliland, 1993). As such, there is strong incentive for companies to 1) publicize their privacy practices (e.g. data gathering procedures), and 2) promote the awareness of industry self-regulation (e.g. privacy seals) among consumers (Culnan, 1995; Xu et al., 2011). Moreover, it is discovered that consumers' awareness and FIP at the organizational level exert influence on each other in a reciprocal manner: consumer awareness over data collection can prompt companies engage in self-regulation process, while awareness-increasing practices such as explicit notice will increase consumers' knowledge over privacy protection mechanisms and further increase individuals' perceived control (Benassi, 1999; Culnan, 1995, 2000).

2. Privacy practice conducted at the legislation level

In the year 1974, the privacy act was passed in the US stating that government officials may not maintain secret files or gather information about people irrelevant to a lawful purpose, which serves as a precedent of legislation on civil privacy protection. In the early 1990s, Foxman and Kilcoyne (1993) claimed that cooperation choose to actively abide ethical behavior in order to avoid restrictive legislation. It is also found that individuals' awareness of Internet privacy legislation is effective in mitigating their privacy concerns (Zhao et al., 2012). Despite the importance of legislation, privacy policies and adherence to them vary across industries, and new regulation from legislation is necessary in many fields due to poor self-regulatory regime for consumer privacy online (Miyazaki & Fernandez, 2000).

Public policy and self-regulatory efforts should be fast incorporated into the practice of

policymakers to alleviate different dimensions of consumer privacy concerns (Phelps et al., 2000). It is found that individuals with high social-consciousness are more likely to be aware of privacy policies and follow privacy issue developments, which in turn will exert influence on their privacy concern (Smith et al., 2011). One thing also worth mentioning is that social awareness, defined as the passive involvement and raised interest in social issues such as privacy disclosure policy, possess a positive influence on privacy concerns (Liao et al., 2011).

When it comes to the suitability and effect comparison between self-regulation and legislation effort, the boundary is always blurred. However, the government authorities and business leaders have realized the importance of this issue and exert joint cooperation to assess the appropriateness of industry self-regulation or legislation in regard to various consumer privacy protection issues, which resulted in some fruitful outcomes such as the establishment of Federal Trade Commission (FTC) (Culnan, 2000).

Appendix B: Summary of Privacy Control and Privacy

1. The antecedent view

One school of control definition in regards to privacy has taken an antecedent view, claiming privacy control is a factor influencing individual's privacy perception, which is in accordance with the summarization of extant literature (Yun et al., 2014). Among the six identified predictors of privacy invasion perception, individual control over the collection and dissemination of personal information exerts the strongest influence in a firm-based empirical study (Zweig & Webster, 2002). As an abstract construct, the sense of control might be a little bit hard to capture, but its impact can be verified through the occurrence of 'loss of control' (Goodwin, 1991; Culnan, 1993; Caudill & Murphy, 2000), which resembles the principle of hypothesis testing. Following this technique, Culnan (1995) states that individuals with positive control over personal information are less concerned about privacy, and the 'loss of control', executed via the opt-in and opt-out options, has a significant impact on individuals' attitude toward secondary information usage. Taking the opportunity of the unprecedented News Feed features launched by Facebook, Hoadley et al. (2010) empirically showed that the 'illusory' loss of control can significantly rise individuals' privacy concern, even if the same amount of information has been accessible to the same group of audience before and after.

It is worth mentioning that the main stream under this antecedent view is converged from the E-commerce domain (Milne & Gordon, 1993; Culnan, 1995; Milne, 1997; Phelps et al., 2000; Hoadley et al., 2010). Phelps et al. (2000) showed that consumers, regardless of their innate level of sensitivity over personal information usage by marketers, perceive higher privacy concern when more concrete control on personal information dissemination was granted. Similarly, the perceived vulnerability and perceived ability to control

information are claimed to influence internet users' privacy concern over personal information (Dinev & Hart, 2004). In a qualitative manner, Zweig and Webster (2002) demonstrated that the capability to control one's image availability directly influences an individual's privacy invasion perception in electronic performance monitoring systems.

There is a blurred line between antecedent view and later discussed dimension view. Started from the dimension view, Laufer et al. (1973) at first claimed that the perceived control, representing the freedom over interaction with others and the manipulation over stimulation from and to others, is one dimension of a second order privacy construct. This understanding was soon modified and re-structured. Based on a three dimensional definition of privacy (self-ego, environmental, and interpersonal), Laufer et al. (1977) later claimed that the ability to control information disclosure serves as a key factor shaping individuals' privacy protection and privacy invasion perception. Moreover, studies at early stages tend to adopt a formative way of privacy measurement, e.g. Culnan (1993) measured privacy through items covering three major components: general privacy concern, loss of control and individuals' sensed protection for unauthorized usage of submitted information.

Among the empirical papers identified, not all proposed correlations between control and privacy are well supported. In the study conducted by Dinev and Hart (2004), the coefficient between individuals' ability to control and privacy concern was not statistically significant, although the measurement items deserve more consideration. For a summary of all the identified papers taken an antecedent view of the control-privacy association, please see tables at the end of this appendix.

2. The 'control is privacy per se' view

One other group of definitions has defined control as privacy per se (H. Gross, 1971; Parker, 1973; Polyviou, 1982). Given the fact that any adequate conceptualization of privacy must involve personal control as a core construct (Johnson, 1974), it is not surprising to see that information privacy is most often defined as the ability to control information at an individual level, particularly by scholars from the social sciences and information systems (IS) (Bélanger & Crossler, 2011; Dinev, Xu, Smith, & Hart, 2013). In the very early stage of privacy measurement exploration, the perception of privacy has already been measured as individuals' control over submitted personal information (Culnan, 1993).

Privacy itself is an interpersonal boundary control process in sustaining a 'personal space', which is subjected to the influence of a sense of territoriality and many other behavioral mechanisms (Westin, 1968; Bakker & Bakker-Rabdau, 1973; Altman, 1976; Margulis, 1977; Stone et al., 1983; Clarke, 1999). Similar ways defining privacy can also be identified with great resemblance to this control view of privacy: Turn (1985), for example, proposes that privacy refers to the rights of individuals with respect to the collection, storage, processing, dissemination, and use of personal information about them.

Not all scholars taking this 'privacy is control' perspective define control as a state that can be achieved with a singular process. According to Johnson (1974), control is achieved through two complementary phases: the state of primary control is attained through behaviors with direct outcomes, while secondary control is achieved via configuration behaviors which set conditions for certain outcomes. Similarly, Schoeman (1984) differentiate control over information about oneself from individuals' applied mechanisms exercising that control. Derived from consumer right theories, Goodwin (1991) defines privacy based on two control dimensions: control of information disclosure and control over

unwanted intrusions into the environment. This delineation of two types of control is later adopted by Hoffman et al. (1999), who claimed that consumers crave for control over personal information – a notion consistent with the healthy development of the online marketplace.

According to scholars exploring business field, control related studies have been focused on individuals' ability to decide the dissemination and re-usage of information that they provided during commercial transactions (Margulis, 1977; Stone et al., 1983; Goodwin, 1991; Hoffman et al., 1999; Belanger et al., 2002; Dinev & Hart, 2004). E.g. Belanger et al. (2002) examined the extent to which consumers are willing to provide personal information to merchants and demonstrated that the perceived control is nonexistent or in a diminishing manner when it comes to further usage of that information with third parties. A summary of papers taken this control as privacy view can be found in the tables at the end of this appendix.

