THIRD PERSON EFFECT AND INTERNET PRIVACY RISKS

A Dissertation

by

HONGLIANG CHEN

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Robert Kirby Goidel
Committee Members,	Richard L. Street, Jr.
	Jennifer Lueck
	Myeongsun Yoon
Head of Department,	J. Kevin Barge

August 2017

Major Subject: Communication

ABSTRACT

The current study tests the third-person effect (TPE) in the context of Internet privacy. TPE refers to the phenomenon that people tend to perceive greater media effects on others than on themselves. The behavioral component of TPE holds that the self-others perceptual gap is positively associated with support for restricting harmful media messages. Using a sample (N=613) from Amazon Mturk, the current research documented firm support for the perceptual and behavioral components of TPE in the context of Internet privacy. Moreover, social distance, perceived Internet privacy knowledge, negative online privacy experiences, and Internet use were found to be significant predictors of the TPE perceptions of Internet privacy risks. There are four novel contributions of the current study. First, this study systematically tests TPE in a new context－Internet privacy. Second, this study examines five antecedents of TPE perceptions, of which perceived Internet privacy knowledge, negative online privacy experiences, and Internet use are novel to TPE studies. Unlike prior studies which assume social distance and desirability of media content, the current study provides direct empirical tests of these two antecedents. Third, prior research primarily examines support for censorship of harmful media messages, a context in which individuals do not have control over policy enforcement. In the case of Internet privacy, people can decide whether to adopt privacy protective measures or not. The current study addresses two types of behavioral intentions to reduce privacy risks: (1) the willingness to adopt online privacy protection measures; and (2) recommend such measures to others. Fourth, unlike

prior studies using fear based theories to investigate Internet privacy issues, the current

tests Internet privacy from a novel perspective一TPE theory.

ACKNOWLEDGEMENTS

Diligence is the path to the mountain of knowledge, hard work is the boat through the endless sea of learning. Han Yu.

Chinese people believe that perseverance is the key of success. There are challenges on the road to be an excellent scholar but I have been fortunate to receive tremendous support and guidance during the past four years at Texas A&M University.

Above all, I would like to express my sincere gratitude to Dr. Christopher E. Beaudoin and Dr. Traci Hong who taught me how to develop research projects systematically and how to be a good person. Since I came to Texas A&M, I have had opportunities to work on research projects under their careful supervision. Each comment they provided led me to grow as a communication scholar. Their rigorous approach to research was the most valuable lesson I as a student.

My advisor, Dr. Robert Kirby Goidel set an example of as a scholar. I have been grateful for his guidance as I have written this dissertation. When I have felt lost or uncertain about my future career, his encouragement and advice encouraged me to move forward. I am very grateful to Dr. Myeongsun Yoon, Dr. Richard L. Street, Jr., and Dr. Jennifer Lueck for their service as dissertation committee members. Their intelligent suggestions helped me to complete my dissertation successfully.

I appreciate the support from other faculty members, my graduate cohorts, and my friends at Texas A&M. Whenever I have needed help, someone has always stood by

me and lent a helping hand. The support and collegiality made my study experience more enjoyable.

Last but not least, I would like to say thank you to my family: my wife Qike Jia, my father Shibin Chen, and my mother Jingzhi Li. Without their love and consistent support and love, I would be nowhere.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by a dissertation committee consisting of Professor

Kirby Goidel, Richard Street, and Jennifer Lueck of the Department of Communication

and Professor Myeongsun Yoon of the Department of Educational Psychology.

All work for the dissertation was completed independently by the student.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 Importance of Internet Privacy

Online information privacy is a growing concern. The ubiquity of online information collection has spurred Internet users' privacy concerns (Li, Sarathy, & Xu, 2010). Internet users worry about the unauthorized access to personal data online as well as the consequences of privacy loss (Smith, Dinev, &Xu, 2011). Privacy invasions occur in three ways. First, providing personal information when registering on websites increases the risk of privacy loss. For instance, social media require users to provide personal information to open an account that allows users to find contacts with similar interests and backgrounds, but the cost is exposing private information to third-party agencies (Chen & Beaudoin, 2015). Through data mining technology, they can gain access to millions of users' data and design spam emails and soliciting messages accordingly. Second, hackers distribute malware through the Internet to collect private information (Shin, 2010). Visiting unsafe websites and opening emails from unknown sources can result in the installation of malware. Hackers use these programs to steal users' credit card information that can result in the monetary loss (Debatin, Lovejoy, Horn, & Hughes, 2009; Moore, Clayton, & Anderson, 2009). Third, criminals design fake websites to steal money from Internet users. These websites offer special discounts and descriptions of nonexistent products to seduce targeted audience (Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010). Once the transaction is completed, websites can acquire extensive bank account data within seconds (Zahedi, Abbasi, & Yan, 2015).

The major negative consequence of online privacy invasion is the monetary loss. For criminals, anonymous online environments provide opportunities to design fake information to lure potential victims. According to FBI's Internet Crime Complaint Center, the reported financial loss of Internet scams was more than $800 million in 2014 (Internet Crime Complaint Center, 2014). The Internet-based media opened new gates for criminals to implement a variety of scams (Pratt, Holtfreter, & Reisig, 2010; Reyns, 2013; Salu, 2004; Vahdati & Yasini, 2015; Zahedi et al., 2015). Another consequence of privacy invasion is relational conflicts. The unauthorized access to personal accounts can result in inappropriate comments and postings that may spur conflicts with online contacts, damage to users' reputation, and loss of social opportunities (Chen, Beaudoin, & Hong, 2016a).

Prior research has examined Internet privacy using two fear based theories—protection motivation theory (PMT) and extended parallel process model (EPPM). PMT posits that before engaging in the risk-reduction behavior, people first assess the threat and the coping measures cognitively, then develop motivation for risk-reduction behaviors, and finally make the behavioral changes (Rogers, 1975). EPPM adds that only when people perceive both high efficacy and high threat, they are willing to engage in risk reduction behaviors, whereas in other cases, they tend to ignore the threat (Witte, 1994). Related studies provided limited support that privacy protection motivation is the outcome of threat appraisal and coping appraisal (Abbasi et al., 2010; Chen et al., 2016a; Chen, Beaudoin, & Hong, 2016b; Mohamed & Ahmad, 2012; Wirtz, Lwin, & Williams, 2007; Youn, 2009). Some studies found that even though some Internet users expressed

high privacy concerns, they are still willing to disclose private information as a result of online social interaction and online shopping (Norberg, Horne, & Horne, 2007; Young & Quan-Haase, 2013). The mixed results indicate that Internet users often do not follow the logics of PMT and EPPM before engaging in risky online activities.

One potential limitation of PMT and EPPM can be people's tendency to attribute privacy risks to others but not to themselves (Debatin, Lovejoy, Horn, & Hughes, 2009). Internet users tend to believe that they will not encounter negative experiences because of perceived control over their privacy online (Li, 2008). However, such perceptions can be incorrect for some users. The low awareness of one's online privacy risks explains why the adoption rate of privacy protective measures is relatively low (Buchanan & Whitty, 2014).

1.2 Third-person Effect (TPE) and Internet Privacy

Given these limitations, researchers need to incorporate other theoretical frameworks to study Internet privacy. One alternative theoretical framework is the third-person effect (TPE). In communication studies, TPE theory has been widely used to explain differing perceptions of media effects on self and others. The perceptual component of TPE holds that people tend to perceive greater media effects on others than on self (Davison, 1983). In studies of traditional mass media (i.e., television and newspaper) (Gunther, 1995) and the Internet (B. Lee & Tamborini, 2005), researchers have found that people often think that harmful media messages influence others' judgments on certain issues but the impact on themselves is minimal.

The behavioral component of TPE adds that people's overestimation of media effects on others can increase their support for restricting harmful media content (Xu & Gonzenbach, 2008). The majority of existing research emphasizes the association between TPE perceptions and the intention to support media censorship (Xu & Gonzenbach, 2008). For instance, in a study of Internet pornography, scholars found that the perceived negative effects of pornography on others led to greater willingness to support the related media censorship (Chen, Wu, & Atkin, 2015). Very few studies assessed the behavioral component of TPE in contexts other than media censorship that yielded mixed results, ranging from a non-significant correlation (Gunther, 1991) to a moderate correlation (Tewksbury, Moy, & Weis, 2004) to a strong correlation (Gunther & Storey, 2003; Tsfati & Cohen, 2003). A recent meta-analysis suggested that future research should expand the focus of behavioral intentions in contexts other than media censorship (Xu & Gonzenbach, 2008).

1.3 Aims of Current Study

The current study aims to contribute to the literature of TPE and Internet privacy in four ways. First, this study systematically tests TPE in the context of the Internet. Most existing TPE studies focus on conventional mass media (i.e., radio, television, and newspaper), in which, people have limited choice in media content (Gunther, 1991, 1992). In contrast, on the Internet, people have access to an abundance of media information and a variety of Internet services (Flanagin, Metzger, Pure, Markov, & Hartsell, 2014). Individuals are not passive receivers of media messages but actively use the Internet for useful information, social contacts, entertainment, online shopping, and

online gaming (Flanagin et al., 2014). In addition to the benefits, the Internet also triggers concerns about privacy. The pervasiveness of Internet privacy risks necessitates average users to understand the mechanisms of privacy invasions and employ protective measures accordingly. In association with prior studies, this study provides insight into how TPE perceptions of Internet privacy risks differ from traditional media.

Second, the current study addresses five antecedents of TPE perceptions of Internet privacy risks. Prior studies have focused on two antecedents—desirability and social distance. In the research on desirability, researchers have noted that desirable media messages decrease TPE perceptions, whereas undesirable media messages function in the opposite way (Paul, Salwen, & Dupagne, 2000). In the research of social distance, researchers found that social distance between self and a reference group positively predicts the magnitude of TPE perceptions (Paul et al., 2000). Prior studies assume the anti-social[1]media messages, such as pornographic and violent videos, to be undesirable, and the pro-social media content[1], such as anti-smoking advertisements, to be desirable (Perloff, 1999). Also, researchers assume the social distance between self and others according to the differences in social class, gender, race, and other personal characteristics (Houston, Hansen, & Nisbett, 2011). For instance, college students perceive other students in the same university as closer than residents living in another state. Unlike prior studies, the current study provides empirical tests of desirability and social distance. Moreover, three other novel antecedents of TPE perceptions of Internet

---

[1] Pro-social behaviors refers to a social behaviors that benefits the society, whereas anti-social behaviors are the conducts that are against the social norms (Hodge & Lonsdale, 2011).

5

privacy—perceived Internet privacy knowledge, negative online privacy experiences, and Internet use—are also tested. The findings of the current study, thus, provide implications for research and practice specific to how Internet security providers can, by decreasing the TPE perceptions of Internet privacy risks, raise the behavioral intentions to adopt privacy protective measures.

Third, prior studies operationalize the behavioral component of TPE as the willingness to endorse restrictions on harmful media content. It is the government and media authorities that determine what media content is harmful, sensitive, and politically incorrect (Xu & Gonzenbach, 2008). Individual users cannot decide what type of media content to be censored. The current study expands TPE research to a novel context— Internet privacy. Internet users can respond to the privacy risks individually by adopting protective measures. Individual perceptions and behaviors, not the government agencies, play principal roles in reducing privacy loss on the Internet. The current study focuses on two types of behavioral intentions: 1) the willingness to adopt privacy protection measures, and 2) the willingness to recommend such measures to others. The current study aims to advance the understanding of how TPE perceptions impact behavioral intentions to adopt privacy protective measures.

Fourth, the current study tested the antecedents of privacy protection intention from a novel perspective—TPE. Prior Internet privacy studies have used PMT and EPPM to test people's behavioral intentions to protect online privacy (Mohamed & Ahmad, 2012; Youn, 2009; Youn & Hall, 2008). These two fear based theories posit that when people perceive a high threat and high effectiveness of coping strategies, they are

likely to adopt protective measures (Witte, 1994). Prior studies of Internet privacy found

limited support for fear based theories, indicating that the cognitive appraisal of privacy

risk and protection measures cannot fully predict the privacy protection intention. The

current study advances an alternative framework—TPE—to explore the antecedents of

privacy protection intention.

2. LITERATURE REVIEW

2.1 TPE Theory and Conceptualization

TPE was found in the studies of conventional mass media. In Davison's (1983) early research, he detected that college students held distinct perceptions of media effects on self and others. Respondents reported greater perceived influence of political and commercial advertisements on others than on themselves. Davison's innovative research unveiled a new chapter in media audience study－TPE. At the core of this research is the perceptual component of TPE, which entails that people perceive greater media influence on others than on self (Davison, 1983). As Davison (1983) noted, media viewers often think that media messages do not have a sizable effect on "me" and "you," but have a strong effect on "them." The behavioral component of TPE adds that this biased perception can lead to behavioral intentions to thwart the media influence (Xu & Gonzenbach, 2008). Multiple studies have found support for TPE. For instance, a meta-analysis conducted by Paul and colleagues (2000) documented 32 studies that support the existence of TPE in the contexts of pornography, political news, violent media content, and video games. TPE research on the Internet has been primarily limited to online pornography, where multiple studies found support for TPE (B. Lee & Tamborini, 2005; Lo & Wei, 2002, 2005; Wu & Koo, 2001). Researchers found that people perceive a greater negative impact of Internet pornography on others (Chen et al., 2015).

Critical to the current study is that there has been a very limited extension of Internet research to Internet privacy. In fact, only three empirical studies have examined

TPE perceptions of Internet privacy. Debatin and colleagues (2009) found that, even though people are concerned about Internet privacy, they still upload large amounts of personal data online because they often ascribe related privacy risks to others. Additionally, users who experienced privacy loss were found to be more likely to change privacy settings than those who merely heard online privacy risks from others and media. While the findings are suggestive, this study used qualitative interview methods and did not test TPE in a rigorous manner. Two survey studies have tested TPE perceptions of Internet privacy (Cho, Lee, & Chung, 2010; Li, 2008). Cho and colleagues (2010) found that Internet users tend to believe that others are more vulnerable to online privacy risks. Perceived control over online privacy and prior online privacy experiences were found to be significant predictors of TPE perceptions. In another study, Li (2008) found that respondents with stronger perceived computer skills and knowledge perceive themselves as having greater control over their Internet privacy. A limitation of these two studies is that computer skills and knowledge may not fully reflect a person's understanding of online privacy risks.

2.2 Theoretical Bases

Two important psychological theories—attribution theory and biased optimism theory—provide explanations of TPE (Paul et al., 2000; Xu & Gonzenbach, 2008). This literature review centers on these two theories.

2.2.1 Attribution Theory

Attribution theory refers to an individual's appraisal of the causes of certain behaviors (Paul et al., 2000). Researchers proposed that people seek to understand

surrounding events and relevant behaviors based upon their personal experiences and observations (Heider, 2013). According to Paul and colleagues (2000), attribution theory consists of four assumptions: 1) people perceive behaviors as intentional or with certain causes; 2) people possess traits, abilities, and intentions that predict behaviors; 3) people assess behaviors and events by using internal factors (e.g., knowledge, attitudes, moods, needs, and preexisting opinions) and external factors (e.g., task difficulty); and 4) people usually perceive others to be similar to themselves.

Scholars have found, that at least in some situations, the fourth assumption of attribution theory does not hold. Heider (2013) notes that people sometimes assume other people to be different from themselves. Researchers refer to this phenomena as "actor and observer differences" (Jones & Nisbett, 1972). For instance, a student, as an actor, may submit an assignment late and explain to his or her professor that such a tardy submission is due to a computer malfunction. However, the professor, as an observer, may attribute the tardy submission to the student's laziness. In such scenario, actors (e.g., the student in the prior example) tend to attribute actions to situational factors (i.e., factors external to a person), whereas observers (e.g., the professor in the prior example) are likely to ascribe the same actions to dispositional properties (i.e., factors internal to a person) (Jones & Nisbett, 1972; Paul et al., 2000). The actor-observer difference is an outcome of people's underestimation of situational factors and overestimation of dispositional factors (Zebrowitz, 1990). Gunther (1991) further noted that the differing perception of dispositional factors is the main contributor of TPE perceptions of media content. Media users tend to overestimate the effect of dispositional factors on

themselves, thinking that they fully understand the persuasive purpose of media content but underestimate dispositional factors on others, assuming that others lack the ability to judge the persuasive intent of media messages (Gunther, 1991; Rucinski & Salmon, 1990). Researchers call people's tendency to perceive oneself in a favorable manner as self-serving bias (Campbell & Sedikides, 1999). Self-serving bias leads people to think that their performance is better than others, which results in enhanced self-esteem (Gunther, 1991).

2.2.2 Biased Optimism

Another theoretical base of TPE is biased optimism, which makes individuals believe they are less likely to encounter negative experiences than others (Paul et al., 2000). There are two aspects of biased optimism: 1) people believe that they are more likely to encounter desirable experiences than others, and 2) people tend to believe that positive events are more likely to occur to themselves than others (Paul et al., 2000). For instance, prior research found that people believe that they are better drivers (Svenson, 1981) and receive better health care (Culbertson & Stempel, 1985). In this manner, people are expected to hold differing perceptions of media effects on themselves versus others (Tyler & Cook, 1984). Another rationale for biased optimism is that, by aiming to maintain self-esteem, people perceive themselves as smarter than others and, as a result, they can resist the media influences but others cannot (Paul et al., 2000).

There are two notable empirical studies related to biased optimism. In an experimental study, Gunther and Mundy (1993) assigned respondents to read eight print advertisements, four positive and four negative. The results indicated that, for the

negative issues, respondents reported that they would not be influenced by media messages, whereas others would be influenced. In contrary, for the positive issues, people were more likely to accept the positive media messages than others. In the second study, researchers found that the credibility of media messages is responsible for the size of the TPE perceptions (Brosius & Engel, 1996). For a credible medium, such as newspapers, the TPE perceptions of media influence are trivial. However, for commercial advertisements (which are viewed to be unreliable), people tended to perceive that others are more likely to be influenced. These two studies confirm people's biased optimism about media effects. Biased optimism has also received robust support in other contexts, including health care adequacy (Culbertson & Stempel, 1985), being a crime victim (Perloff, 1999), contracting AIDS (Bauman & Siegel, 1987), and suffering from bungee jumping accidents (Middleton, Harris, & Surman, 1996).