3. The dimension view

In addition to the two types of control-privacy relationship discussed, some IS scholars proposed a third way of interpreting privacy control, which established itself as a new favorite in the realm of privacy study. Although from the very early stage of privacy craze, scholars have defined the ability to control personal information and interactions as one dimension of privacy (Rapoport, 1972; Altman, 1976; Stone et al., 1983), the concept of control was not well fabricated into the dimension view of privacy. Based on an extensive literature review, previous studies exploring the dimensionalities of information privacy concern have been summarized into four primary sub-scales: data collection, unauthorized secondary usage, improper access and errors (Smith et al., 1996).

In the new century researchers start to treat control as a crucial dimension of privacy, which now becomes a second order construct (Malhotra et al., 2004). In line with previous studies on information secondary usage (e.g. Culnan, 1995), scholars have conceptualized control as a key dimension constituting consumer privacy (Culnan, 1995; Caudill & Murphy, 2000; Milne & Rohm, 2000). Began with a summary of privacy defining scales, Malhotra et al. (2004) proposed a second-order IUIPC factor to represent internet users' information privacy concern, in which control is incorporated as one of the three first-order constituting dimensions.

Under this dimension view, one of the most frequently co-existent factors parallel control as a dimension of privacy is internet users' knowledge of secondary data usage (Caudill & Murphy, 2000; Milne & Rohm, 2000; Malhotra et al., 2004). It is claimed that combined with consumers' awareness of the information practice conducted by online companies, individuals' perceived control over the reuse of submitted data significantly influence the degree of privacy consumers perceive (Caudill & Murphy, 2000). According to Phelps et al. (2000), control not only serves as a key dimension defining privacy, but also is a influential predictor of firms' information practices. A summary of papers taken this dimension view can be found in the tables at the end of the appendix.

Summary of the Privacy Control Literature (Antecedent View)

Authors	Definition of Control / Control-oriented Construct	Definition of Privacy / Privacy Related Construct (Influenced by Control)	Other Identified Antecedents of Privacy
(Laufer & Wolfe, 1977)	Control refers to the ability to choose how, under what circumstances, and to what degree the individual is to disclose information	Privacy is a three-dimensional construct including self-ego, environmental, and interpersonal.	Privacy-related experiences; dynamic of time
(Phelps et al., 2000)	Information control stands for control over who has access to personal data (i.e., disclosure), how personal data are used (i.e., appropriation and false light), and what volume of advertising and marketing offers arises from the use of personal data (i.e., intrusion)	Consumer privacy concern: individuals' overall concern over the ways companies use personal information	The type of personal information requested; the potential consequences and benefits offered in exchange; consumer characteristics
(Zweig & Webster, 2002)	Individual control over the collection and dissemination of personal information represents a critical construct in defining perceptions of privacy (Stone & Stone, 1990)	Privacy is defined as the extent to which people can control the release and dissemination of personal information (Stone & Stone, 1990)	Image clarity; frequency of image updating; knowledge of others' access to awareness information
(Dinev & Hart, 2004)*	Individual control refers to the technology and procedures a website provides for consumers to control their disclosed personal information	Privacy represents the control of Transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability (Margulis, 1977)	Vulnerability: perceived potential risk when personal information is revealed (Raab, 1998)
(Hoadley et al., 2010)	Control is conceptualized as a psychological perception (instead of actual control)	Privacy concern over individuals' perceived control of their submitted information and the ease of information access by others was used as the dependent variable	Ease of information access
Culnan (1995) & 1993	Control over information reuse: the perceived degree of control loss through the fact of unwanted mail and telephone solicitations based on disclosed information	Privacy invasion: the occurrence of secondary information usage against the stated purpose when collecting, without the knowledge or consent of the individual	Knowledge on information usage (Whether consumer is aware of collection and informed about the reuse of personal information)

*The link between control and privacy was not supported

Summary of the Role of Privacy Control (Privacy is Control per se View)

Authors	Definition of Privacy	Definition of Control
Altman (1976)	Privacy is conceptualized as selective control of access to the self or to one's group, as well as interpersonal control.	Control is conceptualized as an active and dynamic regulatory process.
(Stone et al., 1983)	Information privacy, defined as the ability of the individual to control personal information usage by other parties	Control stands for individuals' capacity of handling personal information vis-a-vis other individuals, groups, organizations, etc.
(Culnan, 1993)	Privacy is defined as the ability of an individual to control the access others have to submitted information (Schoeman, 1984) (Westin, 1968).	Control refers to the ability of individuals to decide how their information is reused. Loss of control is operationalized as a dimension of privacy concerns.
(Goodwin, 1991)	Consumer privacy is defined in terms of control over information disclosure and the environment in which a consumer transaction occurs	Information control includes dissemination control and environmental control. Dissemination control refers to the ability to influence how marketers use personal information. Environmental control involves influencing the types and volume of solicitations that result from marketers' use of personal data.
(Belanger et al., 2002)	Privacy is defined as the ability to manage information about oneself.	Control over secondary use of information relates to the consumer's concern that once the information is freely submitted to a Website
(Hoffman et al., 1999)	Privacy concern spans the dimensions of environmental control and secondary use of information control	Environmental control represents the consumer's ability to control the actions of a Web vendor; Control over secondary use of information reflects consumers' perceived ability to control the use of their personal information for other purposes subsequent to the transaction during which the information is collected
(Clarke, 1999)	Information privacy refers to the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves	Control includes the individuals' ability to exercise a substantial degree of control over submitted data and its usage when data is possessed by another party
(Johnson, 1974)	Privacy is defined as behaviors which enhance and maintain one's control over outcomes indirectly by controlling interactions with others	Personal control was conceptualized as a four-stage process beginning with outcome choice and behavior selection control, and ending with outcome effectance and outcome realization control.
(Bélanger & Crossler, 2011)	Information privacy refers to the desire of individuals to control or at least significantly influence the data usage about themselves (Clarke, 1999)	Control represents an individual's capability to exercise a substantial degree of influence over that data and its use

Summary of the Role of Privacy Control (Dimension View)

Authors	Definition of Control / Control-oriented Construct	Definition of Privacy / Privacy Related Construct (Influenced by Control)	Other identified dimensions of Privacy
(Malhotra et al., 2004)	Control refers to individuals' ability to decide how their information is collected, used, and shared.	Privacy is defined as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.	Data collection; Awareness of privacy practice
(Milne & Rohm, 2000)	Control refers to the ability to remove names from marketing list (i.e., through opt-out mechanism).	Privacy is defined as a state, on the basis of who controls consumer data and whether consumers are informed of information collection and privacy rights.	Consumers' awareness of information collection
(Caudill & Murphy, 2000)	Control refers to the ability to decide the amount and depth of information collected (i.e., through opt-in and opt-out options).	Privacy is defined as consumers' control of their information in a marketing interaction and the degree of their knowledge of the collection and use of their personal information.	Whether consumer is knowledgeable about data collection
(Phelps et al., 2000)	Control refers to the ability to influence how personal information is used and who will have access to it	Privacy refers to the ability to affect the dissemination and use of personal information and control over unwanted use	Type of personal information requested; potential consequences and benefits; consumer characteristics

Appendix C: Survey Procedure for Each Treatment Group

- Group 1: measure self-efficacy and PU of timeline and tagging management options on Facebook → measure individuals' perceived privacy control → measure disclosure intention and perceived privacy → awareness checklist of timeline and tagging management options & awareness checklist of other privacy control options on Facebook → open-ended questions (feeling about available options, what else control options are expected, etc.)

- Group 2: plain function tutorial → measure self-efficacy and PU of timeline and tagging management options on Facebook → measure individuals' perceived privacy control → measure disclosure intention and perceived privacy → awareness checklist of timeline and tagging management options → open-ended questions.

- Group 3: warning messages → measure self-efficacy and PU of timeline and tagging management options on Facebook → measure individuals' perceived privacy control → measure disclosure intention and perceived privacy → awareness checklist of timeline and tagging management options → open-ended questions.

- Group 4: function tutorial incorporating warning messages→ measure self-efficacy and PU of timeline and tagging management options on Facebook → measure individuals' perceived privacy control → measure disclosure intention and perceived privacy → awareness checklist of timeline and tagging management options → open-ended questions.

- Group 5: awareness checklist of timeline and tagging management options→ measure self-efficacy and PU of timeline and tagging management options on Facebook → measure individuals' perceived privacy control → measure disclosure intention and perceived privacy → open-ended questions.

- Group 6: awareness checklist of timeline and tagging management options & awareness checklist of other privacy control options on Facebook → measure self-efficacy and PU of timeline and tagging management options on Facebook → measure individuals' perceived privacy control → measure disclosure intention and perceived privacy → open-ended questions.

It took approximately 15 minutes for each subject to complete the study. Each participant was thanked for their participation and rewarded with 2 dollars, which was consistent with the minimum payment standard ($7.25/hour) in America ("Minimum wage in the United States," 2015).

Appendix D: Survey Development Record

1. Development of checklists

Subjects' awareness of privacy control options is measured by two checklists listing available privacy control features on Facebook. Current privacy-oriented control options on Facebook can be classified into six categories, as shown in the following table. According to Nadkarni and Hofmann (2012), Facebook users engage in social networking activities to fulfill two primary needs: the need to belong and the need for self-presentation. In line with this statement, it has been identified that nearly 90 percent of Facebook users use it as a way to browse through their friends' updates, and more than half of the users have use Facebook as the medium of self-disclosure (the reciprocal trust paper). In order to select a manipulation (in this case, control options) that most likely to influence OSN users' interaction and self-disclosure activities, a preliminary interview was conducted among 8 Facebook users. According to the interviewees' feedback, timeline browsing and photo tagging activities have been identified as one of the common purposes of using Facebook, yet control options for Timeline and Tagging management have shown only medium level of awareness. On average, 5 out of 9 control options are claimed as known.

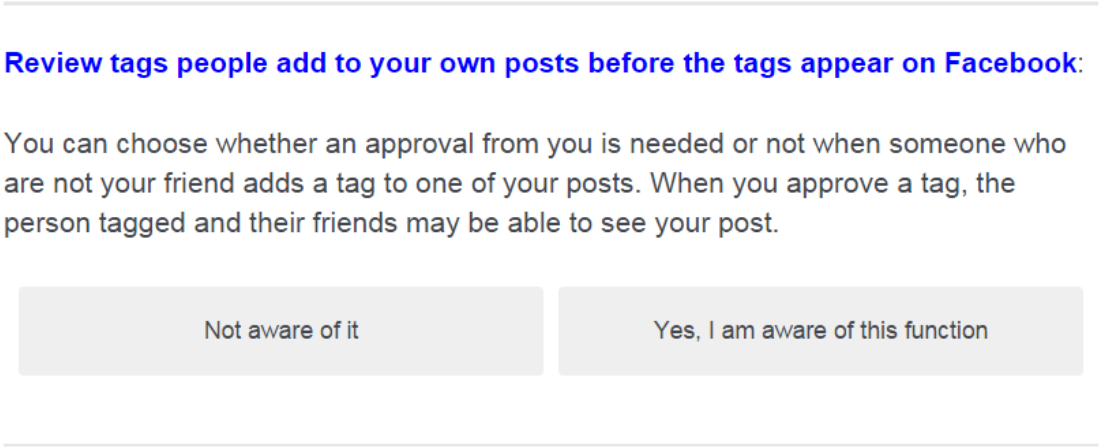
Summary of privacy control options

Category	No. of available options	Option examples
General Privacy Management	8	Control who can see my profile, Control who can look me up, etc.
Account Security Management	9	Login alerts, Login approvals, Trusted contacts, etc.
Timeline & Tagging Management	9	Who can add things to my Timeline, Review tags before they appear on Timeline, etc.
Apps & Ads Management	7	Always play anonymously, Pair ads with friends, etc.
Blocking Management	6	Block users, Block event invites, etc.
Other	10+	Management notifications, Mobile settings, Payment management, etc.

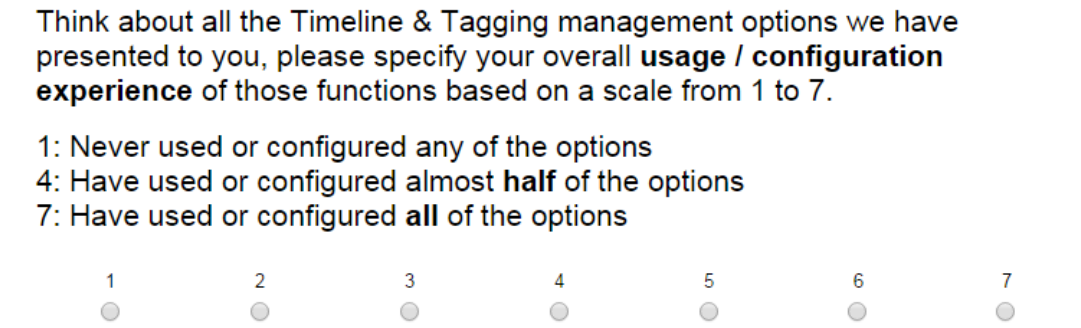
Options summarized as of July, 2015

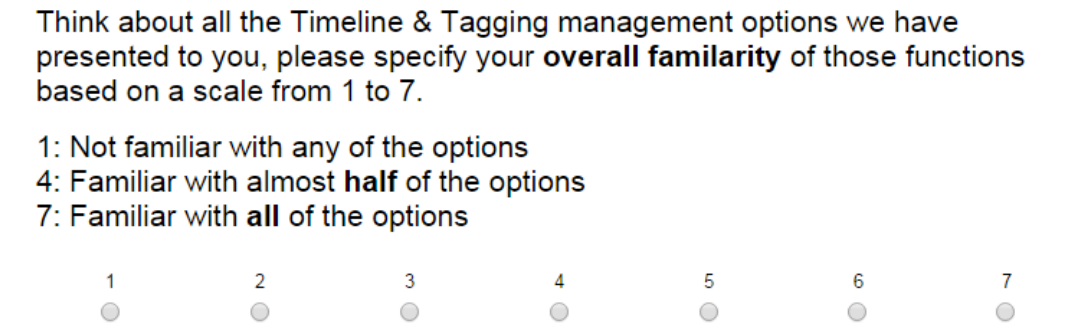
For the reason above, eight options under Timeline and Tagging Management are chosen as the key manipulation features for this study, one was not selected because the mobile version of Facebook doesn't provide this option. These eight options are organized and introduced in Checklist 1, and an example of the option description is shown in Figure 4.2. In order to test the potential impact of too much awareness, 16 other options on Facebook covering different aspects of privacy control (account security, general privacy, Apps and Ads management) are selected. The name and function description of these options are summarized in Checklist 2. In addition, the general familiarity and usage/configuration frequency of options presented in one or both checklists are measured respectively, Examples can be found in the following figures.