The similarity between biased optimism and TPE is that both theories aim to compare self and others. The comparison depends on the awareness of others' existence in certain social environments and the judgment of others (Glynn, Ostman, & McDonald, 1995; Tyler & Cook, 1984). Some scholars argue that TPE is an example of biased optimism in the context of media research (Brosius & Engel, 1996). There are two aspects of TPE that differ from the biased optimism. First, TPE is often related to perceptions of negative media messages, whereas biased optimism involves both negative and positive topics (Li, 2008). Second, TPE often entails a specific reference group (e.g., residents living in other states), whereas biased optimism, at times, only reflects the promoted perception of self (Li, 2008).

2.3 Behavioral Component of TPE

Another innovative aspect of this study entails the behavioral component that holds that TPE perceptions of media effects can lead people to develop behavioral intentions to counteract the negative media influence (Davison, 1983). Davison (1983) argued that individuals tend to think they can resist negative media effects but others are likely to be impacted. For instance, Internet users with high TPE perceptions tend to perceive high control over privacy online but recommend others to manage their online privacy carefully. Researchers found that, when people possess high TPE perceptions, they tend to support the restriction of such media content, but refuse to change their own media use habits (Gunther, 1995; Paul et al., 2000; Wu & Koo, 2001; Xu & Gonzenbach, 2008; Youn, Faber, & Shah, 2000).

Specific to censorship (Gunther & Storey, 2003; Perloff, 1999), scholars have found that TPE perceptions have an influence on individuals' intention to support related censorship (Chen et al., 2015; Gunther, 1995). Censorship refers to the suppression of public communication, speech, or other types of media, which contain harmful, politically incorrect, or sensitive content (Fu, Chan, & Chau, 2013). Related TPE research on censorship includes restrictions on pornography (Chen et al., 2015), violent media (Rojas, Shah, & Faber, 1996), violent music (McLeod, Eveland, & Nathanson, 1997), television violence (C. Hoffner & Buchanan, 2002), and gambling advertisements (Wan & Youn, 2004; Youn et al., 2000), all of which documented support for the behavioral component of TPE.

Very few studies have extended the behavioral component of TPE in contexts other than censorship. Existing studies yielded mixed results. Researchers found no support for the relationship between TPE perceptions and the willingness to support a penalty against a newspaper which presented defamatory news stories (Gunther, 1991). In another study of the millennium bug[2], researchers studied how TPE perceptions of millennium bug news predicted people's intention to stockpile food, water, and gas. The people with high TPE perceptions were found to perceive others were panicked about the arrival of 2000 (Tewksbury et al., 2004). Also, researchers found that TPE perceptions of news coverage of unsafe Israeli towns tended to increase people's support for residence relocation for these unsafe residents (Tsfati & Cohen, 2003). The mixed results of related studies suggest that personal experiences and preexisting knowledge influence the association between TPE perceptions and behavioral intentions. The current study aims to test the behavioral component of TPE in a new context—Internet privacy.

Using fear based theories, prior Internet privacy literature has widely tested the effects of threat appraisal and coping appraisal on behavioral intentions to engage in risk-reduction behaviors. PMT assumes that people follow a logical sequence to develop intention of protective behaviors, of which people first engage in threat appraisal and coping appraisal, then develop privacy protection motivation, and finally engage in

---

[2] Millennium bug is also referred as the Year 2000 Problem. Because the early software uses two digits to represent the year, 2000 is indistinguishable from 1900. It is expected that computers in charge of power and communication will be frozen. The transportation system will be impacted. People feared that millennium bug will impact their life significantly.

behavioral changes (Rogers, 1975). EPPM adds that only when people perceive a high threat and high efficacy are they willing to engage in risk-reduction behaviors (Witte, 1994). In the other cases, people tend to ignore the risks. Some studies found support for the framework of PMT and EPPM, suggesting that the perceived Internet privacy threat and the perceived effectiveness of privacy protection measures predict the privacy protection intention (Mohamed & Ahmad, 2012; Youn, 2009). In contrast, other studies detected that the threat appraisal and coping appraisal cannot fully predict the privacy protection intention (Chen et al., 2016a, 2016b). The mixed results suggested the need to provide an alternative theory to explain people's privacy protection intention.

Fear based theories were developed in the context of health. The health management and the promotion of healthy behaviors are complex processes that require people's comprehensive understandings of related health issues. The benefits of healthy behavioral change can only be seen in the long run (Milne, Orbell, & Sheeran, 2002). Because of the high barriers to behavioral changes, people are likely to follow the logic if PMT and EPPM to make further decisions. For instance, in the physical exercise campaigns, researchers documented high resistance of behavioral changes. To persuade people to engage in the physical exercises, the campaigners need to provide a thorough introduction on the health risks and the effectiveness of body exercises and then frequently monitor audience engagement (Milne et al., 2002). There is an immediate effect on audience's increase of physical exercises, but it decays after a period of time.

Unlike the high-barrier behavioral changes, there are other types of health behaviors require less efforts. For instance, the one-time flu shot can protect against

influenza. The generated antibody protects protection for the high-risk population, such as children and elder people (Bish, Yardley, Nicoll, & Michie, 2011). The barrier to such protective measure is relatively lower that one visit to a nearby pharmacy store is enough. Similarly, the Internet privacy protective measures can be as simple as changing the passwords, avoiding the suspicious websites, or installing anti-virus software. People's decisions regarding the adoption of privacy protections may not be as logical and complex as high-barrier health behavioral change (i.e., physical exercises & quit smoking). The key to increase the adoption of online privacy protections is to increase people's perceived relevance of Internet privacy risks. TPE provides a valuable addition to test if the differential perceptions of Internet privacy risks result in the low intention to adopt protective measures. Ignorance of online privacy protections could be the outcome of TPE perceptions. Similarly, beliefs that they will not be a subject of privacy loss could also lead to the indifference toward protective measures. This study aims to test if TPE perceptions of Internet privacy influence intent to personally adopt protective measures and to recommend these measures to others.

2.4 Antecedents of TPE

Previous studies have addressed two antecedents of TPE—desirability of media content and social distance of comparison groups in conventional media contexts. The current study extends this research by more directly measuring and testing desirability and social distance within the context of Internet privacy. This study also assesses three other novel antecedents of TPE—perceived Internet privacy knowledge, negative online privacy experience, and Internet use.

2.4.1 Social Distance

Social distance reflects the perceived difference between individuals with different backgrounds (Karakayali, 2009). The magnitude of the disparity between self and others increases with social distance. Researchers attribute this phenomenon to a person's uncertainty toward unfamiliar people (Paek, Pan, Sun, Abisaid, & Houden, 2005). Prior research found that, when others are perceived as distant, the self-others perceptual gap was large (Andsager & White, 2009; Chen et al., 2015; Duck & Mullin, 1995; Gibbon & Durkin, 1995; Gunther, 1991). In contrast, when comparing oneself to close friends, TPE perceptions diminished significantly (Brosius & Engel, 1996; White, 1997).

Researchers have documented that the magnitude of TPE perceptions is a function of the differing backgrounds of the reference group. Individuals have more favorable and optimistic perceptions about in-group members who share similar backgrounds (Eveland, Nathanson, Detenber, & McLeod, 1999). When it comes to out-group members with dissimilar backgrounds, however, individuals develop stereotypical and less favorable perceptions (Hinkle & Schopler, 1986). In one study, for example, researchers found that when respondents were randomly assigned to different groups, respondents evaluated in-group members more favorably than out-group members even though these groups were constructed solely for the experiment (Sherif, 1958).In studies of college students, respondents have been found to be more concerned about the effect of pornographic media content on unfamiliar students in the same school than the students they know well (Chen et al., 2015; Gunther, 1991). College students have

similarly been found to believe that behaviors of in-group members are similar to oneself and predictable. Out-group members, in contrast, are believed to lack the ability to resist the negative influences of pornography. Similarly, another study found that the more educated perceive greater media influence on the less educated; and older adults perceive greater media influence on the young (Paul et al., 2000). As an outcome of self-serving bias, individuals underestimate out-group members and engage in downward comparison, meaning they consider these others as less proficient (Wills, 1981). Such biased comparisons result in negative judgments (David & Johnson, 1998; Paek et al., 2005).

Not all social distance studies have yielded positive results. For instance, in a study of political advertising, respondents reported similar estimates of media effects on same-state residents and other-state residents (Cohen & Davis, 1991). The authors attributed this finding to a general distaste for political advertising and doubt about its effectiveness across groups.

A significant limitation of existing research on social distance is social distance is that no prior research has empirically measured social distance. Existing research assumes the social distance between self and others through predefined groups (Chen et al., 2015; Gunther, 1991; Paek et al., 2005). For instance, researchers assume that college respondents consider other students in the same school to be closer than residents living in another state (McLeod et al., 1997). However, college students from another state may perceive residents from their home state as closer than the students at the focal university. Given this limitation, the current study uses Bogardus social distance scale to

define the social distance of others. Bogardus social distance scale was developed in 1933 (Bogardus, 1933) and was improved by subsequent studies (Parrillo & Donoghue, 2005). This scale was originally designed to measure the perceived acceptance of ethnic groups in U.S society. The scale reflects varying closeness between self and others according to the degree of social connections. The social distance scale contains seven categories: 1) close relatives by marriage, 2) close personal friends, 3) neighbors on the same street, 4) co-workers in the same occupation, 5) citizens in my country, 6) only visitors in my country, and 7) people outside my country.

The systematic categorization of others in this scale is of great value for the current study. In the current study, "others" are divided into the aforementioned seven categories as defined by the social distance scale. This permits a rigorous and novel empirical assessment of social distance in TPE studies.

2.4.2 Perceived Severity and Vulnerability of Internet Privacy Risks

In addition to social distance, the desirability of media content is another predictor of TPE perceptions. Desirability reflects the extent that media messages are favored by viewers (Jensen & Hurley, 2005). The magnitude of TPE perceptions is influenced by the desirability of media messages (Paul et al., 2000). In general, people tend to overestimate the effects of desirable media messages (i.e., health promotion exercises) on themselves and underestimate the undesirable media messages (i.e., pornography). Prior studies have found that desirable media messages decrease or even reverse TPE perceptions (Gunther & Mundy, 1993).

Ego-defense and ego-enhancement mechanisms provide explanations for why desirable messages tend to reduce TPE perceptions (Duck & Mullin, 1995; Gunther & Mundy, 1993). Ego-defense entails that, to deal with problems and conflicts, people use defensive mechanisms to resist negative feelings and maintain positive perceptions about the self (Freud, 1992). The ego-defense operates at the unconscious level at times when people feel threatened, overwhelmed, and depressed. For instance, in viewing negative media messages, individuals attribute negative media impact to others, thus reducing anxiety about negative media impact. The ego-defensive mechanism increases TPE perceptions of negative media messages. In contrast, when viewing desirable media messages (e.g., anti-smoking advertisements), individuals think that they are more likely to adopt positive behaviors (Lewis, Watson, & Tay, 2007). TPE diminishes in the context of pro-social media messages.

Ego-enhancement refers to a psychological mechanism that makes people feel good about themselves and act in ways that enhance or maintain self-esteem (Boyle, McLeod, & Rojas, 2008). When a media message is perceived as negative, people believe that they are less influenced by such message, which increases TPE perceptions (Boyle et al., 2008). For example, people who play violent video often believe that they can resist the negative influence of gaming violence but believe that violent games can increase the verbal and physical aggressiveness of other players (Boyle et al., 2008). The ego-enhancement motivation becomes stronger when a person experiences threat, failure, or disappointing events (Beauregard & Dunning, 1998). To reduce anxiety, individuals often engage in downward comparison, comparing themselves to those who

are worse off than themselves (Yip & Kelly, 2013). The ego-enhancement mechanism contributes to enhancing one's psychological well-being.

Past research provides support for the relationship between the desirability of media content and TPE perceptions of media influence (Eveland & McLeod, 1999). In the study of media violence, researchers found that people perceive a greater impact of media violence on others, expecting that media violence increases others' aggressive behaviors (Huesmann & Taylor, 2006). Research on anti-social media messages found strong support of TPE in contexts of violent lyrics (Eveland & McLeod, 1999), libelous news stories (Cohen, Mutz, Price, & Gunther, 1988), pornography (Chen et al., 2015; Gunther, 1995; Lo & Wei, 2005; Wu & Koo, 2001), cigarette advertising (Henriksen & Flora, 1999), and media violence (Gunther & Hwa, 1996; Henriksen & Flora, 1999). In contrast, studies found that pro-social media content decreases or even reverses TPE perceptions (Golan & Day, 2008; Paul et al., 2000). For instance, researchers found that, after watching an anti-smoking advertisement, children believed they would be less likely to smoke in the future than others (Henriksen & Flora, 1999).

The major limitation of previous research is that researchers simply assume the desirability of media messages instead of measuring this empirically (Eveland & McLeod, 1999). Media users can hold different perceptions on the same media messages. For example, active news readers consider news from prestigious news agencies as credible, while non-active readers cannot tell the credibility of a news agency (Eveland & McLeod, 1999; Lord, Ross, & Lepper, 1979). Researchers have

found that if media messages are inconsistent with personal opinion, people develop

hostile media judgments (Giner-Sorolla & Chaiken, 1994).

Given the limitation of prior research, the current study provides empirical

measurements of the perceived undesirability of an online privacy invasion. Prior TPE

studies have used perceived severity (Li, 2008) and vulnerability (Cho et al., 2010) to

represent people's perceived online privacy threat. Severity reflects people's judgments

on how serious the problem of Internet privacy is (LaRose, Lai, Lange, Love, & Wu,

2005), whereas vulnerability reflects the perceived likelihood the threat will take effect

in the future (D. Lee, Larose, & Rifon, 2008). Internet users' perceived severity and

perceived vulnerability reflect their judgment about the outcomes of privacy invasions as

well as the possibility of being attacked by cyber criminals. The current study

empirically tests the undesirability of Internet privacy invasion, using perceived severity

and vulnerability of online privacy risks, and explores the effects on TPE perceptions.

2.4.3 Perceived Internet Privacy Knowledge

Some personal features (or characteristics) are also expected to function

regarding TPE. One such feature is perceived knowledge, which reflects individual

familiarity with an issue (Krosnick & Milburn, 1990; Nunes et al., 2011). Individuals

acquire knowledge from media, education, and personal experiences. People who are

highly involved in a topic tend to think that others are more influenced by media

messages because of their limited knowledge (Price & Tewksbury, 1996). For instance,

during presidential campaigns, people who believed they are more knowledgeable about

political news think that others lack knowledge and, subsequently, are more likely to be

22

influenced by news coverage. In this case, perceived knowledge increases TPE perceptions of media effects (Price & Tewksbury, 1996). In a news coverage of the Lebanon War, researchers found that pro-Arab and pro-Israel viewers believed they were more knowledgeable on Israel-Palestine conflicts than other viewers. These viewers believed news coverage had little effect on them personally but that it persuaded the neutral viewers to support the opposing side.

Researchers have noted that perceived knowledge—and not the actual knowledge—predicts TPE perceptions (Salwen & Dupagne, 2001). Lasorsa (1989), for example, had respondents watch the television show *Amerika*, which portrayed the life of Americans after a takeover by the Soviet Union. Lasorsa tested respondents' actual versus perceived political knowledge of the U.S-Soviet Union conflict. The results revealed that people with high perceived knowledge reported sizable TPE perceptions, whereas their actual knowledge had no such effect. Overall, people who perceive themselves to be knowledgeable about the U.S-Soviet Union conflict also believe that the general public lacks knowledge and could be easily fooled by the show. Researchers have also found that the higher their perceived knowledge, the more likely people would be to perceive themselves as superior to others (Salwen & Driscoll, 1997). A person with high perceived knowledge, thus, believes they also have the capacity to resist the media effects than others.

Not all research has provided support for the aforementioned theorizing. Some studies suggest that increased knowledge and expertise—both real and perceived—can lead to greater estimates of media effects on others than on one's self. In one such study,

Tiedge and colleagues (1991) found that both self-supporting judgments (i.e., actual knowledge) and self-enhancing judgments (i.e., perceived knowledge) lead to biased assessments of media effects. In a subsequent study, researchers documented that perceived knowledge increase TPE perceptions of political news (Price & Tewksbury, 1996). Other studies, however, have found no support for the effects of perceived knowledge. For instance, in the contexts of Internet pornography (Chen et al., 2015) and violent rap music (McLeod et al., 1997), the effects of perceived knowledge were not significant.

The current study expects that perceived knowledge of Internet privacy increases TPE perceptions. In line with one prior study (Li, 2008), the current study measures respondents' perceived knowledge in terms of the understandings of virus attacks, hacker attacks, identification theft, credit card theft, privacy invasion, and online insults.

2.4.4 Negative Online Privacy Experiences

Another focal antecedent of this study is negative online privacy experiences. Negative online privacy experiences refer to the occurrence of identity theft, financial loss, and relational conflicts in the past (Chen et al., 2016a; Debatin et al., 2009). Consequences of online privacy invasion include financial loss and relational conflicts. The misuse of personal financial accounts by others can lead to monetary loss, whereas unauthorized access to a person's social media account can cause relational conflicts with online contacts. Privacy invasions increase with the use of social networking services (SNSs), on which people disclose private information (Ellison, Steinfield, & Lampe, 2007). Another factor leading to the increase of privacy loss is online shopping.

Hackers can have access to users' bank account information through the function of malicious software (Moore, Clayton, & Anderson, 2009; Thomas & Martin, 2006). According to the biased optimism theory, people often perceive that others are more likely to encounter negative experiences than self (Paul et al., 2000).

Internet users who have experienced privacy loss before tend to be highly aware of online privacy risks. Researchers noted that people form an understanding of the world via their estimation of prior experiences (Cho et al., 2010). People often use personal experiences to predict future decisions and behaviors. Prior negative experiences were found to decrease self-serving bias, leading people to think that they are no better than others (Helweg-Larsen & Shepperd, 2001). Similarly, in the context of the Internet, one's perceived Internet privacy risks increases with the negative online privacy experiences. For instance, in a study of Internet privacy, researchers found that the experiences of information stolen and unauthorized access to personal SNS accounts resulted in increased awareness of information disclosure (Chen et al., 2016a). People who personally experienced privacy loss tend to realize that online privacy risk is relevant to themselves (Petronio, 2002), which, in turn, leads to the intention to adopt protective measures (Cho et al., 2010). For Internet users who have experienced online privacy invasion, the enhanced understanding of one's online privacy risks can potentially decrease the TPE perceptions.

In line with previous studies (Chen et al., 2016a; Cho et al., 2010), the current study tests five types of privacy invasions: 1) online theft of financial assets, which results in monetary loss and other conflicts (Chen et al., 2016a); 2) reception of spam

emails, which entails soliciting information from unknown sources (Wainer, Dabbish, & Kraut, 2011); 3) unauthorized access to online personal accounts, such as SNS, which results in improper postings on personal accounts and relational conflicts with friends (Chen et al., 2016a); 4) experiencing of online harassment; and 5) reception of unwanted friend invitations (Kenneally & Claffy, 2010). The current study examines how these negative experiences influence TPE perceptions of Internet privacy risks.