Example item from checklist 1



Items for familiarity and usage frequency





2. Development of measurement items

All the privacy control options we discussed in the survey are currently available functions

on Facebook, while the majority of the measurements of key constructs included in the survey are adopted from extant literature. For those constructs that we could not find proper measurement in the literature, we create new items based on the definition of the constructs (e.g. aware or not of a control option, familiarity with a function) for this study. Number of items used to measure each construct and their corresponding origins are shown in the following table. A pilot survey issued to 20 subjects shows good reliability for all the measurement items, and good discriminant validity among different constructs. Detailed content of each measurement item can be found in Appendix E.

Origin of measurement items

Construct	No. of Items	Description
General Privacy Concern[1]	4	3 items adopted from (Dinev & Hart, 2006b), 1 item adopted from (Li, 2014).
Propensity to Share[1]	4	Newly developed for the OSN context.
Awareness	3	1 item is an objective measurement of awareness of control options based on subjects' answer for checklist 1. The other 2 items are newly developed for the OSN context.
Self-efficacy	3	Adopted from (Torkzadeh & Koufteros, 1994; Durndell & Haag, 2002) and adjusted for the OSN context.
PU	4	Adopted from (Davis et al., 1989) and adjusted for the OSN context.
Privacy Control	3	Adopted from (Xu et al., 2011; Dinev et al., 2013) and adjusted for the OSN context.
Disclosure Intention	4	Adopted from (Zhao et al., 2012) and adjusted for the OSN context.
Perceived Privacy	4	3 items adopted from (Dinev et al., 2013), 1 item newly developed for this study.

General privacy and propensity to share are measured as part of demographic questions.

3. Design of tutorials and warning messages

The devised tutorials in the survey represent a true reflection of Facebook functions, as

well as the incorporated warning messages. Given that it is unrealistic to fully cover each privacy control option in a single tutorial and that Facebook is constantly introducing new features and restructuring the existing functions, the tutorials developed in this study had been limited to illustrate seven available options specifically designed for Timeline and Tagging Management. All the select options have been available on Facebook for more than 6 months, and function tutorials targeting these options are widespread online, e.g. (“Facebook 101 Tutorial,” 2015, “Facebook Video Courses and Tutorials from,” 2015). Following the suggestion of Lim and Benbasat (2000) that tutorials utilizing graphical representations are more effective in affecting individuals’ learning outcomes than the text-based ones, tutorials developed in this study offer subjects with a graphic-based tutorials for the following seven options. Detailed demonstration of the function tutorial for group 4 can be found in Appendix E.

1) Control who can post on your timeline
2) Review each post that friends tag you in before they appear on your timeline
3) Control who can see posts you've been tagged in on your timeline
4) Remove the tag you don’t like
5) Report a post to get it removed by Facebook
6) Review tags people add to your own posts before the tags appear on Facebook
7) When you're tagged in a post, control who can be added to the audience if they aren't already in it

While the existence of warning messages is expected to significantly influence OSN users’ information disclosure behaviors (Cheng & Wu, 2010; Y. Wang et al., 2013; Xiao, 2010), too frequent exposure to warnings will show a diminishing effect, and cause individuals to be less sensitive to warning messages in the future (Magat, Viscusi, & Huber, 1988; Stewart & Martin, 1994). Accordingly, two warning messages showing the potential negative consequences resulted from not using or configuring certain privacy control options are developed for this study. The first warning message illustrates potential

negative consequences of not controlling who are authorized to post on one's Timeline; and the second message shows 'who could access photos that you have been tagged in' under default settings. Both messages are derived from the preliminary interview previously discussed. Taking the advice that case-based reasoning is more persuasive than instruction that only contains dos and don'ts (Jonassen & Hernandez-Serrano, 2002; Kolodner, 2014), both warning messages are presented with examples, as shown in the following table. Detailed treatment of the group receiving warning messages (group 3) can be found in Appendix E.

Development of Warning messages

Warning Messages	**Content**
On Timeline management	Be cautious! When you allow friends to post on your Timeline, please make sure they are trusty fellows, or you should check the updates on your Timeline regularly to avoid embarrassment such as unpleasant remarks or annoying ads. For example, if someone unpleasant happened between you and on of your Facebook friends, he / she might act on impulse and post some offensive words on your Timeline that are visible to all those that have access to your Timeline.
On Tagging Activities	Be cautious! Granting others the authority to tag you without notification may cause unforeseeable problems. For example, a frequently posting friend might tag you in many of his/her shared photos. Under the default tagging management setting, all your fiends on Facebook will be able to see photos that you've been tagged in, no matter whether you want them to see or not.

Another treatment group (group 4) is receiving function tutorials incorporating warning messages. For this group, the treatment offered to the function tutorial group (group 2) is integrated with the warning messages developed for group 3, as shown in Appendix E.

Appendix E: Online Survey

1. Demographic questions

1) How long have you been using Facebook?
    - More than 3 years
    - 2 - 3 years
    - More than 1 year and less than 2 years
    - 6 months – 1 year
    - Less than 6 months
2) Approximately how many friends you have on Facebook?
    - Less than 50
    - 50 - 99
    - 100 - 199
    - 200 - 299
    - 300 - 399
    - 400 - 500
    - More than 500
3) On average, approximately how much time per day do you spend on Facebook?
    - Less than 10 Minutes
    - 10 - 29 Minutes
    - 30 - 59 Minutes
    - 1 - 2 Hours
    - More than 2 Hours
4) What is your gender? (Male / Female)
5) What is your age?
6) What country do you currently live in?
7) Please indicate the highest level of education you have attained:
    - Less than high school
    - High school degree
    - College degree
    - Undergraduate degree
    - Graduate degree
8) Please select the activity(ies) that you frequently engage on Facebook (check all that apply):
    - Browse through new Posts posted by my Facebook friends
    - Share my thoughts or pictures via new Posts
    - Chat with my Facebook friends
    - Plan Events, join Groups
    - Play games or use other Apps on Facebook
    - Other, please specify...

2. Awareness checklists for control options

Each subject will be asked to specify his/her level of awareness (Yes, I am aware of this function / No, I am not aware of this function) for each of the function listed below. The first item measuring awareness is calculated as the number of control options each participant is aware of.

Checklist 1

1) **Control who can post on your timeline**

   Facebook allows you to decide who can post on your Timeline. Two available options are provided: Friends or Only Me.

2) **Review each post that friends tag you in before they appear on your timeline**

   When this function is enabled, you have to manually approve posts you're tagged in before they go on your timeline.

3) **Control who can see posts you've been tagged in on your timeline**

   Facebook allows you to choose who can see the posts on your timeline that you've been tagged in. There are five available options: Everyone, Friends of Friends, Friends, Only Me or Custom.

4) **Remove a tag you don't like**

   You can utilize this function to remove a tag you don't like. When a tag is removed, the original photo is still accessible to the authorized audience.

5) **Report a post to Facebook to get it removed**

   If a post contains abusive words or photos, you can use this option to report the post to Facebook to get it removed.

6) **Review tags people add to your own posts before the tags appear on Facebook**

   You can choose whether an approval from you is needed or not when someone who you are not friends with adds a tag to one of your posts. When you approve a tag, the person tagged and their friends may be able to see your post.

7) **When you're tagged in a post, control who can be added to the audience if they aren't already in it**

   Default setting of this option will allow all your Facebook friends to see a post if you are tagged in, even if they weren't in the original audience. You can also choose to add selected friends of you to the original audience by choosing 'Custom'. These people may see it in News Feed, search and other places on Facebook. You can also choose 'Only Me' for this option, in this case none of your friends will be added to the original audience of a post you're tagged in.

8) **Control who can see tag suggestions when photos that look like you are uploaded**

When a photo that looks like you is uploaded, Facebook will suggest adding a tag of you. This helps save time when adding tags to photos, especially when labeling many photos from one event. Suggestions can always be ignored and no one will be tagged automatically.

You can choose whether you are the only one seeing those suggestions or all your friends (the default setting) are able to see suggestions when a photo that looks like you is uploaded by them.

Checklist 2

1) **Login Alerts**

Login Alerts allow you to get an alert when anyone logs into your account from a new device or browser.

2) **Login Approvals**

Login Approvals is an extra layer of security that uses your phone to protect your account.

3) **App Passwords**

Generate app passwords. You are allowed to use an app password instead of your account password to securely log into apps such as Jabber, Skype, and Xbox.

4) **Trusted Contacts**

Trusted contacts are friends that can securely help you if you ever have trouble accessing your account. Facebook allows you to create a list of trusted contacts.

5) **Control the audience of your future posts**

You can manage the privacy of things you share by using the audience selector right where you post; available choices include Public, Friends, etc.

6) **Limit the audience for old posts on your Timeline**

You can use this function to change the content on your timeline you've shared with Friends of Friends or Public to Friends.

7) **Who can send you friend requests**

There are two available options for you, you can set to received friend request from Public or only from Friends of Friends.

8) **Control whose messages can be filtered into my Inbox**

You can filter your Inbox using one of the two available functions: 1) basic filtering (messages from friends and people you may know) or 2) strict filtering (messages from friends).

9) **Control who can look you up using the email address you provided**

This control option allows you to select who is able to search for you using your email address. You have three available options: Everyone, Friends of Friends or Friends. This function applies to people who currently can't see your email address.

10) **Control who can look you up using the phone number you provided**

This control option allows you to select who is able to search for you using the phone number you provided. You have three available options: Everyone, Friends of Friends or Friends. This function applies to people who currently can't see your phone number.

11) **Control whether search engines can be linked to your Timeline**

When this setting is on, search engines can provide links to your Timeline in their search results. When this setting is turned off, search engines will not display the links to your Timeline in their search results.

If you turn off this setting, it may take a while for search engines to stop showing the link to your timeline in their results.

12) **Control Apps, Websites and Plugins on your Facebook**

When you grant third party apps, websites or plugins the authority, you are able to use them on Facebook and elsewhere.

When Facebook's integration with apps, games and websites is disabled using this option, you can no longer use the third party apps or websites on Facebook.

13) **Control audience of your information that are posted through old versions of Facebook for mobile**

This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for Blackberry. You can set your audience from one of the following four groups: Public (default), Friends of Friends, Friends, Only Me.

14) **Control which of your information is available to applications, games and websites when your Friends use them**

Under this setting, you can manually choose which piece of your information (Hometown, Birthday, Family & Relationships, Photos, etc.) is available to third parties when your friends use them.

Your name, profile picture, gender, networks and user ID (along with any other information you've made public) is available to friends' applications unless you turn off Platform applications and websites.

15) **Audience Control for Ads from Third Party Sites**

Facebook currently does not give third party applications or ad networks the right to use your name or picture in ads. If Facebook allow this in the future, you can choose from the following two options: 1) show my information to My Friends, 2) show my information to no one.

16) **Pair Ads and Friends**
Facebook make it easier for you to know what your friends like to buy through this 'pair ads and friends' function. When select the 'Friends' option, you can find products and services you're interested in, based on what your friends share and like. When select the 'No one' option, no products or services recommendation will be sent to you based on your friends' activities on Facebook.

Additional questions in both checklists

1) Think about all the Timeline & Tagging management options we have presented to you, please specify your overall usage / configuration experience of those functions based on a scale from 1 to 7.
2) Think about all the Timeline & Tagging management options we have presented to you, please specify your overall familiarity of those functions based on a scale from 1 to 7.

3. Measurement items of key constructs

Subject's agreement on each item below is measured via a 7-point Likert Scale, from 'strongly disagree' to 'strongly agree'.

General Privacy Concern (GPC)

1) I am concerned that too much information about me and my online activities has been purposely collected.
2) I am concerned about my privacy when I am browsing through websites.
3) I am concerned that the personal information I disclosed online could be misused.
4) I am concerned that the personal information I disclosed online could be accessed by unknown parties.

Propensity to Share (PTS)

1) I feel happy to share my thoughts and pictures with my friends through online social networks such as Facebook.
2) Sharing my thoughts and pictures on social networks such as Facebook is a pleasure to me.
3) It feels natural for me to share my thoughts and pictures on social networks such as Facebook.
4) I find sharing my thoughts and pictures on social networks such as Facebook is fun and interesting.

Perceived Usefulness (PU)

1) I find the control options provided by Facebook useful to protect my privacy.
2) I find the control options provided by Facebook help me to keep my personal information and posts from the unwanted audience.
3) The control options provided by Facebook help me to manage my timeline and my posts.
4) The control options provided by Facebook help me to manage my photos and tags.

Perceived Self-efficacy (PSE)

1) I am capable of using control options on Facebook to control my timeline.
2) I am confident of using control options to manage my tags on Facebook.
3) I am capable of using control options on Facebook to control my photos.

Privacy Control (PCtrl)

1) I feel I have control over who can get access to my shared content such as posts and photos on Facebook.
2) I have control over what personal information I disclosed could be accessed by other people on Facebook.
3) I believe I have control over what activities other people can perform (e.g. comment or tag a photo) with my shared personal information on Facebook.

Perceived Privacy (PP)

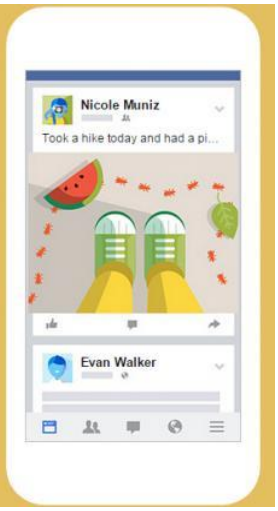
1) I feel I have enough privacy when I use Facebook.
4) I am comfortable with the amount of privacy I have on Facebook.
5) I think my privacy is preserved when I use Facebook.
6) I am satisfied with my state of privacy when I use Facebook.

Disclosure Intention (DI)

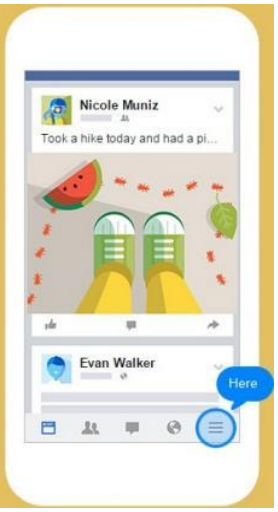
1) I am willing to disclose my personal information (e.g. post daily activities) on Facebook in the future.
2) It is probable for me to disclose my personal information to Facebook for daily social activities and other relevant usages.
3) It is possible for me to disclose my personal information to Facebook in the future to get connected with my friends
4) Given the need, I am willing to provide my personal information to Facebook in order to get the benefit of using it.

4. Function tutorial

You get to decide whether friends are allowed to post things on your Timeline or not.