2.4.5 Internet Use

As discussed before, media is an important source for people to acquire information. Media use can lead people to develop understandings of a particular issue. Active political news viewers tend to be knowledgeable about the backgrounds of campaign candidates (Brosius & Engel, 1996; Rucinski & Salmon, 1990). When the news coverage resonates with preexisting perceptions or provides new thoughts to viewers, viewers' expertise toward specialized topics increases (Salwen, 1998). Given that the accumulation of knowledge is a longitudinal process, frequent media viewers tend to think that other non-active viewers lack the ability to judge the media messages and tend to follow the media messages (Rucinski & Salmon, 1990). The biased perceptions of other media users can lead to the increase of TPE perceptions.

Support for the association between media uses and TPE perceptions was found in studies of traditional mass media, but not the Internet. Similar to traditional media, people use the Internet to follow up on news reports or watch streaming videos. The difference is that the Internet provides a tremendous amount of media information for users to choose. People use the features of the Internet for advanced information

searches (Flanagin et al., 2014; Kaye & Johnson, 2002), building and maintaining online social contacts (Ellison et al., 2007), online shopping (Pratt et al., 2010), and online gaming (Kuss, Louws, & Wiers, 2012). Users tend to be involved in frequent online information exchanges and develop Internet skills through daily use. For instance, active SNS users tend to be familiar with account setting and privacy settings. Social media users develop social skills online by maintaining existing contacts and establishing new contacts (Ellison et al., 2007). Even though online privacy risk is universal, experienced Internet users tend to understand the risky behaviors and adopt privacy protection strategies in advance. For example, one prior study found that the frequency and variety of Internet use increase TPE perceptions of Internet pornography (B. Lee & Tamborini, 2005). Researchers also found that active Internet users perceive greater benefits of the Internet use for themselves (Li, 2008). Active Internet users' positive perceptions of Internet can intensify beliefs that negative online encounters will not occur to themselves.

The current study operationally defines Internet use in terms of the following online activities: online information searches, online news consumption, online shopping, online gaming, online chatting, and the use of SNSs. Online information searches refer to the use of Internet to seek useful information of a specific topic (Singh, 2014). Online news consumption refers to Internet users' viewing of textual, audio, and video news reports on the Internet (O'Brien & Lebow, 2013). Compared with traditional media channels, the Internet provides a greater variety of news channels and allows viewers to interact with content producers. Online gaming refers to the use of online

gaming platforms, which allow gamers to build social networks and finish game assignments collectively (Ko et al., 2013). Online chatting refers to the use of instant messaging, audio chatting, and video chatting on the Internet (Wei, Wang, & Fass, 2014). Use of social media refers to the engagement of social networking services to build new contacts and maintain existing online contacts. The current study measures the frequency of these six types of Internet use. I hypothesize that that frequent Internet users will perceive greater TPE perceptions of Internet privacy risks than others.

2.5 Literature Gaps in TPE

Compared with other media contexts, there is limited TPE research focusing on Internet privacy. Debatin and colleagues (2009) examined how individuals perceive Internet risks specific to self and others. The findings suggested that Facebook users tended to ascribe the privacy risks to others. Even though users claimed to understand privacy risks, they still uploaded a tremendous amount of personal data online. This research also found that Facebook use was integrated into users' daily routines. This study used mixed research methods (quantitative and qualitative), providing an initial understanding of TPE perceptions of online privacy risks. In other research, Li (2009) documented TPE perceptions of Internet privacy risks and found that respondents believe they have more knowledge of Internet privacy than others. In addition, Internet user experiences can influence perceived vulnerability of online privacy risks. In a subsequent study, Cho and colleagues (2010) confirmed that people had strong optimistic biases about online privacy risks, believing that they are less vulnerable than others to such risks. Additionally, perceived controllability of online privacy was found

to increase optimistic bias, whereas prior negative online privacy experiences decreased optimistic bias.

One major limitation of the existing research is that the antecedents of TPE perceptions of online privacy risks have not been examined systematically. The effects of perceived knowledge, negative online privacy experiences, and Internet use are still uncertain. In broader TPE literature, very few studies have tested how perceived knowledge, prior experiences, and media use influence the magnitude of TPE perceptual gap. These three factors can have the following types of influence on TPE perceptions: 1) perceived knowledge can enhance self-serving bias that increases TPE perceptions (Lasorsa, 1989); 2) negative prior experiences can lead people to be aware that negative outcomes are relevant to oneself, which decrease TPE perceptions (Li, 2008); and 3) active media users tend to be familiar with potential negative media impact and are likely to attribute such negative media effects to others, which increases TPE perceptions. Issues related to these three antecedents represent gaps in the literature.

Another gap in the literature involves the current study's testing of two antecedents of TPE—social distance and desirability–in the context of Internet privacy. TPE research on the desirability of media content assumes social distance without directly measuring it (Price, Huang, & Tewksbury, 1997; Rojas et al., 1996; Rucinski & Salmen, 1990; Salwen, 1998). Similarly, we know that people can develop differing attitudes toward same media messages due to differences in personal backgrounds. The assumption of the desirability of media messages may not reflect how audience perceptions. For instance, people who have experienced financial loss online are likely

to perceive greater threats to their personal data online. In contrast, those who benefit

from Internet use tend to perceive Internet privacy risks as far removed from themselves.

Similarly, the research on social distance is based upon the assumption of predefined

groups (Eveland et al., 1999; Gunther, 1991). Such assumptions may not accurately

reflect perceived social distances between self and others. The majority of existing

research treats "others" as a general concept without a clear definition (Paul et al., 2000).

When respondents are asked to evaluate media effects on others, some respondents may

think of others as close friends, but other respondents may think of people living in

foreign country. Because perceptions of "others" may vary across individuals, this study

implements scaled measurements to test social distance.

The next gap in the literature entails the behavioral component of TPE. Prior

studies on the behavioral component primarily focus on people's support for media

censorship (Gunther & Hwa, 1996). In traditional media environments, the enforcement

of media censorship relies on the policy makers and media authorities. Average users do

not have the power to change the category of content under censorship. However, on the

Internet, the adoption of privacy protection measures becomes an individual behavior.

The behavioral component of TPE should be reexamined in the novel context of Internet

privacy.

A final gap in the literature is that prior studies primarily focused on the

antecedents of privacy protection intention with basis on fear based theories. PMT and

EPPM assume that people develop privacy protection intention through the function of

threat appraisal and coping appraisal (Rogers, 1975). However, the related studies did

not test people's differential perceptions of privacy risks. People may simply refuse to adopt protective measures because of the optimistic beliefs that they will not encounter privacy invasion. In such case, the threat appraisal and coping appraisal can be ineffective. The differential perceptions of Internet privacy risks between self and others should be examined using an alternative theoretical framework.

In response the literature gaps, the current study contributes to existing research on TPE in the context of Internet privacy. A classic theory originated from conventional media is revisited in the Internet-based media context. Specifically, the current study tests how social distance, desirability, perceived knowledge, prior negative Internet use experiences, and activities of Internet use influence the magnitude of TPE perceptions. In doing so, the current study extends the behavioral component of TPE into a novel context other than support for media censorship. Unlike prior studies primarily use the fear based theories to assess the antecedents of Internet privacy protection motivation, the current study test the privacy protection intention from the perspectives of TPE.

3. RESEARCH HYPOTHESES

The first hypothesis relates to the perceptual component of TPE. The perceptual component of TPE entails that people think media messages exert greater influence on others than on self (Davison, 1983). The current study will test TPE in the context of Internet privacy risks by asking the respondents how they estimate Internet privacy risks on self and others. It is expected that perceived risks on others are greater than on self.

H1: People perceive greater Internet privacy risks on others than on self.

The behavioral component of TPE holds that TPE perceptions lead to behavioral intentions to support the restriction of harmful media messages. Prior research mainly focuses on the censorship of negative media messages (Gunther & Storey, 2003; Perloff, 1999). The current study expands the behavioral component of TPE to the context of the Internet by testing the relationship between TPE perceptions of Internet privacy risks and the willingness to adopt protective measures. Notably, researchers found that the adoption rate of Internet protection practices is relatively low (Chen et al., 2016a). When TPE perceptions are high specific to Internet privacy risks, it is expected that people will overestimate Internet privacy risks on others and underestimate Internet privacy risks on self, which, in turn, will increase one's intention to recommend online privacy protection measures to others. Differently, when individuals perceive similar levels of Internet privacy risks between self and others, individuals are likely to be aware of privacy risks on self and are willing to take measures to enhance privacy protection. Therefore, it is

expected that TPE perceptions of Internet privacy risks are negatively associated with the willingness to adopt Internet privacy protection measures by oneself.

H2: TPE perceptions of Internet privacy risks positively predict the willingness to recommend the privacy protection measures to others.

H3: TPE perceptions of Internet privacy risks negatively predict the willingness to adopt online privacy protection measures by oneself.

In line with prior research (Chen et al., 2015; Gunther, 1991), the current study proposes that social distance positively predicts TPE perceptions of Internet privacy risks. The greater the social distance between self and reference groups, the greater TPE perceptions. In the current study, based upon the Bogardus social distance scale (1933), "others" are divided into seven categories: (1) close blood relatives and relatives by marriage, (2) close personal friends, (3) coworkers in the same organization, (4) people in the same occupation or the same educational level, (5) citizens and permanent residents in your country, (6) visitors in my country, and (7) people outside my country. Respondents were asked to estimate the perceived online privacy risks on each of the seven groups. The current study predicts that TPE perceptions of Internet privacy risks increase with social distance.

H4: Social distance positively predicts TPE perceptions of online privacy risks.

Prior studies noted that the desirability of media messages has even greater influence on TPE than social distance. Researchers found that individuals reported greater TPE perceptions of negative media messages than positive media messages (Paul et al., 2000). The limitation of existing studies is that the desirability of media messages

is assumed by the researchers instead of empirical tests (Eveland & McLeod, 1999). The current study examines the undesirability of online privacy invasion using two indicators: perceived severity and perceived vulnerability of Internet privacy invasion. Perceived severity and perceived vulnerability of Internet privacy invasion are expected to increase TPE perceptions.

> H5a: Perceived severity of Internet privacy invasions positively predicts TPE perceptions of online privacy risks.

> H5b: Perceived vulnerability of Internet privacy invasions positively predicts TPE perceptions of online privacy risks.

Perceived knowledge reflects people's confidence in their understanding of certain topics (Lasorsa, 1989; Salwen & Dupagne, 2001). Studies of conventional media have found that perceived knowledge—and not actual knowledge—leads to greater TPE perceptions (Lasorsa, 1989). In line with prior research, the current study measures perceived knowledge with perceived understanding of virus attacks, hacker attacks, identification theft, credit card theft, privacy invasion, and online insults (Li, 2008). People with high levels of perceived knowledge tend to overestimate one's control over online privacy, which is expected to increase the TPE perceptions.

> H6: Perceived Internet privacy knowledge positively predicts TPE perceptions of online privacy risks.

The current study entails five types of negative online privacy experiences, including online theft of financial assets, reception of spam emails, unauthorized access to personal accounts online, online harassment, and reception of unwanted friend

invitations. According to prior studies, negative online privacy experiences diminish optimistic bias and lead people to be aware that they are at risk of personal privacy invasion (Cho et al., 2010). People who experience online privacy losses are likely to have a better understanding of the outcomes of privacy invasion and perceive higher Internet privacy risks on self (Cho et al., 2010). The negative online privacy experiences, thus, are expected to reduce TPE perceptions.

H7: Negative online privacy experiences negatively predict TPE perceptions of Internet privacy risks.

The current study also addresses the association between Internet use and TPE perceptions. A prior study found that active Internet users reported higher Internet efficacy than inactive users. Frequent Internet users tend to be familiar with potential Internet privacy risks and experienced in dealing with online conflicts (B. Lee & Tamborini, 2005). Active Internet users tend to estimate lesser effects of Internet privacy concerns on self than on other less experienced users. In line with prior research (Chen et al., 2016a; Li, 2008), the current study measures the frequency of six types of Internet use, including online information searches, online news consumption, online shopping, online gaming, online chatting, and the use of SNSs. It is expected that the Internet use is positively associated with TPE perceptions.

H8: Internet use positively predicts TPE perceptions of Internet privacy risks.

Theoretical Framework of the current study is as follows (See Figure 1).

Figure 1. Theoretical Framework of the Current Study
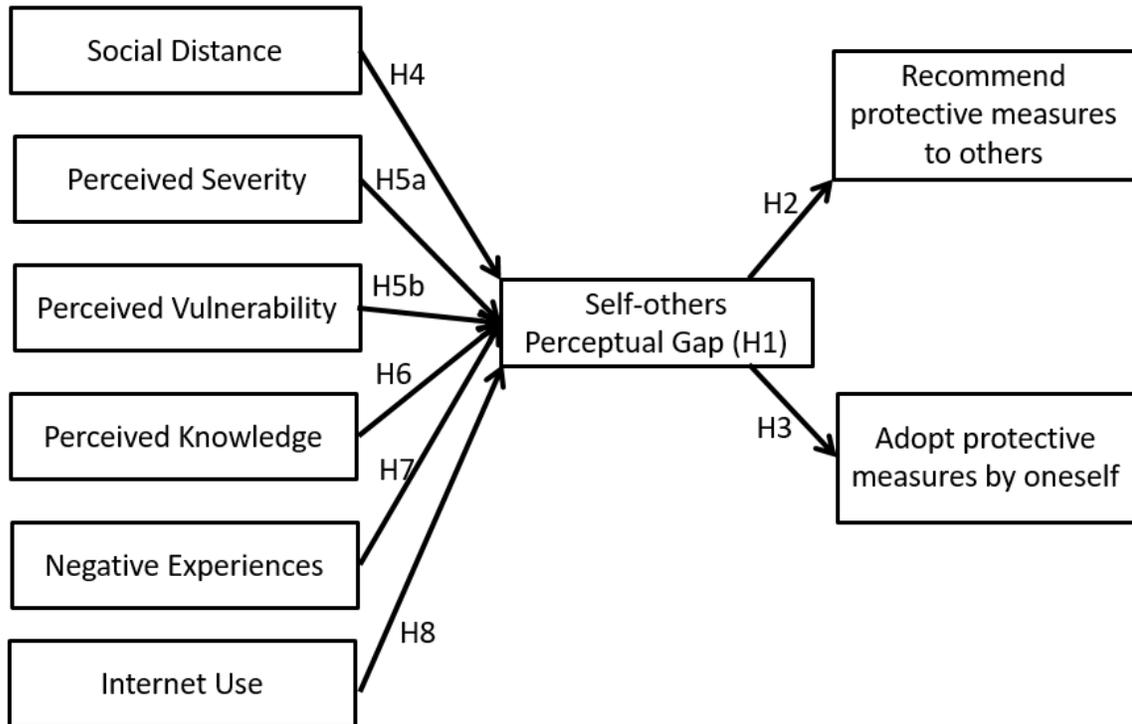
4. RESEARCH METHODOLOGY

4.1 Sampling

4.1.1 Sampling Process

The survey data was collected through Amazon Mechanical Turk. Amazon Mturk (www.MTurk.com) is a novel website that contains a participant compensation system and large numbers of subscribers, which allows researchers to design survey research, recruit participants, and collect numeric data (Buhrmester, Kwang, & Gosling, 2011). Survey designers can deposit money in a Mturk account and set a compensation amount for each survey respondent. When respondents complete the survey, they will receive an automatic payment from the survey designers, of which Amazon charges a 10% commission fee.

The current study used a sample of the U.S Mturk respondents in November 2016. The survey link was posted on Amazon Mturk and Mturk self-selected respondents to participate the survey. A respondent who completed the questionnaire received $3. Such compensation is common in survey research as a means to enhance response rates (Largent, Grady, Miller, & Wertheimer, 2012). Survey questions included all independent variables, dependent variables, and control variables.

The sample size of the current study is 613. According to prior statistical research, if continuous variables play primary roles in data analysis and the alpha level is set a priori at .05, level of acceptable error at 3%, and standard deviation of scale is

1.167 (7/6), the minimum recommended sample size is 118 using Cochran's sample size

formula (Kotrlik & Higgins, 2001). The formula for the size calculation is as follows:

$$n_0 = \frac{t^2 + s^2}{d^2} = \frac{1.96^2 + 1.167^2}{(7 * .03)^2} = 118$$

A sample size greater than 118 will provide sufficient statistical power for the current

study. In survey studies, researchers often increase the minimum sample size by 40% to

50% as compensation for the incomplete submissions (Fink, 1995; Salkind, 1997). In the

current study, the size sample of 613 should provide satisfactory statistical power.

4.1.2 Descriptive Statistics of Respondents

The current study measured a set of socio-demographic variables as control

variables. Education was measured with a categorical scale (1=some grade school,

2=some high school, 3=high school graduate, 4=technical or vocational school, 5=some

college,

6=college graduate, and 7=graduate/professional degree). Annual household income was

measured with a 7-item scale (1=less than $20,000, 2=$20,000 to $40,000, 3=$40,001 to

$60,000, 4=$60,001 to $80,000, 5=$80,001 to $100,000, 6=$100,001 to $120,000,

7=more than $120,000). Age was measured with an open-ended question. Respondents'

ethnic backgrounds were measured with two questions: the first question asked

respondents to identify if they are Hispanic; the second question asked respondents to

identify their specific ethnicity (1=White, 2=African American, 3=Asian, 4=Other

Race). Employment status was measured with a multiple-choice item (1=not employed,

2=part-time employed, 3=full-time employed).