To manage who can post on your Timeline, go to **Settings**. This function is available on the top right corner of your interface or bottom right corner if you are using a smartphone to login Facebook

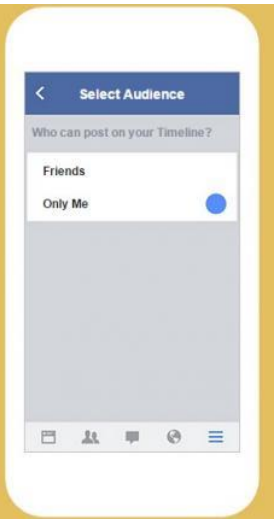


Go to **Settings** and select Timeline and Tagging.

Once you select **Timeline and Tagging**, you are able to deicide who can post on your Timeline with options.

Under the section **Who can post on your timeline**?, there's a menu that gives you control over whether your Friends are allowed to post on your Timeline.

Here you can choose whether you are the only one that can post on your Timeline or whether your Friends can post there, too.



You can also decide whether you want to review posts that friends tag you in before they appear on your Timeline.

Similarly, you can choose the audience for **Posts that you've been tagged in** on your Timeline under **Timeline and Tagging**. There are five available options: Everyone, Friends of Friends, Friends, Only Me or Custom.

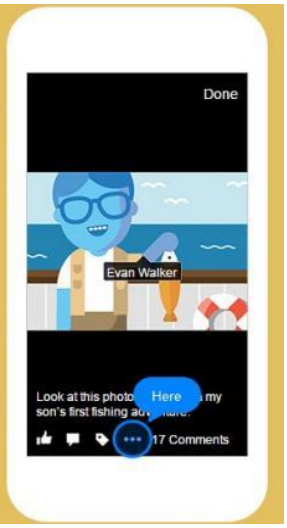
You can also decide **who can see what others post** on your Timeline.

For your own post, you can choose whether you want to review tags people added before they appear on Facebook.

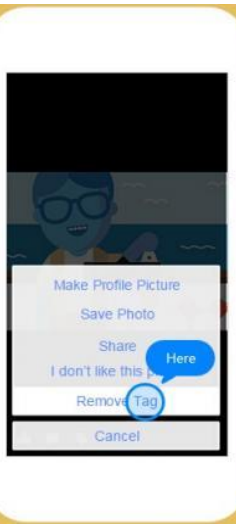
Furthermore, when you're tagged in a post, you can **add audience** to that post if they were not granted the access.

How to remove a tag?

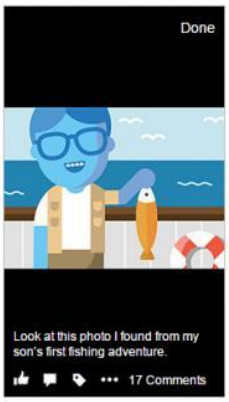
If you're tagged in a photo and don't want to be, go to the photo and open the menu at the bottom.



Choose **Remove Tag**.



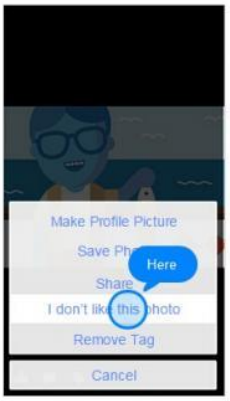
After you confirm, you'll be untagged and no one else can re-tag you in the photo.



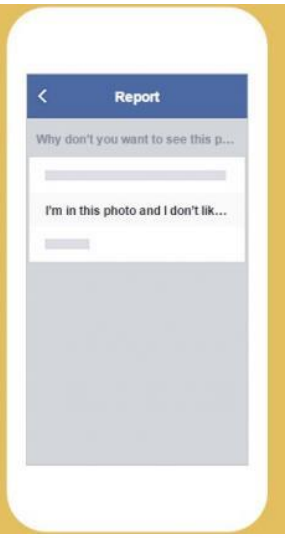
Keep in mind that the person who posted the photo might still have it on their own Timeline and in albums that their friends may see.

Other people in the audience for the photo might see it in News Feed or search results, too.

If you don't want the photo to be on Facebook anymore, go to the photo, open the menu at the bottom and choose **I don't like this photo**.



Next choose **I'm in this photo and I don't like it.**



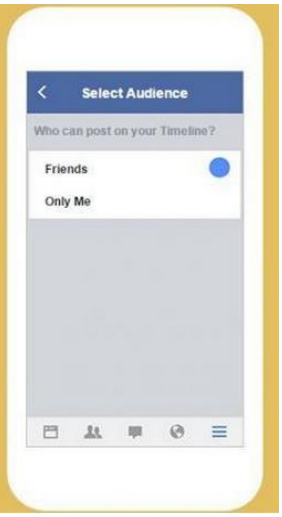
Then indicate a **reason** why you don't like that photo.

You can then send a message asking the person who posted the photo to take it down. This is the best way to get a photo removed.

5. Warning messages

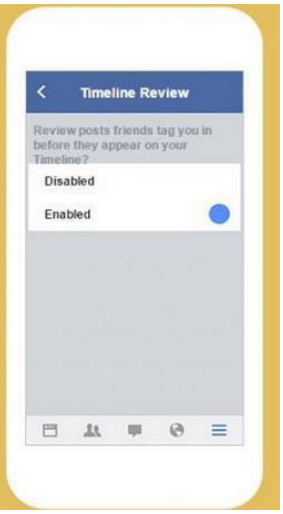
Under the **default** setting, your Friends are allowed to post things on your Timeline.

When you allow friends to post on your Timeline, please make sure they are trusty fellows, or you should check the updates on your Timeline regularly to avoid embarrassment such as unpleasant remarks or annoying ads.



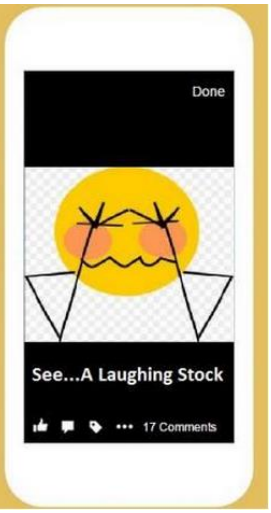
For Example, if something unpleasant happened between you and one of your Facebook Friends, he / she might act on impulse and post some **offensive** words on your Timeline that are visible to all those that have access to your Timeline.

You can deciede whether you want to **Review** posts friends tag you in before they appear on your Timeline.



Be cautious!
Granting others the authority to tag you without notification may cause unforeseeable problems.

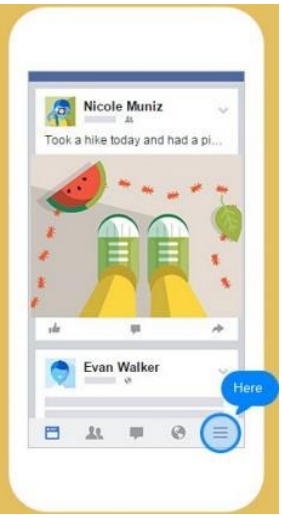
For example, a frequently posting friend might tag you in many of his/her shared photos.
Under the **default** tagging management setting, all your friends on Facebook will be able to see photos that you've been tagged in, no matter whether you want them to see or not.



6. Function tutorial incorporating warning messages

You get to decide whether friends are allowed to post things on your Timeline or not.

To manage who can post on your Timeline, go to **Settings**. This function is available on the top right corner of your interface or bottom right corner if you are using a smartphone to login Facebook

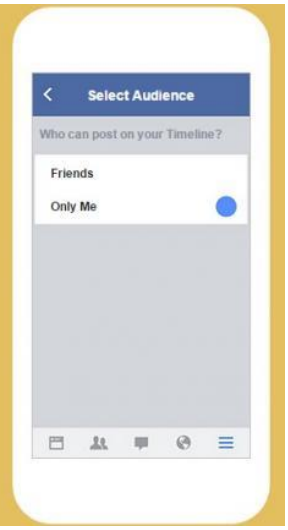


Go to **Settings** and select Timeline and Tagging.