According to the self-reported survey, most respondents identified themselves as non-Hispanic White (74.71%), followed by Hispanic (7.50%), Asian (7.50%), African American (7.34%), and Other Race (6.04%). The average age of respondents was 35.69. In terms of gender, 54.16% of respondents were male. The household income of respondents is as follows: 1) "Less than $20,000" (15.99%); 2) "$20,000 to $40,000" (32.30%); 3) "$40,001 to $60,000" (22.02%); 4) "$60,001 to $80,000" (14.03%); 5) "$80,001 to $100,000" (7.50%); 6) "More than $100,001" (8.16%). The respondents' educational backgrounds are as follows: 1) "Some grade school" (.16%); 2) "Some high school" (.33%); 3) "High school graduate" (10.77%); 4) "Technical or vocational school" (7.67%); 5) "Some college" (31.16%); 6) "College graduate" (40.95%); 7) "Graduate/Professional degree" (8.97%). The respondents' employment status is as follows: 1) "Not employed" (18.11%); 2) "Part-time employed" (18.92%); 3) "Full-time employed" (62.97%). According to the U.S Census Bureau, in 2015, the median household income was $56,516, 49.6% of the overall population was male, median age was 37.7, and 86.7% of the population has high school degree or higher (U.S Census Bureau, 2017). Internet use was found to be positively associated with being male, younger, and more educated (Pearce & Rice, 2013). Consistent with prior studies, the respondents of the current study are younger and more educated than the average population. More male respondents participated in the current study. The demographic information of the respondents is representative of the average Internet users in the U.S.

Table 1. Descriptive Statistics of Control Variables

Variables	Mean	SD	Min	Max
Age	35.69	10.97	19	72
Sex (Male)[a]	54.16%			
Ethnicity				
White	74.71%			
Hispanic	7.50%			
Asian	7.50%			
African American	7.34%			
Other Race	6.04%			
Household Income	2.89	1.46	1	6
(1) Less than $20,000	15.99%			
(2) $20,000 to $40,000	32.30%			
(3) $40,001 to $60,000	22.02%			
(4) $60,001 to $80,000	14.03%			
(5) $80,001 to $100,000	7.50%			
(6) More than $100,001	8.16%			
Education	5.28	1.12	1	7
(1) Some grade school	.16%			
(2) Some high school	.33%			
(3) High school graduate	10.77%			
(4) Technical or vocational school	7.67%			
(5) Some college	31.16%			
(6) College graduate	40.95%			
(7) Graduate/Professional degree	8.97%			
Employment Status	2.45	.78	1	3
(1) Not employed	18.11%			
(2) Part time employed	18.92%			
(3) Full time employed	62.97%			

a. Represents the frequency of dichotomous variables

4.1.3 Effects of demographic variables on TPE

The effects of control variables on the TPE perceptions were tested using ordinal regression. Regression is a method to estimate the linear relationships between unknown parameters and the goal of regression is to minimize the difference between observed data and the proposed linear regression line (Dhillon, Foster, Kakade, & Ungar, 2013). Ordinal regression is a type of regression model with ordinal dependent variables.

The results of the ordinal regression model suggested that male respondents perceived higher TPE perceptions than female respondents (See Table 2). Prior studies of conventional media found that males tend to perceive greater TPE perceptions of media effects because males tend to be more confident in their knowledge of media uses (Cynthia Hoffner et al., 2001; McLeod, Detenber, & Eveland, 2001). The finding of current study suggested that similar to conventional media, male tend to be confident in control over personal data online and perceive others to be at greater risk of invasions online. Prior study has detected that age is a positive predictor of TPE perceptions (Antonopoulos, Veglis, Gardikiotis, Kotsakis, & Kalliris, 2015). In contrast, such effect was not significant in the current studies.

Table 2. Ordinal Regression Predicting TPE Perceptions with Control Variables

	TPE perceptions
Age	.00
Gender (Male)	.33*
Household Income	.04
Education	.01
Hispanic	.20
African American	.30
Asian	.38
Other Race	-.22
Employment Status	.04
Pseudo R^2	.01

*p<.05; **p<.01; ***p<.001

Next, the current study tested the variations of TPE perceptions among different ethnicities (See Table 3). The differences in TPE perceptions were not significant between different ethnicities. Asian respondents reported highest TPE perceptions (M=.83, SD=1.23), followed by non-Hispanic White (M=.54, SD=1.05), African

American (M=.53, SD=.84), Hispanic (M=.39, SD=.71), and other race (M=.39, SD=.80). According to PEW research center, by the end of 2016, 88% of White and Hispanic and 85% of African American population are Internet users (PEW Research Center, 2017). The current study suggested that in addition to the similar Internet adoption rate, respondents of different ethnicities possess similar TPE perceptions of Internet privacy risks.

Table 3. Descriptive Statistics of TPE Perceptions by Ethnicity

	Mean (SD)	Min	Max
Non-Hispanic White	.54(1.05)	-6	6
Hispanic	.39(.71)	-6	6
African American	.53(.84)	-6	6
Asian	.83(1.23)	-6	6
Other Race	.39(.80)	-6	6

4.1.4 Limitations of Mturk Sample

Scholars across the social sciences have increasingly recognized that—despite their limitations—online surveys can be useful tools for understanding attitudes and behaviors. The advantages of the online survey include efficiency in terms of costs and time as well as the accessibility to existing respondents of survey platforms (Wright, 2005). However, online surveys also present certain disadvantages. First, Mturk respondents are individuals who have previously registered to participate in survey panels. Non-Mturk subscribers are excluded, making it difficult to generalize to the general population (Goodman, Cryder, & Cheema, 2013). Second, the validity and accuracy of data collected are questionable. Respondents may answer the questions randomly and rush through the survey items (Johnson & Borden, 2012). For those who

are interested in the monetary reward, they may register multiple accounts to participate

a single survey. Also, prior studies found that, because they receive monetary

compensation, some respondents provide what they perceive as desirable responses to

the researchers (Reese et al., 2013).

For these reasons, in the current study respondents who completed the survey

less than 5 minutes were dropped from the analysis. Also, respondents were required to

complete all of the questions before submitting their final responses. If there were any

missing items, respondents could not receive the monetary rewards for survey

participation. To avoid robotic responses, at the end of each survey respondents need to

fill in a set of randomly generated confirmation codes. Despite the limitations, the Mturk

survey provides a reasonable and costs effective method for understanding TPE within

in an online context. First, as noted above, the sample is reasonably representative of the

general online population. Second, as a study of online behaviors, the sample provides

respondents who already online. Had this been a traditional telephone survey, we would

have a need to screen for internet users before conducting the interview, adding greatly

to the costs of collecting the data.

4.2 Measurements

This section provides a summary of the measurement of independent and

dependent variables. The descriptive statistics are presented in Table 4. Specific question

wordings are provided in the Appendix.

Table 4. Descriptive Statistics of Endogenous Variables

Variables	Mean	SD	Max	Min
PERCEPTUAL COMPONENT OF TPE				
Perceived Internet privacy risks on self	5.03	1.40	1	7
Perceived Internet privacy risks on general others	5.59	1.15	1	7
BEHAVIORAL COMPONENT OF TPE				
Willingness to recommend the use of privacy protection measures to others	5.09	1.37	2	7
Willingness to adopt privacy protection measures by Yourself	5.00	1.47	1	8
ANTECEDENTS OF TPE				
Social Distance (Perceived Internet privacy risks on 7 categories of others)				
(1) Close relatives	5.13	1.37	1	7
(2) Close friends	5.18	1.38	1	7
(3) Colleagues in the same organization	5.21	1.37	1	7
(4) People in the same occupation or the same educational level	5.28	1.34	1	7
(5) Citizens or permanent residents in U.S.	5.62	1.28	1	7
(6) Visitors in U.S.	5.43	1.25	1	7
(7) People outside U.S.	5.70	1.19	1	7
Perceived severity of Internet privacy invasion	6.13	.93	1	7
Perceived vulnerability of Internet privacy invasion	6.29	.86	2	7
Perceived Internet privacy knowledge	5.08	1.28	1	7
Negative online privacy experiences	3.22	1.78	0	9
Internet use				
(1) Search information online	6.01	1.11	1	7
(2) News consumption	5.62	1.28	1	7
(3) Online shopping	5.03	1.18	1	7
(4) Online gaming	4.16	1.75	1	7
(5) Online chatting	3.82	1.85	1	7
(6) Social media	5.10	1.64	1	7

4.2.1 Perceived Internet Privacy Risks on Self and Others

Adopted from prior measurements on TPE (Gunther & Hwa, 1996; Price &

Tewksbury, 1996), perceived Internet privacy risks were measured with two items.

Perceived Internet privacy risks on self was measured with "How much do you think your Internet privacy is at risk?" Responses ranged from 1 (no risk at all) to 7 (great risk). The measurement of Internet privacy risks on others was as follows: "How much do you think other people's Internet privacy is at risk?" The responses were on a 7-item scale from 1 (no risk at all) to 7 (at great risk). In such measurement, "others" refers to a general others. Respondents reported higher perceived Internet privacy risks on others (M=5.59, SD=1.15) than on themselves (M=5.03, SD=1.40).

4.2.2 Behavioral Component of TPE

Two survey items were used to measure behavioral component of TPE: 1) the willingness to recommend privacy protection measures to others, 2) the willingness to adopt privacy protection measures for oneself (See Appendix A for specific item wording). Responses were measured on a 7-item scale from 1 (not at all likely) to 7 (highly likely). More than of half of the respondents (63.62%) claimed that they were somewhat willing to recommend privacy protection measures to others (M=5.09, SD=1.37). Similarly, 65.25% of respondents reported the willingness to adopt privacy protection measures themselves (M=5.00, SD=1.47).

4.2.3 Social Distance

Based upon the Bogardus social distance scale , the current study divided "others" into the following seven categories: 1) close blood relatives or relatives by marriage, 2) close personal friends, 3) colleagues in the same organization, 4) people in the same occupation or the same educational level, 5) citizens and permanent residents in your country, 6) visitors in the U.S, 7) people outside the U.S. A lower score

represents closer social connection. Respondents were asked to rate the perceived

Internet privacy risks on each of the seven categories of "others". The responses were

coded on a 7-item scale from 1 (no risk at all) to 7 (at great risk). The results are as

follows (See Table 5). In general, perceived risks on others increased with the social

distance with respondents believing more distant others are at greater risks than close

relatives and friends.

Table 5. Descriptive Statistics of Perceived Internet Privacy Risks on Others

Social Distance Categories	Mean	SD	Max	Min
(1) Close relatives	5.13	1.37	1	7
(2) Close friends	5.18	1.38	1	7
(3) Colleagues in the same organization	5.21	1.37	1	7
(4) People in the same occupation or the same	5.28	1.34	1	7
educational level				
(5) Citizens or permanent residents in U.S.	5.62	1.28	1	7
(6) Visitors in U.S.	5.43	1.25	1	7
(7) People outside U.S.	5.70	1.19	1	7

4.2.4 Perceived Severity and Vulnerability of Internet Privacy Risks

Perceived severity and perceived vulnerability were used as proxies for the

undesirability of Internet privacy invasions. A higher score on these items represents the

higher undesirability of Internet privacy risks. The perceived severity measure was

adapted from three previous studies (Crossler, 2010; LaRose & Rifon, 2007; Mohamed

& Ahmad, 2012). The four items included are listed as follows:

- *I believe that losing information privacy through Internet would be a serious problem for me.*

- *Having my online identity stolen through Internet would be a serious problem*

- *Losing photo privacy online would be a serious problem.*

- *Unauthorized access into my personal account, such as social networking sites,*
  personal financial account, would be a serious problem to me.

Responses were coded on a 7-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree). A composite variable was computed by averaging the four items. The reliability of the scale was satisfactory (α=.83). The majority of respondents agreed that cyber-attacks impose a great risk to Internet users' personal data security (M=6.13, SD=.93).

The measurement of perceived vulnerability of Internet privacy invasion was adapted from one prior study (Dinev & Hart, 2004). The related questions included the following:

- *Internet users could be subjected to a malicious information security*
  problems (e.g., virus, privacy, identity theft, hacking and etc.) online
- *Internet users' personal information online could be misused*
- *Internet users' personal information online could be made available to*
  unknown individuals or companies without the acknowledgment
- *Personal information online could be made available to government*
  agencies
- *Users personal information online could be inappropriately used.*

Responses were on a 7-point Likert scale from 1 (strongly disagree) to 7 (strongly agree). The items were averaged to compute a composite variable. The reliability of this measurement was good (α=.90). The results suggested that respondents

believed that the majority of Internet users are vulnerable to potential privacy invasions (M=6.29, SD=.86).

4.2.5 Perceived Internet Privacy Knowledge

Adapted from prior research (Li, 2008), six items were used to measure perceived Internet privacy knowledge. Instead of testing actual knowledge, the current study measured how confident respondents are about Internet privacy risks. The seven questions included perceptions related to knowledge about virus attacks, hacker attacks, identification theft, credit card theft, privacy invasion, and online insult. The questions asked respondents to assess how knowledgeable they were about each of this Internet privacy risks. The responses were coded on a 7-point Likert scale from 1 (do not know anything) to 7 (know very much). Descriptive statistics for these measures are listed in Table 6.

Table 6. Descriptive Statistics of Perceived Internet Privacy Knowledge

Perceived Knowledge Categories	Mean	SD	Max	Min
(1) Virus attack	4.92	1.44	1	7
(2) hacker attack	4.81	1.50	1	7
(3) Identification theft	5.14	1.47	1	7
(4) Credit card theft	5.19	1.51	1	7
(5) General online privacy invasion	5.07	1.45	1	7
(6) Cyber harassment	5.33	1.48	1	7

The six items were averaged to compute a composite variable of perceived knowledge. The reliability of the scale was satisfactory (α=.93). The average value of perceived knowledge was 5.08 out of 7, indicating that respondents believed that they have developed basic understandings of Internet privacy risks.

4.2.6 Negative Online Privacy Experiences

Adapted from previous studies, the current study used ten items to measure the online negative privacy experiences (Chen et al., 2016a; Cho et al., 2010). Items include having financial accounts stolen, receiving solicitations through emails and social media, experiencing unauthorized access to personal online accounts, experiencing online harassment, and receiving unwanted friend invitations (Kenneally & Claffy, 2010). Respondents were asked to recall each type of prior negative experience (Yes=1, No=0). The items were added to create an index (M=3.22, SD=1.78, KR-20=.67). More than ninety percent of respondents reported at least one type of privacy loss on the Internet, 45.19% of respondents reported the experiences of monetary loss online, 87.77% of respondents received unwanted advertisements online, 36.70% of respondents were harassed or bullied online, and 88.58% of respondents experienced the unauthorized access into social media accounts.

4.2.7 Internet Use

The current study measured six types of Internet use, including online information searches, news consumption, shopping, gaming, chatting, and social media use. Online information searches refer to the use of the Internet to look for answers and useful information. Online news consumption represents reading and viewing of online news in different platforms, such as web portals, news websites, social media, and blogs. Online shopping refers to product and service purchase behaviors online. Online gaming involves the playing of online games in the gaming community and via social media. Online chatting refers the use of Instant Messaging online to contact others. Social

media use refers to involvement in social technologies, such as Facebook, Twitter, Instagram, and Pinterest. The respondents were asked to report the frequency of each type of Internet use, ranging from 1 (never) to 7 (very often). Descriptive statistics are provided in Table 7.

Table 7. Descriptive Statistics of Internet Use

Variables	Mean	SD	Min	Max
(1) Search information online	6.01	1.11	1	7
(2) News consumption	5.62	1.28	1	7
(3) Online shopping	5.03	1.18	1	7
(4) Online gaming	4.16	1.75	1	7
(5) Online chatting	3.82	1.85	1	7
(6) Social media	5.10	1.64	1	7

4.3 Statistical Procedure

Hypothesis 1 proposes that the perceived Internet privacy risks is greater on others than on self. The current study compared the perceived Internet privacy risks on self and general others. The seven categories of "others" were also tested using two sample t-test. The t-test formula is as follows:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\dfrac{S_1^2}{n_1} + \dfrac{S_2^2}{n_2}}}$$

In the formula, $\overline{X_1}$ and $\overline{X_2}$ represent the mean values of perceived Internet risks on self and others. S1 and S2 represent the standard deviations of the perceived Internet privacy risks on self and others, whereas n represents the sample sizes. The significance level was determined through the t-test table.

Hypothesis 2 and Hypothesis 3 test the effects of TPE perceptions on behavioral intentions of privacy protection. Consistent with prior studies, the TPE perception was

computed by perceived Internet privacy risks on general others subtracting the perceived Internet privacy risks on self(Chen et al., 2015; Gunther & Hwa, 1996). Because the dependent variables—TPE perceptions—is an ordinal variable, the current study used ordinal regression to test the effects of TPE antecedents. In the current study, the ordinal regression formula for H2 and H3 are as follow:

DV (behavioral responses) = IV (self-others perceptual gap) + Control variables+ Intercept

Hypothesis 4 contends that the self-others TPE perceptual gap on Internet privacy risks increases with social distance. To explore the effect of social distance on the TPE perceptual gap, the current study asked the respondent to rate the perceived Internet privacy on each of the seven "others" category. Then, seven TPE perceptions were computed using perceived risks on others subtracting perceived effects on self. Social distance was coded from 1-7 with higher values representing further social distance. Respondents were asked to report perceived Internet privacy risks on seven groups of others. Using repeated measures analysis of variance (ANOVA), the current study can identify if the perceived Internet privacy risks increase as a function of social distance. Repeated measures ANOVA is used test the differences in mean values under more than two conditions. This measure can be used to test the linear growth trend of dependent variables. The formula of repeated measures ANOVA is as follows. If F value is significant at .05 level, the assumption of linear growth is supported.

$$F = (SS_{Treatment}/df_{Treatment})/(SS_{Error}/df_{Error})^3$$

---

[3] SS stands for the sum of standard deviations; df refers to degree of freedom

Hypothesis 5 tests the effects of perceived severity and perceived vulnerability of Internet privacy risks on the self-others TPE perceptual gap of Internet privacy risks. Using ordinal regression, the formula for H5a and H5b is as follows:

DV (self-others perceptual gap) = IV_1(perceived severity) +IV_2(perceived vulnerability) + Control Variables + Intercept

Hypothesis 6 tests the effects of the perceived Internet privacy knowledge on the TPE perceptions of the Internet privacy risks. Using ordinal regression, the formula for H6 is as follows:

DV (self-others perceptual gap) = IV (Perceived knowledge) + Control Variables + Intercept

Hypothesis 7 tests the effects of negative online privacy experiences on the TPE perceptions of Internet privacy risks. Using ordinal regression, the formula for H7 is as follows:

DV (self-others perceptual gap) = IV (negative online privacy experiences) + Control Variables + Intercept

Hypothesis 8 tests the effects of Internet use on the TPE perceptions of the Internet privacy risks. The current study tests six types of Internet use, including online information searches, online news consumption, online shopping, online gaming, online chatting, and use of social media. Using ordinal regression, the formula for H8 is as follows:

DV (self-others perceptual gap) = IV₁ (information search) + IV₂ (online news

consumption) + IV₃ (online shopping) + IV₄ (online gaming) + IV₅ (online

chatting) + IV₆ (uses of social media) + Control Variables + Intercept

4.4 Data Cleaning

4.4.1 Missing Data

On Amazon Mturk, the respondents can only receive rewards after completing

the full survey. In the current study, missing values in the survey items were all below

1%. Consistent with prior studies, the missing values in continuous and ordinal variables

were replaced with the grand mean, while missing values in dichotomous variables were

recoded as zero (Eekhout, de Boer, Twisk, de Vet, & Heymans, 2012; Tabachnick &

Fidell, 2007). The recoded data were used for following statistical analysis.