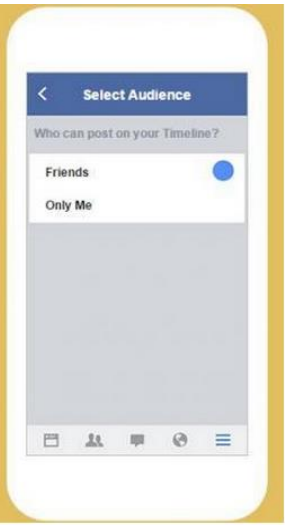
Once you select **Timeline and Tagging**, you are able to deicide who can post on your Timeline with options.

Under the section **Who can post on your timeline**?, there's a menu that gives you control over whether your Friends are allowed to post on your Timeline.

Here you can choose whether you are the only one that can post on your Timeline or whether your Friends can post there, too.



Be Cautious!
When you allow friends to post on your Timeline, please make sure they are trusty fellows, or you should check the updates on your Timeline regularly to avoid embarrassment such as unpleasant remarks or annoying ads.



For Example, if something unpleasant happened between you and one of your Facebook Friends, he / she might act on impulse and post some **offensive** words on your Timeline that are visible to all those that have access to your Timeline.

You can also decide whether you want to review posts that friends tag you in before they appear on your Timeline.

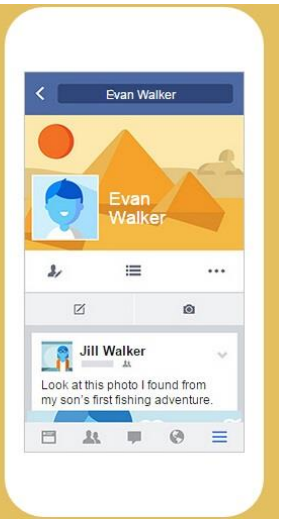
Similarly, you can choose the audience for **Posts that you've been tagged in** on your Timeline under **Timeline and Tagging**. There are five available options: Everyone, Friends of Friends, Friends, Only Me or Custom.

You can also decide **who can see what others post** on your Timeline.

For your own post, you can choose whether you want to review tags people added before they appear on Facebook.

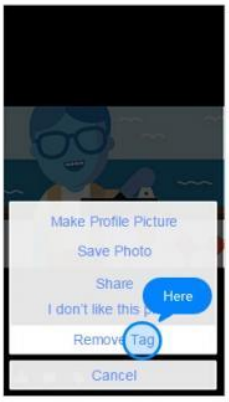
Furthermore, when you're tagged in a post, you can **add audience** to that post if they were not granted the access.

How to remove a tag?

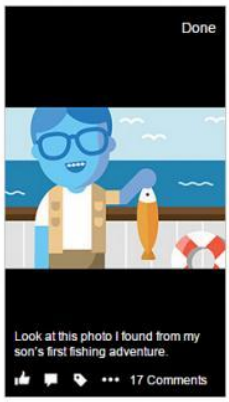


If you're tagged in a photo and don't want to be, go to the photo and open the menu at the bottom.

Choose **Remove Tag**.

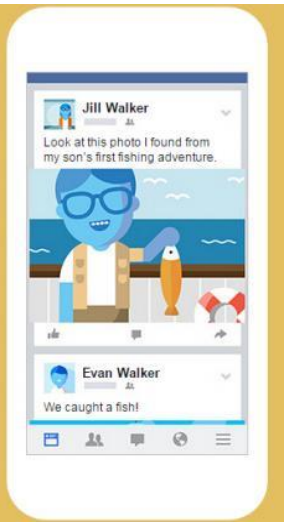


After you confirm, you'll be untagged and no one else can re-tag you in the photo.

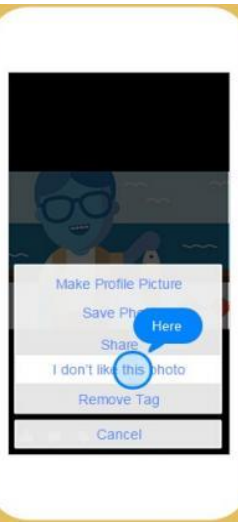


Keep in mind that the person who posted the photo might still have it on their own Timeline and in albums that their friends may see.

Other people in the audience for the photo might see it in News Feed or search results, too.



If you don't want the photo to be on Facebook anymore, go to the photo, open the menu at the bottom and choose **I don't like this photo**.



Next choose **I'm in this photo and I don't like it.**

Then indicate a **reason** why you don't like that photo.

You can then send a message asking the person who posted the photo to take it down. This is the best way to get a photo removed.

Be cautious!
Granting others the authority to tag you without notification may cause unforeseeable problems.

For example, a frequently posting friend might tag you in many of his/her shared photos.
Under the **default** tagging management setting, all your friends on Facebook will be able to see photos that you've been tagged in, no matter whether you want them to see or not.

Appendix F: Data Cleaning Procedure

Altogether 364 AMT workers have completed our online survey. Their responses are organized and cleaned in the following procedure to ensure the reliability of the dataset.

1. Remove re-takers

   Subjects with duplicate AMT worker ID and duplicate IP address are removed. In addition, some of the subjects have previously failed our screening questions and completed our survey in a later attempt; those subjects are removed as well. 15 subjects have been removed in this step.

2. Remove subjects that failed attention check (trap questions)

   There are two attention check questions in the survey, e.g. for this question, please simply choose ‘strongly disagree’. 9 subjects are removed due to incorrect answer of these attention check questions.

3. Remove subjects from outside the United States

   Although it was set through AMT settings that only residents of the United States are qualified to take part in our survey, some subjects are actually from other countries, which were revealed by a residency specifying question in the survey. 15 subjects from India and 1 subject from Bulgaria are removed from the dataset.

4. Remove subjects that used far too less time in answering the surveys

   There are on average 80 questions for each treatment groups, not to mention the tutorial treatments offered to some groups. The average time answering the survey is 680 seconds. Based on the time participants took in completing the survey, 12 subjects within the lower five percent in the respective group and have used unreasonably small amount of time have been removed.

After the data cleaning procedure, 313 subjects remained. 16 subjects who have failed the manipulation check were further removed. Altogether there are 297 subjects qualified for future analysis.

Appendix G: Sample Demographics

Gender	Frequency	Percent
Male	168	56.6
Female	129	43.4
Total	297	100.0

Age	Frequency	Percent
18 - 29	138	46.5
30 - 39	93	31.3
40 - 49	34	11.4
50 - 59	27	9.1
60 +	5	1.7
Total	297	100.0

Number of friends	Frequency	Percent
Less than 50	37	12.5
50 - 99	50	16.8
100 - 199	65	21.9
200 - 299	50	16.8
300 - 399	31	10.4
400 - 500	20	6.7
More than 500	44	14.8
Total	297	100.0

Length of usage	Frequency	Percent
More than 3 years	263	88.6
2 - 3 years	23	7.7
More than 1 year and less than 2 years	11	3.7
Total	297	100.0

Usage time per day	Frequency	Percent
Less than 10 Minutes	37	12.5
10 - 29 Minutes	80	26.9
30 - 59 Minutes	89	30.0
1 - 2 Hours	61	20.5
2 - 3 Hours	20	6.7
More than 3 Hours	10	3.4
Total	297	100.0

Activities	Frequency	Percent
Browse through new Posts posted by my Facebook friends	285	96.0
Share my thoughts or pictures via new Posts	194	65.3
Chat with my Facebook friends	215	72.4
Plan Events, join Groups	100	33.7
Play games or use other Apps on Facebook	91	30.6
Other, please specify...	11	3.7

Education	Frequency	Percent
Less than high school	2	.7
High school degree	90	30.3
College degree	113	38.0
Undergraduate degree	64	21.5
Graduate degree	28	9.4
Total	297	100.0

Group	Frequency	Percent
1	50	16.8
2	49	16.5
3	53	17.8
4	49	16.5
5	48	16.2
6	48	16.2
Total	297	100.0

Appendix H: Additional Mediation Analysis

The mediation role of perceived self-efficacy between awareness and privacy control is also tested and supported.