4.4.2 Univariate Normality

In social science research, normal distribution is important in representing the

random variables whose distribution property is unknown (Little & Rubin, 1989). The

typical normal distribution is bell shaped (Hoeffding, 1948). The symmetry and

peakedness of the distribution are reflected by Skewness and Kurtosis (Azzalini &

Capitanio, 1999). The positive skewed distribution has values clustered to the left,

whereas the negative skewed distribution has values nested to the right (Mardia, 1970).

Positive Kurtosis represents the peak distribution, whereas the negative Kurtosis

represents the flat distribution (Mardia, 1970). In perfect normal distribution, both

Skewness and Kurtosis scores are zero. The farther score from zero, indicates the higher

level of non-normality Azzalini & Capitanio, 1999).

The current study tested the normality of each continuous endogenous variable using Shapiro-Wilk test, which is widely used to test the normality in statistics. Shapiro-Wilk can be used with a sample size smaller than 2000 and greater than 4 (Razali & Wah, 2011). For skewed variables, the current study used histogram to test the direction of skewness. The results of normality tests are as follows (See Table 8). Consistent with prior studies, the current study computed log transformations for variables that were skewed right and square transformations for variables that were skewed left (Manning & Mullahy, 2001; Osborne, 2005). Then, the transformed variables were used for regression analysis, whereas the untransformed variables were presented in the descriptive statistics and t-tests.

Table 8. Shapiro-Wilk Test of Endogenous Variables

Variables	z	Direction of Skewness
PERCEPTUAL COMPONENT OF TPE		
Perceived Internet privacy risks on self	6.92***	Left
Perceived Internet privacy risks on general others	7.78***	Left
BEHAVIORAL COMPONENT OF TPE		
Willingness to recommend the use of privacy protection measures to others	2.14*	Left
Willingness to adopt privacy protection measures by oneself	3.69***	Left
ANTECEDENTS OF TPE		
Social Distance (Perceived Internet privacy on 7 categories of others)		
(1) Close relatives	6.60***	Left
(2) Close friends	6.82***	Left
(3) Colleagues in the same organization	7.07***	Left
(4) People in the same occupation or the same educational level	6.94***	Left
(5) Citizens or permanent residents in U.S.	7.44***	Left
(6) Visitors in U.S.	6.89***	Left
(7) People outside U.S.	7.96***	Left

Table 8. Continued

Undesirability of Internet privacy invasion		
(1) Perceived severity of Internet privacy invasion	9.74***	Left
(2) Perceived vulnerability of Internet privacy Invasion	9.65***	Left
Perceived Internet privacy knowledge	7.31***	Left
Negative online privacy experiences	7.27***	Right
Internet use		
(1) Search information online	8.07***	Left
(2) News consumption	6.84***	Left
(3) Online shopping	3.78***	Left
(4) Online gaming	.94	NA
(5) Online chatting	2.99**	Right
(6) Social media	5.64***	Left

*p<.05; **p<.01; **p<.001

4.4.3 Multicollinearity

In statistics, multicollinearity refers to the case that two or more independent variables are highly correlated. In multiple regression models, multicollinearity does not influence the predictive power of the whole model but the individual predictive size is heavily impacted (Grewal, Cote, & Baumgartner, 2004). Researchers use Variance Inflation Factor (VIF) to measure the magnitude of multicollinearity in OLS models (Hair, Anderson, Tatham, & Black, 1995). The lower levels of VIF is desirable for social science research. Most commonly, the VIF value of 10 is considered as a maximum acceptable value (Kennedy, 1992; Neter, Wasserman, & Kutner, 1989). Other researchers held that VIF values should be lower than 5 (Rogerson, 2001) or even 4 (Pan & Jackson, 2008). In the current study, multicollinearity was tested in regression models (H5 & H8) with more than one independent variable, by running an ordinary least square regression (OLS) first and then use the VIF coefficients to identify the potential multicollinearity.

In test regression model testing H5, the VIFs of two independent variables are smaller than 3 (See Table 9), indicating that multicollinearity is at minimum level.

Table 9. OLS Predicting TPE Perceptions with Perceived Severity and Vulnerability

	b	VIF(Model2)
Independent Variables		
Perceived severity	-.02	2.24
Perceived vulnerability	.06	2.18
Control Variables		
Age	-.06	
Gender (Male)	.08	
Household Income	.03	
Education	-.02	
Hispanic	-.04	
African American	-.01	
Asian	.07	
Other Race	-.01	
Employment Status	-.04	
Total R^2	.02	

*p<.05; **p<.01; ***p<.001

Similarly, in the regression model testing H8, the VIFs of six independent variables are smaller than 3 (See Table 10), indicating that multicollinearity is not a concern.

Table 10. OLS Predicting TPE Perceptions with Internet Use

	b	VIF
Independent Variables		
Information Search	.13**	1.44
News Consumption	-.05	1.54
Online Shopping	-.04	1.30
Online Gaming	.08	1.28
Online Chatting	.03	1.32
Social Media Use	-.00	1.21
Control Variables		
Age	-.03	

Table 10. Continued

Gender (Male)	.07
Household Income	.03
Education	-.01
Hispanic	-.04
African American	-.02
Asian	.06
Other Race	.00
Employment Status	-.02
Total R^2	.04

*p<.05; **p<.01; ***p<.001

5. RESULTS

5.1 Perceptual Component of TPE

Hypothesis 1 posits that perceived Internet privacy risks are greater on others than on self. The current study used a two-sample t-test to examine TEP perceptual gap (t=13.33, p<.001) between self and general others. Next, I compared the perceived Internet privacy risks on self and each category of "others." The results indicated that perceived risks on each category of others were significantly higher than perceived risks on self. Hence, H1 received robust support in the current study (See Table 11).

Table 11. Two Sample t-tests between Perceived Internet Privacy Risks on Self and Others

	General Others	Relatives	Friends	Colleagues	Similar occupation or education	Citizens or permanent residents	Travelers in the U.S.	Foreigner
Mean (SD)	5.59(1.15)	5.13(.06)	5.18(1.25)	5.21(1.37)	5.28(1.35)	5.62(1.28)	5.43(1.25)	5.70(1.34)
t-value[a]	-13.33***	-1.96*	-2.84**	-3.49***	-5.09***	-10.44***	-7.08***	-12.34***

   a. Negative t value suggested that perceived Internet privacy risks on others is higher;
   b. *p<.05; **p<.01; ***p<.001

5.2 Behavioral Component of TPE

Hypothesis 2 and Hypothesis 3 address the association between TPE perception and behavioral intentions. H2 posits that TPE perceptions of Internet privacy positively predict willingness to recommend privacy protection measures to others. Variables were grouped into two blocks, primary independent variables, and control variables. Model 1 tested the effects of the independent variables holding the control variables constant,

whereas Model 2 excluded the control variables. The effect was positive and significant

(b=.35, p<.001) across models (See Table 12). Hence, H2 was supported.

Table 12. Ordinal Regression Predicting Willingness to Recommend Privacy
Protection Measures to Others

	Model 1	Model 2
Independent Variables		
TPE perceptions of Internet Privacy	.35***	.35***
Risks		
Control Variables		
Age	.00	
Gender (Male)	.18	
Household Income	.03	
Education	.03	
Hispanic	.42	
African American	.34	
Asian	.24	
Other Race	-.30	
Employment Status	.07	
Pseudo R^2	.05***	.05***

*p<.05; **p<.01; ***p<.001

According to H3, TPE perceptions of Internet privacy should be inversely related

to willingness to adopt privacy protection measures for oneself. Holding the control

variables constant, the effect was negative and significant (b=-.11, p<.001) (See Table

13). Hence, H3 was supported. In the current study, TPE perceptions were found to be

highly associated with the behavioral intentions to protect Internet privacy.

Table 13. Ordinal Regression Predicting Willingness to Adopt Privacy Protection
Measures by Oneself

	Model 1	Model2
Independent Variables		
TPE perception of Internet Privacy Risks	-.11***	-.11***
Control Variables		
Age	.00	

Table 13. Continued

Gender (Male)	-.09	
Household Income	.08	
Education	.01	
Hispanic	.34	
African American	-.02	
Asian	-.20	
Other Race	-.02	
Employment Status	-.19	
Pseudo R^2	.02***	.01***

*p<.05; **p<.01; ***p<.001

5.3 Antecedents of TPE

H4 posits that TPE perceptions should increase with social distance. The results

in Table 14 indicate that in general, TPE perceptions of Internet privacy risks increased

with social distance. The results of repeated measures ANOVA supported the

assumption that TPE perceptions increase with social distance (F=(1, 5.243), p<.001).

Hence, H4 was supported.

Table 14. Descriptive Statistics of TPE Perceptions of Internet Privacy Risks

Social Distance Categories	Mean	SD	Max	Min
(1) Close relatives	.09	1.37	-6	5
(2) Close friends	.14	1.38	-6	6
(3) Colleagues in the same organization	.17	1.37	-6	5
(4) People in the same occupation or the same educational level	.25	1.34	-6	6
(5) Citizens or permanent residents in U.S.	.59	1.28	-6	6
(6) Visitors in U.S.	.40	1.25	-6	6
(7) People outside U.S.	.67	1.19	-6	6

Hypothesis 5a and 5b postulate that perceived severity and vulnerability are

positively associated with TPE perceptions of Internet privacy risks. As can be seen in

Table 15, the effects of perceived severity (b=-.02) and vulnerability (b=.02) were not

significant (See Table 15). Hence, H5a and H5b were rejected.

Table 15. Ordinal Regression Predicting TPE Perceptions with Perceived Severity and Vulnerability of Internet Privacy Risks.

	Model 1	Model 2
Independent Variables		
Perceived severity	-.02	-.02
Perceived vulnerability	.02	.01
Control Variables		
Age	-.01	
Gender (Male)	.34*	
Household Income	.02	
Education	-.02	
Hispanic	-.24	
African American	.08	
Asian	.49	
Other Race	-.10	
Employment Status	-.10	
Total R^2	.01	.00

*p<.05; **p<.01; ***p<.001

Hypothesis 6 posits that perceived Internet privacy knowledge is positively associated with TPE perceptions of online privacy risks. In the current study, we find that the effect of perceived knowledge was positive (b=.02) and significant at .05 level (See Table 16). Hence, H6 was supported.

Table 16. Ordinal Regression Predicting TPE Perceptions with Perceived Knowledge

	Model 1	Model 2
Independent Variables		
Perceived Internet privacy knowledge	.02*	.02**
Control Variables		
Age	-.01	
Gender (Male)	.36*	
Household Income	.03	
Education	-.02	
Hispanic	-.14	
African American	-.02	
Asian	.44	

Table 16. Continued

Other Race	-.20	
Employment Status	-.12	
Pseudo R^2	.01*	.01**

*p<.05; **p<.01; ***p<.001

Hypothesis 7 contends that prior negative online privacy experiences lead to the

decreased TPE perception of Internet privacy risks. As can be seen in Table 17, the

effect of negative privacy experiences was negative and significant (b= -.47, p<.05). The

results indicate that people who experienced privacy conflicts online tend to be aware

that their personal data is at risk on the Internet. H7 was supported in the current study.

Table 17. Ordinal Regression Predicting TPE Perceptions with Negative Privacy
Experiences

	Model 1	Model 2
Independent Variables		
Negative Privacy Experiences	-.47**	-.41*
Control Variables		
Age	-.01	
Gender (Male)	.45**	
Household Income	.01	
Education	-.01	
Hispanic	-.23	
African American	.07	
Asian	.38	
Other Race	-.20	
Employment Status	-.15	
Total R^2	.01*	.004*

*p<.05; **p<.01; ***p<.001

Hypothesis 8 holds that the Internet use is positively associated with TPE

perceptions of Internet privacy risks. The current study tested six types of Internet use,

including information searches, news consumption, online shopping, online gaming,

online chatting, and social media use. In the ordinal regression model, the current study

tested the effects of these six types of Internet use on TPE perceptions. The effect of online information searches was positive and significant (β=.13, p<.01), whereas the effects of other predictors were not significant (See Table 18). H8 was partially supported, though only in the case of online information searches.

Table 18. Ordinal Regression Predicting TPE Perceptions with Internet use

	Model 1	Model 2
Independent Variables		
Information Search	.03**	.03*
News Consumption	-.01	-.01
Online Shopping	-.01	-.01
Online Gaming	.09	.11
Online Chatting	.02	.07
Social Media Use	.00	-.00
Control Variables		
Age	-.03	
Gender (Male)	.07	
Household Income	.03	
Education	-.01	
Hispanic	-.04	
African American	-.02	
Asian	.06	
Other Race	.00	
Employment Status	-.02	
Pseudo R^2	.02*	.01**

*p<.05; **p<.01; ***p<.001

In summary, the results entailed that TPE hypothesis in the context of Internet privacy was supported. The two hypotheses of behavioral component were supported, indicating that TPE perception is an influential predictor of the intention to adopt privacy protective measures. Four factors—social distance, perceived knowledge, negative privacy experiences, and activity of Internet use—were found to be significant predictors of TPE perceptions. The results of the empirical tests are displayed in Figure 2.

Figure 2. Results of Hypotheses Tests
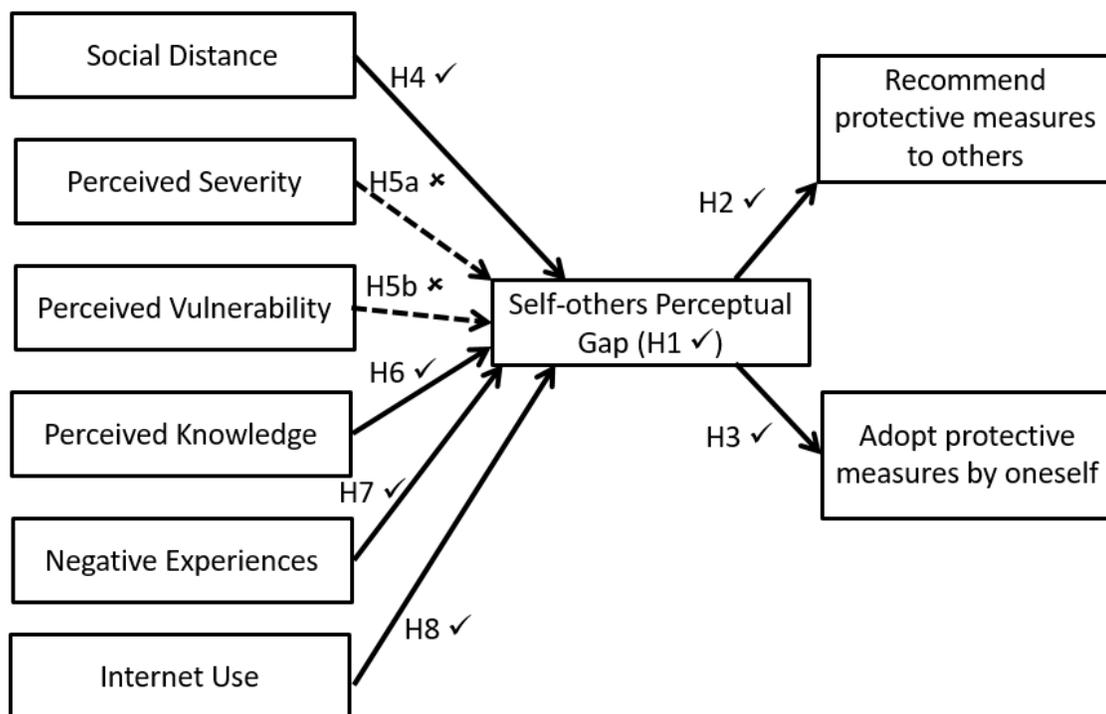
Note: Solid lines represent significant effect, whereas dashed lines represent insignificant effect.

6. DISCUSSION

This study aimed to deepen our existing understanding of perceived Internet privacy risks on the basis of TPE theory. The past decade witnessed the exponential growth of cyber-attacks, ranging from stolen online accounts to monetary losses via Internet scams. In response to privacy threats on the Internet, computer engineers developed anti-virus software, which can detect, prevent, and delete the malware automatically (Kim, Yan, & Zhang, 2015). The social media providers invented the visibility setting that can help users keep unwanted contacts away (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011). For individual Internet users, privacy protection can be as simple as changing passwords frequently, avoiding posting sensitive information, clearing browser cookies regularly, and leaving or not accessing suspicious websites. However, the fact is that people tend to believe that online privacy invasion will not occur to them and therefore, refuse to take the protective measures (Debatin et al., 2009).

To enhance the effectiveness of cyber-security interventions, the question of how Internet users perceive Internet privacy risks was crucial but under-examined in the previous studies. To address this gap in the literature, the current study tested 1) how people construct differential judgments of themselves versus others, 2) how the TPE perceptions influence behavioral intentions to adopt the Internet privacy protection measures and/or recommend these measures to others, 3) how social distance, perceived severity and vulnerability of Internet privacy risks, negative online privacy experiences, perceived Internet privacy knowledge, and Internet use influence TPE perceptions of

Internet privacy. Each of these points represents a significant contribution to our understanding of Internet privacy risks and third-person effect theory. The findings of the current study provided valuable implications to enhance the effectiveness of cyber security campaigns.

6.1 Perceptual Component of TPE

The current study reveals that people develop distinct perceptions in evaluating threats to online privacy. Specifically, people perceive greater privacy risks on others than on themselves. The results supported the TPE in general, suggesting that biased perceptions prevail in the Internet-based media environments.

TPE theory was developed by Sociologist W. Phillips Davison in 1983, a period when television and newspapers were the dominant media. In a study designed to examine the influence of persuasive communication on the mass media, Davison found that respondents perceived other voters were more influenced by campaign themes, children by the television advertisements, and others were more influenced by the presidential campaign advertising (Davison, 1983). At that time, media consumers only had access to a limited number of television and radio channels as well as print media outlets. Media served as the most the important sources for following political events, national or global economic developments, or sports and weather updates. Because of the scarcity of media channels, personal background played a pivotal role in evaluations of the media content. For instance, frequent viewers of political campaigns perceived other people as lacking objective understandings of the candidates and more likely to be influenced by campaign advertisements (Perloff, 1989). Even people lacking knowledge

of presidential candidates perceive others are uninformed on specific issues. One reason

for this optimistic bias is that the conventional media is a one-to-many communication

mode, viewers could not exchange with media producers directly or view comments

from other viewers. Media consumers can only listen to the media reports but cannot

explore news events from other sources. The limited media channels and media content

contributed to the existence of TPE. Also, human beings' natural desire to reduce social

anxiety and improve self-esteem lead people to generate the biased perceptions of media

effects (Davison, 1983).