		Path d (Awareness, PSE -> PCtrl)
Path a (Awareness -> PSE)	0.324***	
Path b (PSE -> PCtrl)	0.461***	0.468***
Path c (Awareness -> PCtrl)	0.131*	-0.020

***p<0.001, **p<0.01, *p<0.1

The privacy control only partially mediated the impact of perceived self-efficacy and PU on perceived privacy, as shown is the following tables. Given the fact that privacy control is frequently claimed as a key dimension of privacy, this finding is consistent with this dimension view.

		Path d (PSE, PCtrl -> DI)
Path a (PSE -> PCtrl)	0.461***	
Path b (PCtrl -> PP)	0.713***	0.779***
Path c (PSE -> PP)	0.216**	-0.143*

***p<0.001, **p<0.01, *p<0.1

		Path a, b, c (PU, PCtrl -> DI)
Path a (PU -> PCtrl)	0.555***	
Path b (PCtrl -> PP)	0.713***	0.624***
Path c (PU -> PP)	0.506***	0.160**

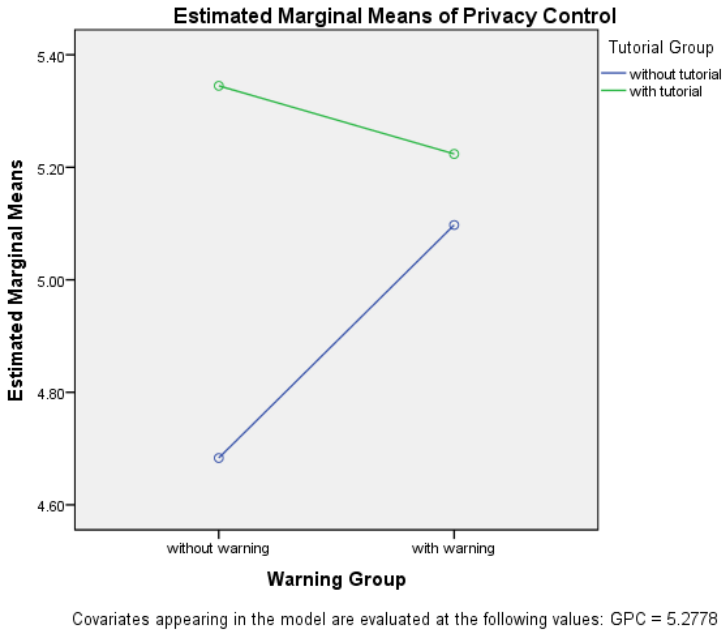
***p<0.001, **p<0.01, *p<0.1

Appendix I: Effect of Tutorials and Warning Messages

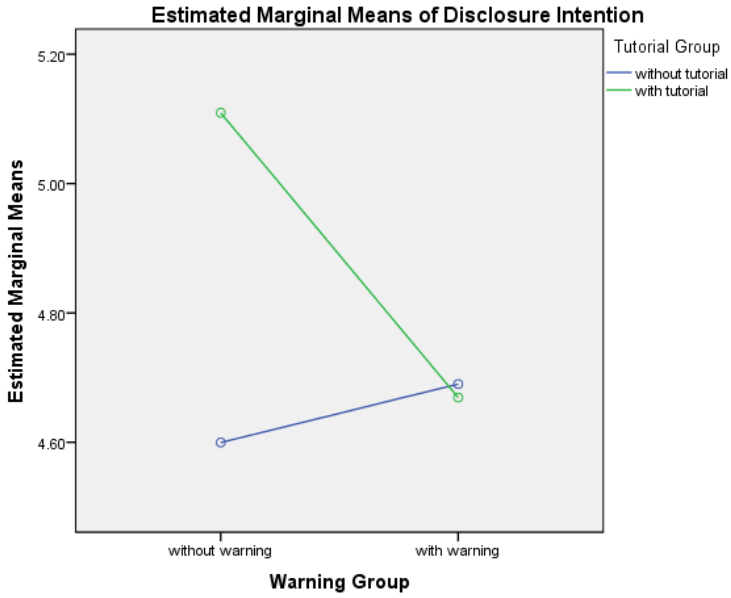
It is hypothesized that tutorials are effective in improving Awareness, perceived self-efficacy and perceived uesfulness, while warning messages are effective in increasing PU. In this study, the awareness and self-efficacy increasing techniques are fabricated into the following four treatment groups:

	No warning messages	**Warning messages**
No tutorial	Group 1	Group 3
Tutorial	Group 2	Group 4

In order to better understand the effect of tutorials and warning messages on individuals' sense of privacy control and disclosure intention. 2 (with or without tutorial) by 2 (with or without warning messages) ANOVAs are further performed. Controlling for the impact of general privacy concern, a significant interaction is found between tutorial groups and warning message groups (F = 5.50, p = 0.02). Without the presence of tutorial, waning messages can effectively improve individuals' perceived privacy control, hopefully through the increase in PU of control options. This effect, however, no longer exists if function tutorials are already provided, as shown in the following figure.



Another marginally significant interaction (p =0.10) was found between tutorial groups and warning message groups in terms of their impact on disclosure intention. It is found that the plain tutorial group (group 2) works best to improve individuals' disclosure intention on Facebook, while this impact is mitigated by the presentation of warning messages, as shown in the following figure. In line with our previous discussion, the presence of warning messages probably has increased individuals' perceived risk when posting on Facebook, which in turn has a negative influence on their disclosure intention.



Covariates appearing in the model are evaluated at the following values: PTS = 5.1441

Appendix J: Privacy Control and Perceived Privacy

In the literature review, it is identified that there are three available perspectives: the antecedent view, the dimension view, and the control is privacy view. In the hope of offering some empirical evidence regarding the relationship between privacy control and perceived privacy, items measuring privacy control and perceived privacy in this study are analyzed using the factor analysis technique. Only one factor is extracted under free loading using maximum likelihood estimation, explaining 72.9 % of the variance. As shown in the following table.

Factor matrix with one factor

	Factor 1
PCtrl1	.815
PCtrl2	.835
PCtrl3	.620
PP1	.919
PP2	.926
PP3	.896
PP4	.924

When two factors are extracted, 85% variance can be explained. In the following table, it can be seen that items measuring privacy control and perceived privacy fell under the assigned latent variables respectively.

Factor matrix with two factors

	Factor 1	Factor 2
PCtrl1	.707	.823
PCtrl2	.731	.826
PCtrl3	.428	.896
PP1	.953	.544
PP2	.959	.550
PP3	.926	.538
PP4	.956	.552

When substituting the position of privacy control with perceived privacy in the proposed research model, the impact of perceived self-efficacy is no longer significant, suggesting that perceived privacy and privacy control enabled by personalization options, although highly correlated, are two different constructs.