Thirty years since the initial findings of TPE, the media environment has

changed dramatically. The new media environment provides unlimited choice to users.

The conventional media platform is no long the sole information source for the media

consumers. In the latest presidential campaign, even though voters still followed the

presidential debate closely, more viewers watched it online than on television (Azari,

2016). One of the main reasons is that people are used to multi-tasking today (Pilotta,

Schultz, Drenik, & Rist, 2004). In the middle of the debate, people may also post their

personal reflections, read the instant posting from commentators and celebrities, and

search for key words that the debate has covered. The multi-channel and multi-media

features of today's communication technology enable users to develop in-depth thinking

of certain social events. Another major difference is that interactive media channels

make it hard to attract the attention of the public with a single communication channel.

Media marketers and campaigners use integrated marketing communications to

distribute their media products with a variety of communication channels and disciplines (Reid, Luxton, & Mavondo, 2005).

The current study found firm support for TPE perceptions of Internet privacy risks. This finding provides two valuable contributions to our understanding of TPE theory. First, the variety of features in today's Internet-based media did not lead to objective judgments of media effects. Even though the online sources create opportunities for media consumers to research on a topic and develop a more comprehensive understanding of topics, such as Internet privacy risks, TPE perceptions still prevail. Internet users tend to separate themselves from others and develop self-serving biases regarding Internet privacy risks. Second, Internet users are highly motivated to reduce the social anxiety and enhance self-esteem. People's desire to outperform others still persist in the new media environment. The powerful operating systems of the new media technology create an illusion that users have absolute control over their personal data online. However, the fact is that hackers can easily break through the defense systems and collect the users' personal information. For the cyber-security training providers, the key of successful training is to raise Internet users' awareness of privacy risk by reducing the TPE perceptions of the Internet privacy risks.

6.2 Behavioral Component of TPE

The behavioral component of TPE proposes that the TPE perceptions of media effects lead to the behavioral intentions to counteract negative media influence (Davison, 1983). The current study found that TPE perceptions of Internet privacy risks positively predict people's willingness to recommend the Internet privacy protection measures to

others and negatively predict the willingness to adopt the protective measures themselves.

In the studies of conventional media, researchers found that people with high levels of TPE perceptions believe that they possess stronger ability to resist the negative impact of the mass media than other people (McLeod et al., 1997). One outcome of TPE perceptions is support for media censorship to protect the public (Gunther, 1995; Paul et al., 2000; Wu & Koo, 2001; Youn et al., 2000). Specific to pornography, prior studies documented strong support for the behavioral component of TPE (Chen et al., 2015).

Prior behavioral TPE studies concentrated on the censorship of pornographic media content, which refers to the restriction of distributing media content with sexually explicit information (Wu & Koo, 2001). People express concerns for the negative consequences of pornography and are willing to support for restrictions (Chen et al., 2015). From the perspective of feminist scholars, women are portrayed as powerless in pornographic videos, thus intensifying the unfair treatment of women and increasing violent sex crimes (Cowan, 1992). Due to the negative perceptions of pornography, in multiple studies, people were found to favor the censorship. However, when we focus on perceptions of the Internet, people's perceptions vary significantly. For instance, computer engineers may perceive the Internet as a series of programming codes, young female users may perceive it as major shopping carriers, political savvy activists may perceive it as news forums, video gaming fans may treat as a gaming platform, and people who are victims of Internet scam may perceive it as threat to personal financial accounts. Depending on people's personal characteristics, occupation, age, personal

experiences, and needs, people perceive the Internet differently and develop differential intentions to make use of the Internet.

The current study contributes to our understanding of behavioral component of TPE in the context of Internet privacy. Unlike media censorship, which is primarily the responsibility of the government, the behavioral intentions of Internet privacy protection reflect people's individual reactions to potential online privacy threats. The Internet efficacy and the proficiency of protective measures exert great influence over the outcomes of privacy security online. The findings of the current study revealed that TPE perceptions of Internet privacy risks is one of the major barriers to adopt privacy protective measures online. People who possess high TPE perceptions believe that they have already built effective defense mechanisms for personal data online or that they are not at risks for privacy invasions. The consequences of these biased beliefs are the continuation of risky online activities and the refusal to update protective measures. This finding reveals that to increase people's adoption of privacy protective measures, it is important to diminish the TPE perceptions of Internet privacy.

Similar to the pornography censorship studies, the current study found that TPE perceptions positively predict the willingness to recommend protection measures to others. When the media content is considered as negative, people oppose the content and are more likely to recommend protective measures to their personal contacts. Interpersonal communication appears to be a valuable channel to enhance to online privacy protection. For campaign programs promoting cyber security, the use of mass media can satisfy the population-level market demand, but viewers often do not pay

attention to the programs and do not receive immediate feedback (Randolph &

Viswanath, 2004). The advantage of interpersonal channel is that trainer and trainees can

exchange information instantly, the trainer can modify message delivery to ensure the

effectiveness of the training program, facilitate constructive interactions, and discover

the sources of resistance to change (Hwang, 2012). To increase the adoption of privacy

protection measures, security trainers should make use of interpersonal counseling

session to resolve users' confusion and concerns. Also, trainers should focus on opinion

leaders of a community, an organization, or a family first. The opinion leaders can then

further spread the ideas of privacy protection to followers. The strategic use of

communication channels can improve the effectiveness of cyber-security training

programs.

      In addition, the current study provides a novel perspective to research on

people's intention of adopting privacy protective measures. Prior research used PMT and

EPPM as the primary framework to examine the antecedents of privacy protection

intention (Chen, Beaudoin, & Hong, 2017; Mohamed & Ahmad, 2012; Youn, 2009).

PMT assumes that protection motivation is a function of six factors, perceived severity,

perceived vulnerability, rewards of maintaining risky behaviors, response efficacy, self-

efficacy, and costs of adopting behavioral changes (Rogers, 1975). Later, EPPM added

that only when people perceive both high efficacy and threat, they are willing to engage

in behavioral changes, whereas in other cases, people tend to ignore the threat (Witte,

1994). Scholars developed PMT and EPPM in the context of health promotion studies

(Rogers, 1975; Witte, 1994). PMT and EPPM have received robust support in related

health context, such as promotion of physical exercise, healthy diets, and anti-smoking (Pechmann, Zhao, Goldberg, & Reibling, 2003; Plotnikoff & Higginbotham, 1998; Plotnikoff, Trinh, Courneya, Karunamuni, & Sigal, 2009), but the Internet privacy studies yielded mixed results of PMT and EPPM. In many studies, the six antecedents of PMT failed to predict the intention of adopting privacy protective measures (Chen et al., 2016b; Feng & Xie, 2014).

The weak support for PMT and EPPM in Internet privacy studies can be attributed to contextual differences. In the health promotion practices, the barrier of behavioral changes is relatively high. For instance, for long term smokers, quitting smoking can lead to the painful physiological reactions. To lead healthy behavioral change, health interventionists need to improve smokers' understanding of health risks and set reasonable goals for quitting smoking (Stevens, Thorogood, & Kayikki, 2002). Smokers need to weigh the health risks seriously and then make decisions about behavioral change. In contrast, Internet privacy protection can be as simple as adopting complex passwords and avoiding visiting risky websites. The results of the current study suggested that the optimistic bias is the main reason for ignoring privacy protection measures. Respondents tend to believe that they will not be victims of the Internet privacy attacks even though their perceived online privacy risk is high. This study provides an alternative theory to assess Internet privacy. The finding of the current study suggests that the key of successful cyber security campaign is to diminish the TPE perceptions.

6.3 Antecedents of TPE Perceptions

The current study also advances our understandings of antecedents of TPE

perceptions in the context of Internet privacy. First, unlike prior studies relying on the

assumption of social distance and desirability of media content, the current study

provided empirical tests on these two factors. Second, three novel antecedents—

perceived knowledge, negative experiences, and activity of Internet use—were also

tested. The research findings provided valuable suggestions to cyber security trainers

about how to increase the adoption of privacy protection measures.

6.3.1 Social Distance

Social distance reflects the perceptual difference between self and others

(Karakayali, 2009). The current study found that TPE perceptions of Internet privacy

risks increase with social distance. Third person perceptions are smaller for close relative

and friends than more distant others.

In sociological research, Bogardus (1933) conceptualized social distance on

affectivity. Social distance is measured by affective distance, such as how much

sympathy an individual feels for another person or another group of people (Bogardus,

1947). Prior TPE studies relied on the assumption of social distance through predefined

groups (i.e., relatives are perceived as closer than residents in another state) (McLeod et

al., 1997). However, the assumption of social distance can be inaccurate. This study is

the first attempt to use structural equation modeling to test the association between TPE

perceptions and social distance. Respondents were asked to evaluate perceived Internet

privacy risks on 1) close relatives, 2) close friends, 3) colleagues in the same

organization, 4) people in the same education or the same educational level, 5) citizens or permanent residents in the U.S, 6) visitors in the U.S, and 7) people outside of the U.S. Social distance was found to be positively associated with TPE perceptions. Group 1 of close relatives recorded the lowest level of TPE perceptions, whereas group 7 of people outside the U.S displayed the highest TPE perceptions. There is only one exception: TPE perceptions of group 5 (citizens or permanent residents in the U.S) is greater than group 6 (visitors in U.S). One reasonable explanation is that respondents may perceive international travelers who can afford the long-distance trip as rich, well-educated, and better off than the average U.S residents.

How do people compare self and others? Researchers found that people tend to develop positive perceptions of self and close others (Eveland et al., 1999). The uncertainty increases with the social distance. People can clearly tell the life standards and media use habits of relatives and close friends. When it comes to the general citizens of the U.S and the people outside of this country, people may find it difficult to define who these "others" are. A foreigner can be an engineer from a developed country or a refugee living in the camps of an underdeveloped country. When there is high level of uncertainty, people often engage in downward comparison that refers to the negative perceptions of out-group individuals (Taylor & Lobel, 1989). Downward comparison is a defensive mechanism that is used to enhance self-esteem. When a person compares self with another individual with poorer living conditions, for example, their life satisfaction is enhanced (Gibbons & Buunk, 1999). In the current study, the results

indicated that people tend to engage in downward comparison when others are perceived as distant.

This finding provides important implications for the cyber security professionals. To persuade consumers to adopt the protection measures, the key is to design campaign messages using examples that are closer to the audiences. The campaigners need to examine the backgrounds of the audiences first and then design personalized training messages to engage the audiences.

6.3.2 Perceived Severity and Vulnerability of Internet Privacy Threat

The current study also finds significant effects for perceived severity and vulnerability. In the studies of TPE in mass media, the desirability of media messages predicts TPE perceptions. When media content is perceived as desirable, such as anti-smoking advertising, people perceive that they are willing to engage in the behavioral change (Lewis et al., 2007). In such case, TPE diminishes or even gets reversed. In contrast, when the media content is perceived as negative, such as violent video games, people think that they are able to resist the negative media effects but others are heavily impacted (Boyle et al., 2008).

Ego-defense and ego-enhancement mechanism provides theoretical explanations of this phenomenon. With respect to ego-defense, when people view negative media content, they often attribute the negative media impact to others to reduce the anxiety (Freud, 1992). Ego-enhancement, in contrast, refers to people's motivation to feel good about themselves (Boyle et al., 2008). For instance, in viewing anti-smoking advertisement, smokers are likely to perceive themselves to be early quitters even when

they are not. These differential perceptions result in widened self-other perceptual discrepancies. One of the major limitation of prior studies is that the desirability of media content is assumed rather than empirically tested. For instance, researchers assumed that the public perceives smoking and eating junk food as bad for their health (Glanz, Basil, Maibach, Goldberg, & Snyder, 1998; Watson, Clarkson, Donovan, & Giles-Corti, 2003). However, people may perceive these topics differently due to differences in personal backgrounds, suggesting the need to test the desirability of media content empirically.

The current study provides an empirical test of the undesirability of Internet privacy invasion using perceived severity and perceived vulnerability. Respondents reported high perceived severity and vulnerability of Internet privacy invasion, indicating that they are aware of the privacy risks. However, the effects on TPE perceptions were not significant. One reason can be the flawed measurement. The current study measured perceived severity and vulnerability of general privacy invasion but did not specify what type of privacy invasion it is. When asked to evaluate privacy invasions, some respondents may think about loss of SNS account, whereas some others may consider the case of monetary loss. Respondents' inconsistent attributes detriment the validity of perceived severity and vulnerability measurement. Future study should ask the respondents to estimate the severity and vulnerability of different privacy invasions first and then build a scale of undesirability of online privacy invasion according to the responses (similar to Bogardus social distance scale). Next, respondents

estimate TPE perceptions of each type of privacy invasion. Such study can identify if TPE perceptions increase with perceived undesirability of Internet privacy invasions.

6.3.3 Perceived Internet Privacy Knowledge

Consistent with prior studies on conventional media, the current study finds that perceived Internet privacy knowledge positively predicts TPE perceptions. The current study extended the research of perceived knowledge into a new context—Internet privacy.

Prior studies on the effects of perceived knowledge on the TPE perceptions yielded mixed results. Media consumers with higher perceive knowledge were found to report greater TPE perceptions of media effects (Price & Tewksbury, 1996; Salwen & Driscoll, 1997; Tiedge et al., 1991). For instance, in a study assessing people's perceptions of a fictional TV show, viewers with high perceived political knowledge reported higher TPE perception of media effects (Lasorsa, 1989). Those viewers who claimed to be political knowledgeable believed less informed "others" would be likely to mistake the TV show as reality. Interestingly, this study tested respondents' actual political knowledge by grading the answers of related questions that did not predict the TPE perceptions. In the research of Internet pornography and violent rap music, researchers did not find significant association between perceived knowledge and TPE perceptions.

Unlike prior studies primarily focusing on conventional media, the current study extends this research into the context of Internet privacy. The developer of TPE, Davison, suggested that TPE reflects people's subjective judgments toward other people

and media topics, which revealed the importance of perceived knowledge (Davison, 1983). Perceived knowledge of Internet privacy reflects people's self-reported understandings of Internet privacy risks. People with high perceived knowledge tend to be confident in dealing with privacy threats online even if their perceptions of Internet privacy may not be accurate. With the advancement of technology, the knowledge of Internet privacy is likely to be outdated soon. Ubiquitous use of Internet-based technology exposes people's online information. If the existing perception is wrong, people cannot identify the potential risks and are more likely to be victims of future privacy attacks. Inaccurate perceptions of Internet risk impose risks to the Internet users.

This finding suggested that cyber security training professionals need to introduce the latest hacking technologies to the audience to reduce audiences' TPE perceptions. For instance, in the training session, the trainers may use the anti-virus software to conduct a thorough test on operating systems. They can then explain the function of each malware found in the search. Regards to personal data loss, the trainers may use web mining technology to collect information from the social media user. Then, trainees can understand the ease with which criminals can obtain private information and may become more careful in future online data disclosures. The finding of this study revealed the exigent need to correct the inaccurate perceptions of Internet privacy risks and reduce the TPE perceptions of Internet privacy risks.

6.3.4 Negative Online Privacy Experiences

Another antecedent addressed is the negative online privacy experiences, which refers to identity theft and financial loss. The current study found that negative online

privacy experiences decrease respondents' TPE perceptions of Internet privacy risks. Experiences of privacy loss increase awareness of privacy risk online, which is consistent with prior studies (Chen et al., 2016a, 2017; Cho et al., 2010).

The advancement of Internet-based technology, such as web mining and malware, enable criminals to monitor individual users' private data online. Once the computer is installed with malware, the hackers can collect the information stored in the computer and steal the important account information (Moore et al., 2009; Thomas & Martin, 2006). Criminals can access personal online accounts or even worse steal money from the financial accounts. The misuse of programing technology lead to the increasingly occurence of privacy loss. The current study found that more than 90% of respondents experienced at least one of the following privacy invasions online: 1) online theft of financial assets, 2) reception of spam emails, 3) unauthorized access to online personal accounts, 4) online harrassment, and 5) unwanted friend requests. It is exigent for Internet users to adopt privacy protection measures.

People with negative online privacy expeirences tend to believe that the Internet privacy threat is real and relevant to themselves. People often refer to prior experiences to direct the future decisions and behaviors (Cho et al., 2010). For those who experienced privacy invasions, they have experienced the negative outcomes of privacy loss. Hence, they are likely to perceive higher Internet privacy risks on self, which, in turn, decreases TPE perceptions. Prior studies suggested the victims of Internet privacy loss tend to stay alert to the risky online behaviors (Pratt et al., 2010). For instance, people who lost money on fake commercial websites are more liklely to purchase products from

prestigious online shopping platforms and reject attractive offers from suspicious

websites (Kirlappos & Sasse, 2012). However, the cost is too high if people only realize

the risks after being a victim.

For the cyber security providers, to enhance people' awarenss of privacy risks,

they should make use of virtual reality gaming technology to simulate the scenario of

privacy loss. In the gaming environment, trainees can experience the consequences of a

hypothetical privacy loss. Trainers can create a gaming phase for each type of privacy

loss. After playing the game, trainees can be taught how to respond to the potential risks.

Such training design can engage the audiences effectively and reduce the boredom of

verbal and textual introduction.

6.3.5 Internet Use

A final intriguing antecedent addressed by the current study involves Internet

use. I tested the effects of five types of Internet use on TPE perceptions of Internet

privacy risks. The current study found that the one type of Internet use—online

information searches—positively predicts the TPE perceptions of Internet privacy risks.

The effect of media uses on TPE percpetions was initally assessed in the

conventional media platforms. Media use refers to the consumption of media content and

the engagement in media channels (Marshall, Biddle, Gorely, Cameron, & Murdey,

2004). In conventional media channels such as television and newspaper, individual

viewers are passive receivers of information. The amount and variety of media sources

were limited. For instance, the big three television networks—ABC, CBS, and NBC—

dominated the television market from 1950s to 1980s (Webster, 2005). The prime time

news coverage was the major source for viewers to acquire news information. At that time, media producers served as gatekeeping roles who determine what information is dissemiated to the public (Allen & Hawkins, 1999). As discussed before, people learn from the past experiences and make future decision according to the prior experiences. When it comes to the issues irrelevant to daily life such as intertional relationships and wars, media content plays a central role in invidividuals' knowledge development of such issue (Marshall et al., 2004).

On the Internet, users are not only content consumers but also content producers. For instance, on the social media like Facebook, users post millions of comments, articles, and pictures every day. The citizen journalists today collect, analyze, and report news information indivdiually and post their news reports on social media and personal webpages (Goode, 2009). The major news agency also make use the new media channels to post latest news online (Castronovo & Huang, 2012). Internet-based services provide unlimited channels for users to explore the truth behind the news event. In addition to news consumpiton, the uses of media on the Internet have been expanded to online gaming, chatting, shopping, and social interactions. The Internet becomes an indispensible part of our daily life but also impose users' personal data at the risk of privacy invasion. The changes in media envrionment suggests the need to examine the effects of Internet use on TPE perceptions of Internet privacy risks.

In the current study, online information searches were found to be a positive predictor of TPE perceptions of Internet privacy risks, whereas the effects of online news consumption, online chatting, online shopping, and social media use were not

significant. Nowadays, Internet users frequently use search engines to search

information on the Internet. For instance, when people browse items on the shopping

websites, they are likely to search the products of interest online and read other

customers' comments. In the middle of watching the news, people search for unfamiliar

terms relating to news content. People also search for answers online when they are in

need of career suggestions, health-related information, and job opportunities. Internet

users who search information online frequently tend to be proficient Internet users. They

are more likely to be knowlegeable about Internet privacy risks, which results in a

widened self-other perceptual gap of Internet privacy risks.

7. CONCLUSIONS

7.1 Summary of Research Findings

The current study systematically tests TPE in the context of Internet privcacy. Using a convenience sample from Amazon Mturk, the current study examined the perceptual and behavioral components of TPE and explored five antecedents of TPE—social distance, the undesirability of online privacy invasion, perceived Internet privacy knowledge, negative online privacy experiences, and Internet use. The research findings are as follows.

First, the current study found that respondents perceive higher Internet privacy risks on others than on self. Second, TPE perceptions of Internet privacy risks positively predict the willingness to recommend privacy protection measures to others and negatively predict the intention to adopt privacy protection measures by oneself. Third, social distance, perceived Internet privacy knowledge, and Internet use were found to be significant antecedents of TPE perceptions of Internet privacy risks.

7.2 Theoretical Implications

The current study provides an alternative theoretical framework to address Internet privacy. Prior studies of Internet privacy used PMT and EPPM to test people's intention of online privacy protection. The weak support for these fear based theories suggested that before adopting privacy protection measures, people do not undergo sophisticated threat appraisal and coping appraisal. The finding of current study indicated that TPE perceptions of Internet privacy risks are the major barrier to adopting protective measures.

The current study extends TPE study into the context of Internet privacy. The finding of the current study indicate that even if the media environment changed dramatically, TPE perceptions of media effects still prevail. The new features of the Internet did not erase people's self-serving bias. Prior studies primarily addressed people's behavioral intentions to support for restrictions of harmful media content (i.e., pornography & media violence). This is an area, however, in which policy makers have to restrict media content. The current study extends the TPE study into Internet privacy, a medium in which individuals can easily make decisions to adopt protective measures. The current study advances the understandings of TPE theory in a novel context.

Next, the current study addresses five antecedents of TPE perceptions of the Internet privacy risks. Prior studies focus on two antecedents of TPE perceptions—desirability and social distance. Researchers use their own judgments to assume the social distance of a comparison group and desirability of media content instead of testing these two antecedents empirically. However, the fact is that people may possess differential perceptions of social distance and desirability of media content. Researchers' assumption can be biased and inaccurate. The current study provides empirical tests on the desirability and social distance. Moreover, three other novel antecedents (i.e., perceived Internet privacy knowledge, negative online privacy experiences, and Internet use) are tested. The current study found that perceived knowledge, prior experiences, and media uses are important antecedents of TPE perceptions.

7.3 Practical Implications

The findings of the current study provide valuable implications to cyber security training providers. The first lesson learned is that TPE perception of Internet privacy risks is a major barrier to adopt privacy protection measures. The key to successful training is to reduce audiences' self-serving bias and raise awareness of privacy risks. Second, in designing the cyber security training programs, the trainers should consider making use of the four significant antecedents—social distance, perceived knowledge, negative experiences, and Internet use—to decrease self-serving bias. Trainers should use examples relevant to the audiences, let the audiences experience the consequences of privacy loss, inform the audiences the latest changes in hacking technology, and introduce the privacy risks on multiple online platforms. Third, in the training programs, it is important to use the interpersonal channels to interact with the audiences. Respondents were found to be willing to recommend privacy protection measures to others. If the trainers can successfully educate the Internet privacy risks to opinion leaders, these opinion leaders are likely to recommend privacy protection measures to other opinion followers. Moreover, the trainers need to maintain contact with the trainees. In comparison with the one-to-many communication model, one-to-one conversation is more effective in leading to behavioral change.

7.4 Limitations of the Current Study

First, the convenience sample on Mturk may not be as representative as a random sample as it only includes individuals who are registered on Mturk. Mturk provides a reasonable cost effective approach to reach the Internet users. However, to generalize the

research finding to the overall Internet population, future studies should use random sample strategy. Second, the current study tested people's perceived Internet privcay risks in general without specification of Internet platforms. People's perceptions of online privacy can be significantly different between different platforms. For instance, the level of concerns about SNSs and financial account can be different. Future research should explore the differential perceptions on different online spaces. Third, the data used is cross-sectional which cannot be used to test casual relationships. Future studies should use longitudinal data to explore the cognitive process of threat and coping appraisal. For campaign studies, lognitudinal data can be used to test what strategies are most effective in reducing people's TPE perceptions of Internet privacy risks. Fourth, the measurement of undesirability of privacy invasion need to be improved. There is a need to develop an undesiriablity scale and evaluate people's TPE perceptions toward different types of privacy invasion.

REFERENCES

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly, 34*(3), 435-461.

Allen, S. M., & Hawkins, A. J. (1999). Maternal gatekeeping: Mothers' beliefs and behaviors that inhibit greater father involvement in family work. *Journal of Marriage and the Family*, 199-212.

Andsager, J. L., & White, H. A. (2009). *Self versus others: Media, messages, and the third-person effect*. Mahwah, NJ: Routledge.

Antonopoulos, N., Veglis, A., Gardikiotis, A., Kotsakis, R., & Kalliris, G. (2015). Web Third-person effect in structural aspects of the information on media websites. *Computers in Human Behavior, 44*, 48-58.

Azari, J. R. (2016). How the news media helped to nominate Trump. *Political Communication, 33*(4), 677-680.

Azzalini, A., & Capitanio, A. (1999). Statistical applications of the multivariate skew normal distribution. *Journal of the Royal Statistical Society: Series B (Statistical Methodology), 61*(3), 579-602.

Bauman, L. J., & Siegel, K. (1987). Misperception among gay men of the risk for aids associated with their sexual behavior. *Journal of Applied Social Psychology, 17*(3), 329-350.

Beauregard, K. S., & Dunning, D. (1998). Turning up the contrast: Self-enhancement

    motives prompt egocentric contrast effects in social judgments. *Journal of*

    Personality and Social Psychology, 74(3), 606-621.

Bish, A., Yardley, L., Nicoll, A., & Michie, S. (2011). Factors associated with uptake of

    vaccination against pandemic influenza: A systematic review. *Vaccine, 29*(38),

    6472-6484.

Bogardus, E. S. (1933). A social distance scale. *Sociology & Social Research, 17*, 265-

    271.

Bogardus, E. S. (1947). Measurement of personal-group relations. *Sociometry, 10*(4),

    306-311.

Boyle, M. P., McLeod, D. M., & Rojas, H. (2008). The role of ego enhancement and

    perceived message exposure in third-person judgments concerning violent video

    games. *American Behavioral Scientist, 52*(2), 165-185.

Brosius, H. B., & Engel, D. (1996). The causes of third-person effects: Unrealistic

    optimism, impersonal impact, or generalized negative attitudes towards media

    influence? *International Journal of Public Opinion Research, 8*(2), 142-162.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and

    consequences of victimhood. *Psychology, Crime & Law, 20*(3), 261-283.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new

    source of inexpensive, yet high-quality, data? *Perspectives on Psychological*

    Science, 6(1), 3-5.

Campbell, W. K., & Sedikides, C. (1999). Self-threat magnifies the self-serving bias: A
    meta-analytic integration. *Review of General Psychology, 3*(1), 23.

Castronovo, C., & Huang, L. (2012). Social media in an alternative marketing
    communication model. *Journal of Marketing Development and Competitiveness,
    6*(1), 117.

Chen, H., Beaudoin, C. E., & Hong, T. (2016a). Protecting oneself online: The effects of
    negative privacy experiences on privacy protective behaviors. *Journalism &
    Mass Communication Quarterly, 93*(2), 409-429.

Chen, H., Beaudoin, C. E., & Hong, T. (2016b). Teen online information disclosure:
    Empirical testing of a protection motivation and social capital model. *Journal of
    the Association for Information Science and Technology, 67*(12), 2871-2881.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical
    test on internet scam victimization, online privacy concerns, and privacy
    protection behaviors. *Computers in Human Behavior, 70*, 291-302.

Chen, H., Wu, Y., & Atkin, D. J. (2015). Third person effect and Internet pornography in
    China. *Telematics and Informatics, 32*(4), 823-833.

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks:
    Testing the moderating effects of perceived controllability and prior experience.
    Computers in Human Behavior, 26(5), 987-995.

Cohen, J., & Davis, R. G. (1991). Third-person effects and the differential impact in
    negative political advertising. *Journalism & Mass Communication Quarterly,
    68*(4), 680-688.

Cohen, J., Mutz, D., Price, V., & Gunther, A. (1988). Perceived impact of defamation an experiment on third-person effects. *Public Opinion Quarterly, 52*(2), 161-173.

Cowan, G. (1992). Feminist attitudes toward pornography control. *Psychology of Women Quarterly, 16*(2), 165-177.

Crossler, R. E. (2010). *Protection motivation theory: Understanding determinants to backing up personal data.* Paper presented at the System Sciences (HICSS) 43rd Hawaii International Conference.

Culbertson, H. M., & Stempel, G. H. (1985). Media malaise: Explaining personal optimism and societal pessimism about health care. *Journal of Communication, 35*(2), 180-190.

David, P., & Johnson, M. A. (1998). The role of self in third person effects about body image. *Journal of Communication, 48*(4), 37-58.

Davison, W. P. (1983). The third-person effect in communication. *Public Opinion Quarterly, 47*(1), 1-15.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

Dhillon, P. S., Foster, D. P., Kakade, S. M., & Ungar, L. H. (2013). A risk comparison of ordinary least squares vs ridge regression. *The Journal of Machine Learning Research, 14*(1), 1505-1511.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-

    measurement validity and a regression model. *Behaviour & Information*

    Technology, 23(6), 413-422.

Duck, J. M., & Mullin, B. A. (1995). The perceived impact of the mass media:

    Reconsidering the third person effect. *European Journal of Social Psychology,*

    25(1), 77-93.

Eekhout, I., de Boer, R. M., Twisk, J. W., de Vet, H. C., & Heymans, M. W. (2012).

    Missing data: A systematic review of how they are reported and handled.

    Epidemiology, 23(5), 729-732.

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).

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating

    privacy concerns and social capital needs in a social media environment. *Privacy*

    online (pp. 19-32). Berlin, Germany: Springer.

Eveland, W. P., & McLeod, D. M. (1999). The effect of social desirability on perceived

    media impact: Implications for third-person perceptions. *International Journal of*

    Public Opinion Research, 11(4), 315-333.

Eveland, W. P., Nathanson, A. I., Detenber, B. H., & McLeod, D. M. (1999). Rethinking

    the social distance corollary perceived likelihood of expsoure and the third-

    person perception. *Communication Research, 26*(3), 275-302.

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking

    sites: An analysis of socialization agents and relationships with privacy-

    protecting behaviors. *Computers in Human Behavior, 33*(1), 153-162.

Fink, A. (1995). *The survey handbook*. Thousand Oaks, CA: Sage Publications.

Flanagin, A., Metzger, M., Pure, R., Markov, A., & Hartsell, E. (2014). Mitigating risk

    in ecommerce transactions: Perceptions of information credibility and the role of

    user-generated ratings in product quality and purchase intention. *Electronic*

    Commerce Research, 14(1), 1-23.

Freud, A. (1992). *The ego and the mechanisms of defence*. London, UK: Karnac Books.

Fu, K.-W., Chan, C.-H., & Chau, M. (2013). Assessing censorship on microblogs in

    China: Discriminatory keyword analysis and the real-name registration policy.

    Internet Computing, IEEE, 17(3), 42-50.

Gibbon, P., & Durkin, K. (1995). The third person effect: Social distance and perceived

    media bias. *European Journal of Social Psychology, 25*(5), 597-602.

Gibbons, F. X., & Buunk, B. P. (1999). Individual differences in social comparison:

    development of a scale of social comparison orientation. *Journal of Personality*

    and Social Psychology, 76(1), 129.

Giner-Sorolla, R., & Chaiken, S. (1994). The causes of hostile media judgments. *Journal*

    of Experimental Social Psychology, 30(2), 165-180.

Glanz, K., Basil, M., Maibach, E., Goldberg, J., & Snyder, D. (1998). Why Americans

    eat what they do: taste, nutrition, cost, convenience, and weight control concerns

as influences on food consumption. *Journal of the American Dietetic Association, 98*(10), 1118-1126.

Glynn, C., Ostman, R. E., & McDonald, D. (1995). Opinions, perception, and social reality. In T. Glasser & C. T. Salmon (Eds.), *Public opinion and the communication of consent* (pp. 249-277). New York, NY: Guilford.

Golan, G. J., & Day, A. G. (2008). The first-person effect and its behavioral consequences: A new trend in the twenty-five year history of third-person effect research. *Mass Communication and Society, 11*(4), 539-556.

Goode, L. (2009). Social news, citizen journalism and democracy. *New Media & Society, 11*(8), 1287-1305.

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples. *Journal of Behavioral Decision Making, 26*(3), 213-224.

Grewal, R., Cote, J. A., & Baumgartner, H. (2004). Multicollinearity and measurement error in structural equation models: Implications for theory testing. *Marketing Science, 23*(4), 519-529.

Gunther, A. C. (1991). What we think others think cause and consequence in the third-person effect. *Communication Research, 18*(3), 355-372.

Gunther, A. C. (1992). Biased press or biased public? Attitudes toward media coverage of social groups. *Public Opinion Quarterly, 56*(2), 147-167.

Gunther, A. C. (1995). Overrating the X-rating: The third-person perception and support for censorship of pornography. *Journal of Communication, 45*(1), 27-38.

Gunther, A. C., & Hwa, A. P. (1996). Public perceptions of television influence and

opinions about censorship in Singapore. *International Journal of Public Opinion

Research, 8*(3), 248-265.

Gunther, A. C., & Mundy, P. (1993). Biased optimism and the third-person effect.

Journalism & Mass Communication Quarterly, 70(1), 58-67.

Gunther, A. C., & Storey, J. D. (2003). The influence of presumed influence. *Journal of

Communication, 53*(2), 199-215.

Hair, J. F. J., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate Data

Analysis* (3rd ed.). New York, NY: Macmillan.

Heider, F. (2013). *The psychology of interpersonal relations*. Eastford, CT: Martino Fine

Books.

Helweg-Larsen, M., & Shepperd, J. A. (2001). Do moderators of the optimistic bias

affect personal or target risk estimates? A review of the literature. *Personality

and Social Psychology Review, 5*(1), 74-95.

Henriksen, L., & Flora, J. A. (1999). Third-person perception and children perceived

impact of pro-and anti-smoking ads. *Communication Research, 26*(6), 643-665.

Hinkle, S., & Schopler, J. (1986). Bias in the evaluation of in-group and out-group

performance. In S. Worchel & W. G. Austin (Eds.), *Psychology of intergroup

relations* (2nd ed., pp. 196-212). Chicago, IL: Nelson-Hall.

Hodge, K., & Lonsdale, C. (2011). Prosocial and antisocial behavior in sport: The role of

coaching style, autonomous vs. controlled motivation, and moral disengagement.

Journal of Sport and Exercise Psychology, 33(4), 527-547.

Hoeffding, W. (1948). A class of statistics with asymptotically normal distribution. *The annals of mathematical statistics, 19*(3), 293-325.

Hoffner, C., & Buchanan, M. (2002). Parents' responses to television violence: The third-person perception, parental mediation and support for censorship. *Media Psychology, 4*(3), 231-252.

Hoffner, C., Plotkin, R. S., Buchanan, M., Anderson, J. D., Kamigaki, S. K., Hubbs, L. A., . . . Pastorek, A. (2001). The third-person effect in perceptions of the influence of television violence. *Journal of Communication, 51*(2), 283-299.

Houston, J. B., Hansen, G. J., & Nisbett, G. S. (2011). Influence of user comments on perceptions of media bias and third-person effect in online news. *Electronic News, 5*(2), 79-92.

Huesmann, L. R., & Taylor, L. D. (2006). The role of media violence in violent behavior. *Annual Review of Public Health, 27*(1), 393-415.

Hwang, Y. (2012). Social diffusion of campaign effects: Campaign-generated interpersonal communication as a mediator of antitobacco campaign effects. *Communication Research, 39*(1), 120-141.

Internet Crime Complaint Center. (2014). 2014 Internet Crime Annual Report. Retrieved from https://www.ic3.gov/media/annualreport/2014_IC3Report.pdf

Jensen, J. D., & Hurley, R. J. (2005). Third-person effects and the environment: Social distance, social desirability, and presumed behavior. *Journal of Communication, 55*(2), 242-256.

Johnson, D. R., & Borden, L. A. (2012). Participants at your fingertips using Amazon's

 Mechanical Turk to increase student–faculty collaborative research. *Teaching of*

 Psychology, 39(4), 245-251.

Jones, E. E., & Nisbett, R. E. (1972). The actor and the observer: Divergent perceptions

 of the causes of behavior. In E. E. Jones, D. E. Danouse, H. H. Kelley, R. E.

 Nisbett, S. Valins, & B. Weiner (Eds.), *Attribution: Perceiving the causes of*

 behavior (pp. 79-94). Morristwon, NJ: General Learning.

Karakayali, N. (2009). Social distance and affective orientations *Sociological Forum,*

 24(3), 538-562.

Kaye, B. K., & Johnson, T. J. (2002). Online and in the know: Uses and gratifications of

 the Web for political information. *Journal of Broadcasting & Electronic Media,*

 46(1), 54-71.

Kenneally, E. E., & Claffy, K. (2010). Dialing privacy and utility: A proposed data-

 sharing framework to advance Internet research. *Security & Privacy, IEEE, 8*(4),

 31-39.

Kennedy, P. (1992). *A Guide to Econometrics*. Oxford, UK: Blackwell.

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution

 webpages. *Computers & Security, 49*, 95-106.

Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest

 proposal for a major rethink. *IEEE Security & Privacy, 10*(2), 24-32.

Ko, C. H., Liu, G. C., Yen, J. Y., Chen, C. Y., Yen, C. F., & Chen, C. S. (2013). Brain

 correlates of craving for online gaming under cue exposure in subjects with

Internet gaming addiction and in remitted subjects. *Addiction Biology, 18*(3), 559-569.

Kotrlik, J., & Higgins, C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal, 19*(1), 43-50.

Krosnick, J. A., & Milburn, M. A. (1990). Psychological determinants of political opinionation. *Social Cognition, 8*(1), 49.

Kuss, D. J., Louws, J., & Wiers, R. W. (2012). Online gaming addiction? Motives predict addictive play behavior in massively multiplayer online role-playing games. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 480-485.

Largent, E. A., Grady, C., Miller, F. G., & Wertheimer, A. (2012). Money, coercion, and undue inducement: A survey of attitudes about payments to research participants. *IRB, 34*(1), 1-8.

LaRose, R., Lai, Y., Lange, R., Love, B., & Wu, Y. (2005). Sharing or piracy? An exploration of downloading behavior. *Journal of Computer-Mediated Communication, 11*(1), 1-21.

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127-149.

Lasorsa, D. L. (1989). Real and perceived effects of 'Amerika'. *Journalism and Mass Communication Quarterly, 66*(2), 373-378.

Lee, B., & Tamborini, R. (2005). Third-person effect and internet pornography: The influence of collectivism and internet self-efficacy. *Journal of Communication, 55*(2), 292-310.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Lewis, I., Watson, B., & Tay, R. (2007). Examining the effectiveness of physical threats in road safety advertising: The role of the third-person effect, gender, and age. *Traffic Psychology and Behaviour, 10*(1), 48-60.

Li, X. (2008). Third-person effect, optimistic bias, and sufficiency resource in Internet use. *Journal of Communication, 58*(3), 568-587.

Little, R. J., & Rubin, D. B. (1989). The analysis of social science data with missing values. *Sociological Methods & Research, 18*(2-3), 292-326.

Lo, V.-h., & Wei, R. (2002). Third-person effect, gender, and pornography on the lnternet. *Journal of Broadcasting & Electronic Media, 46*(1), 13-33.

Lo, V.-H., & Wei, R. (2005). Exposure to Internet pornography and Taiwanese adolescents' sexual attitudes and behavior. *Journal of Broadcasting & Electronic Media, 49*(2), 221-237.

Lord, C. G., Ross, L., & Lepper, M. R. (1979). Biased assimilation and attitude polarization: The effects of prior theories on subsequently considered evidence. *Journal of Personality and Social Psychology, 37*(11), 2098.

Manning, W. G., & Mullahy, J. (2001). Estimating log models: to transform or not to transform? *Journal of Health Economics, 20*(4), 461-494.

Mardia, K. V. (1970). Measures of multivariate skewness and kurtosis with applications. *Biometrika, 57*(3), 519-530.

Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., & Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: A meta-analysis. *International Journal of Obesity, 28*(10), 1238-1246.

McLeod, D. M., Detenber, B. H., & Eveland, W. P. (2001). Behind the third‑person effect: differentiating perceptual processes for self and other. *Journal of Communication, 51*(4), 678-695.

McLeod, D. M., Eveland, W. P., & Nathanson, A. I. (1997). Support for censorship of violent and misogynic rap lyrics an analysis of the third-person effect. *Communication Research, 24*(2), 153-174.

Middleton, W., Harris, P., & Surman, M. (1996). Give'em enough rope: Perception of health and safety risks in bungee jumpers. *Journal of Social and Clinical Psychology, 15*(1), 68.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology, 7*(2), 163-184.

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*, 2366-2375.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives, 23*(3), 3-20.

Neter, J., Wasserman, W., & Kutner, M. H. (1989). *Applied Linear Regression Models*. Homewood, IL: Irwin.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Nunes, J. A. W., Wallston, K. A., Eden, S. K., Shintani, A. K., Ikizler, T. A., & Cavanaugh, K. L. (2011). Associations among perceived and objective disease knowledge and satisfaction with physician communication in patients with chronic kidney disease. *Kidney International, 80*(12), 1344-1351.

O'Brien, H. L., & Lebow, M. (2013). Mixed-methods approach to measuring user experience in online news interactions. *Journal of the American Society for Information Science and Technology, 64*(8), 1543-1556.

Osborne, J. (2005). Notes on the use of data transformations. *Practical Assessment, Research and Evaluation, 9*(1), 42-50.

Paek, H.-J., Pan, Z., Sun, Y., Abisaid, J., & Houden, D. (2005). The third-person perception as social judgment An exploration of social distance and uncertainty in perceived effects of political attack ads. *Communication Research, 32*(2), 143-170.

Pan, Y., & Jackson, R. T. (2008). Ethnic difference in the relationship between acute inflammation and serum ferritin in US adult males. *Epidemiology and Infection, 136*(03), 421-431.

Parrillo, V. N., & Donoghue, C. (2005). Updating the Bogardus social distance studies: A new national survey. *The Social Science Journal, 42*(2), 257-271.

Paul, B., Salwen, M. B., & Dupagne, M. (2000). The third-person effect: A meta-analysis of the perceptual hypothesis. *Mass Communication & Society, 3*(1), 57-85.

Pearce, K. E., & Rice, R. E. (2013). Digital divides from access to activities: comparing mobile and personal computer internet users. *Journal of Communication, 63*(4), 721-744.

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing, 67*(2), 1-18.

Perloff, R. M. (1989). Ego-involvement and the third person effect of televised news coverage. *Communication Research, 16*(2), 236-262.

Perloff, R. M. (1999). The third person effect: A critical review and synthesis. *Media Psychology, 1*(4), 353-378.

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

PEW Research Center. (2017). Internet/Broadband Fact Sheet. Retrieved from http://www.pewinternet.org/fact-sheet/internet-broadband/

Pilotta, J. J., Schultz, D. E., Drenik, G., & Rist, P. (2004). Simultaneous media usage: A critical consumer orientation to media planning. *Journal of Consumer Behaviour, 3*(3), 285-292.

Plotnikoff, R. C., & Higginbotham, N. (1998). Protection motivation theory and the prediction of exercise and low-fat diet behaviours among Australian cardiac patients. *Psychology and Health, 13*(3), 411-429.

Plotnikoff, R. C., Trinh, L., Courneya, K. S., Karunamuni, N., & Sigal, R. J. (2009). Predictors of aerobic physical activity and resistance training among Canadian adults with type 2 diabetes: An application of the Protection Motivation Theory. *Psychology of Sport and Exercise, 10*(3), 320-328.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Price, V., Huang, L.-N., & Tewksbury, D. (1997). Third-person effects of news coverage: Orientations toward media. *Journalism & Mass Communication Quarterly, 74*(3), 525-540.

Price, V., & Tewksbury, D. (1996). Measuring the third-person effect of news: The impact of question order, contrast and knowledge. *International Journal of Public Opinion Research, 8*(2), 120-141.

Randolph, W., & Viswanath, K. (2004). Lessons learned from public health mass media campaigns: marketing health in a crowded media world. *Annual Review of Public Health, 25*, 419-437.

Razali, N. M., & Wah, Y. B. (2011). Power comparisons of shapiro-wilk, kolmogorov-smirnov, lilliefors and anderson-darling tests. *Journal of Statistical Modeling and Analytics, 2*(1), 21-33.

Reese, R. J., Gillaspy, J. A., Owen, J. J., Flora, K. L., Cunningham, L. C., Archie, D., & Marsden, T. (2013). The influence of demand characteristics and social desirability on clients' ratings of the therapeutic alliance. *Journal of Clinical Psychology, 69*(7), 696-709.

Reid, M., Luxton, S., & Mavondo, F. (2005). The relationship between integrated marketing communication, market orientation, and brand orientation. *Journal of Advertising, 34*(4), 11-23.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime & Delinquency, 50*(2), 216-238.

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

Rogerson, P. A. (2001). *Statistical methods for geography*. London, UK: Sage.

Rojas, H., Shah, D. V., & Faber, R. J. (1996). For the good of others: Censorship and the third-person effect. *International Journal of Public Opinion Research, 8*(2), 163-186.

Rucinski, D., & Salmon, C. T. (1990). The 'other'as the vulnerable voter: A study of the third-person effect in the 1988 US presidential campaign. *International Journal of Public Opinion Research, 2*(4), 345-368.

Salkind, N. J. (1997). *Exploring research* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Salu, A. O. (2004). Online crimes and advance fee fraud in Nigeria. Are available legal remedies adequate? *Journal of Money Laundering Control, 8*(2), 159-167.

Salwen, M. B. (1998). Perceptions of media influence and support for censorship the third-person effect in the 1996 presidential election. *Communication Research, 25*(3), 259-285.

Salwen, M. B., & Driscoll, P. D. (1997). Consequences of third-person perception in support of press restrictions in the OJ Simpson trial. *Journal of Communication, 47*(2), 60-78.

Salwen, M. B., & Dupagne, M. (2001). Third-person perception of television violence: The role of self-perceived knowledge. *Media Psychology, 3*(3), 211-236.

Sherif, M. (1958). Superordinate goals in the reduction of intergroup conflict. *American Journal of Sociology, 63*(4), 349-356.

Singh, D. P. (2014). Online Shopping Motivations, Information Search, and Shopping Intentions in an Emerging Economy. *The East Asian Journal of Business Management, 4*(3), 5-12.

Stevens, W., Thorogood, M., & Kayikki, S. (2002). Cost-effectiveness of a community anti-smoking campaign targeted at a high risk group in London. *Health Promotion International, 17*(1), 43-50.

Svenson, O. (1981). Are we all less risky and more skillful than our fellow drivers? *Acta Psychologica, 47*(2), 143-148.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Boston: Pearson.

Taylor, S. E., & Lobel, M. (1989). Social comparison activity under threat: downward evaluation and upward contacts. *Psychological Review, 96*(4), 569.

Tewksbury, D., Moy, P., & Weis, D. S. (2004). Preparations for Y2K: Revisiting the behavioral component of the third-person effect. *Journal of Communication, 54*(1), 138-155.

Thomas, R., & Martin, J. (2006). The underground economy: priceless. *USENIX & SAGE, 31*(6), 7-16.

Tiedge, J. T., Silverblatt, A., Havice, M. J., & Rosenfeld, R. (1991). Discrepancy between perceived first-person and perceived third-person mass media effects. *Journalism & Mass Communication Quarterly, 68*(1-2), 141-154.

Tsfati, Y., & Cohen, J. (2003). On the effect of the "third-person effect": Perceived influence of media coverage and residential mobility intentions. *Journal of Communication, 53*(4), 711-727.

Tyler, T. R., & Cook, F. L. (1984). The mass media and judgments of risk: Distinguishing impact on personal and societal level judgments. *Journal of Personality and Social Psychology, 47*(4), 693-708.

U.S Census Bureau. (2017). Quick facts.   Retrieved from https://www.census.gov/

Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Computers in Human Behavior, 51*, 180-187.

Wainer, J., Dabbish, L., & Kraut, R. (2011). *Should I open this email? Inbox-level cues, curiosity and attention to email.* Paper presented at the Proceedings of the SIGCHI conference on human factors in computing systems, Vancouver, CA.

Wan, F., & Youn, S. (2004). Motivations to regulate online gambling and violent game sites: An account of the third-person effect. *Journal of Interactive Advertising, 5*(1), 46-59.

Watson, N., Clarkson, J., Donovan, R., & Giles-Corti, B. (2003). Filthy or fashionable? Young people's perceptions of smoking in the media. *Health Education Research, 18*(5), 554-567.

Webster, J. G. (2005). Beneath the veneer of fragmentation: Television audience polarization in a multichannel world. *Journal of Communication, 55*(2), 366-382.

Wei, F.-Y. F., Wang, Y. K., & Fass, W. (2014). An experimental study of online chatting and notetaking techniques on college students' cognitive learning from a lecture. *Computers in Human Behavior, 34*, 148-156.

White, H. A. (1997). Considering interacting factors in the third-person effect: Argument strength and social distance. *Journalism & Mass Communication Quarterly, 74*(3), 557-564.

Wills, T. A. (1981). Downward comparison principles in social psychology. *Psychological Bulletin, 90*(2), 245-271.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs, 61*(2), 113-134.

Wright, K. B. (2005). Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication, 10*(3), 00-00.

Wu, W., & Koo, S. H. (2001). Perceived effects of sexually explicit Internet content: The third-person effect in Singapore. *Journalism & Mass Communication Quarterly, 78*(2), 260-274.

Xu, J., & Gonzenbach, W. J. (2008). Does a perceptual discrepancy lead to action? A meta-analysis of the behavioral component of the third-person effect. *International Journal of Public Opinion Research, 20*(3), 375-385.

Yip, J. J., & Kelly, A. E. (2013). Upward and downward social comparisons can decrease prosocial behavior. *Journal of Applied Social Psychology, 43*(3), 591-602.

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

Youn, S., Faber, R. J., & Shah, D. V. (2000). Restricting gambling advertising and the third-person effect. *Psychology and Marketing, 17*(7), 633-649.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior, 11*(6), 763-765.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500.

Zahedi, F. M., Abbasi, A., & Yan, C. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems, 16*(6), 448-484.

Zebrowitz, L. A. (1990). *Social percpetion*. Pacific Grove, CA: Brooks/Cole.

APPENDIX A. SURVEY QUESTIONNAIRE

Control Variables

a. GENDER

ITEM: What is your gender?

RESPONSES: 0=female, 1=male

b. HOUSEHOLD INCOME

ITEM: What is the estimated annual household income?

RESPONSES: 1=less than $20,000, 2=$20,000 to $40,000, 3=$40,001 to

$60,000,

4=$60,001 to $80,000, 5=$80,001 to $100,000, 6=more than $100,000

c. ETHNICITY

i. ITEM 1: Do you identify yourself as Hispanic?

RESPONSES: 1=Yes, 2=No

ii. ITEM 2: How you identify your ethnicity?

RESPONSES: 1=White, 2=Black, 3=Asian, 4=Mixed Race, 5=Other Race

d. EDUCATION

ITEM: What is your education level?

RESPONSES: 1=some grade school, 2=some high school, 3=high school

graduate, 4=technical or vocational school, 5=some college, 6=college graduate,

7=graduate/professional degree

e. AGE

ITEM: What is your age?

RESPONSES: This is an open answer question.

f. EMPLOYMENT

ITEM: What is your employment status?

RESPONSES: 1=not employed, 2=part time employed, 3=full time employed

Independent Variables and Dependent Variables

a. PERCEIVED INTERNET PRIVACY RISKS

i. ITEM 1: How much do you think your Internet privacy is at risk?

ii. ITEM 2: How much do you think other people's Internet privacy is at risk

iii. RESPONSES: 1 (no risk at all) to 7 (great risk).

b. BEHAVIORAL COMPONENT OF TPE

i. ITEM 1: In the future, would you recommend the online privacy protection

measures to others?

ii. ITEM 2: In the future, would you adopt privacy protection measures by

yourself?

iii. RESPONSES: 1 (strongly disagree) to 7 (strongly agree).

c. UNDESIRABILITY (PERCEIVED SEVERITY & VULNERABILITY)

Do you agree with the following statements?

i. ITEM 1: I believe that losing information privacy through Internet would be a

serious problem for me.

ii. ITEM 2: Having my online identity stolen through Internet would be a serious problem.

iii. ITEM 3: Losing photo privacy online would be a serious problem.

iv. ITEM 4: Unauthorized access into my personal account, such as social networking sites, personal financial account, would be a serious problem to me.

v. RESPONSES: 1 (strongly disagree) to 7 (strongly agree)

d. PERCEIVED INTERNET PRIVACY KNOWLEDGE

Do you think you know the following Internet privacy risks?

i. ITEM 1: Virus attack

ii. ITEM 2: Hacker attack

iii. ITEM 3: Identification theft

iv. ITEM 4: Credit card theft

v. ITEM 5: Privacy invasion

vi. ITEM 6: Online insult

vii. RESPONSES: 1 (do not know at all) to 7 (very familiar)

e. NEGATIVE INTERNET PRIVACY EXPERIENCES

Do you have the following experiences?

i. ITEM 1: Being stolen of financial accounts, which results in monetary losses

ii. ITEM 2: Being a victim of Internet scams.

iii. ITEM 3: Receiving unwanted commercial advertisements from unknown sources through emails.

iv. ITEM 4: Receiving unwanted commercial advertisements from unknown sources through social media.

v. ITEM 5: The unauthorized access into personal social media accounts

vi. ITEM 6: The unauthorized postings on SNSs results in damaged reputation

vii. ITEM 7: The unauthorized postings on SNSs results in relational conflicts

viii. ITEM 8: The unauthorized postings on SNSs results in losing of job opportunities

ix. ITEM 9: The experiences of online harassment

x. ITEM 10: The experiences of receiving unwanted friend requests

xi. RESPONSES: 0=never, 1=once, 2=twice, 3=three times, 4=four times, 5=five times, 6=six times, 7=seven times or more

f. INTERNET USE

i. ITEM 1: How often do you search useful information online?

ii. ITEM 2: How often do you read news online?

iii. ITEM 3: How often do you shop online?

iv. ITEM 4: How often do you play games online?

v. ITEM 5: How often do you use online chatting?

vi. ITEM 6: How often do you use social media?

vii. RESPONSES: 1 (never) to 7 (very often)

APPENDIX B. VITA

Hongliang Chen received his Bachelors of Arts degree in Communication at China Agricultural University in 2011, his Masters of Arts in Communication at The University of Connecticut in 2013, and his Doctor of Philosophy in Communication from Texas A&M University in 2017. He studies communication technology using survey research methods. Hongliang is particularly interested in cybersecurity, interpersonal interactions online, global media technology diffusion, Internet pornography, and health media campaign.

Hongliang can be reached at the Department of Communication, Texas A&M University. His email address is tamuhlc@tamu.edu.