2019

Understanding Ecommerce Consumer Privacy From the Behavioral Marketers' Viewpoint

Brenda Ivory Jones
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Brenda Ivory

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Thomas Schaefer, Committee Chairperson, Doctor of Business Administration
Faculty

Dr. James Glenn, Committee Member, Doctor of Business Administration Faculty

Dr. Janet Booker, University Reviewer, Doctor of Business Administration Faculty

The Office of the Provost

Walden University
2019

Abstract

Understanding Ecommerce Consumer Privacy From the Behavioral Marketers'

Viewpoint

by

Brenda Ivory

MBA, University of New Haven, 1992

MS, Rennselaer at Hartford, 2002

BS, Western New England University, 1979

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2019

Abstract

Ecommerce sales were expected to increase to $4.8 trillion dollars in 2021 for online retailers in the United States. Behavioral marketers increase sales and revenue by targeting potential customers based on the use of ecommerce consumers' personal information. This correlational research study was framed with the theory of planned behavior. The participants were behavioral marketers based in the United States who completed an online survey. The data were analyzed using multiple regressions and analysis of variance analyses to answer the research question. The results of the analysis answered the research question regarding the correlation between behavioral marketer's attitudes, social norms, and perceived behavioral control (PBC), especially concerning the collection of ecommerce consumers' personal information. The results of the analyses indicated attitude is a strong predictor for behavior intention, as indicated by a positive correlation. The ρ value was greater than .05; therefore, the null hypothesis was rejected. The social norms and PBC variables were not significant. Social norms resulted in $F (14,18) = 2.298$, $\rho = .026$. The p value is less than .05; therefore, the null hypothesis was accepted. PBC results were $F (78,5) = 4.263$, $\rho = .048$. The p value was less than .05; therefore, the null hypothesis was accepted. The findings showed that behavioral marketers have a strong correlation between their attitude and intention to protect ecommerce privacy. Behavioral managers might benefit from this study and contribute to social change by taking the lead in their organizations to change data collection methods to reduce the number of security breaches.

Understanding Ecommerce Consumer Privacy From the Behavioral Marketers'

Viewpoint

by

Brenda Ivory

MBA, University of New Haven, 1992

MS, Rennselaer at Hartford, 2002

BS, Western New England University, 1979

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2019

Dedication

I dedicate this DBA study to my best friend, my husband, Ronnie. I could not have accomplished this task without your love and support. Your encouragement motivated and energized me at the low points of the DBA process. I appreciate the sacrifices you made so I could spend time at the library.

Acknowledgments

I want to acknowledge my village. First, my family members and friends who understood my time commitment to this DBA study. I missed many special occasions and events. This was a long journey made possible by the understanding and assistance of my husband, son, and granddaughters. Second, my Walden University community: Dr. Thomas Schaefer as my committee chair you provided guidance and the encouragement, I needed to complete my DBA journey. Dr. James Glenn and Dr. Janet Booker thank-you for your commitment to excellence. Third, I want to acknowledge the D 'Amour library staff at Western New England University. I spent many hours on the second level writing my DBA study. Fourth, the members of the American Marketing Association were instrumental with launching my survey. Finally, I thank my Lord and Savior for giving me the courage to continue, when I had every reason to quit.

Table of Contents

iii

List of Tables

List of Figures

Section 1: Foundation of the Study

The study of consumer privacy is not a new topic for behavioral marketing managers, although the subject is complex due to the various definitions of privacy. Using the theory of planned behavior (TPB), I examined the issue of privacy for ecommerce consumers from the behavioral marketer's perspectives. Understanding the methods that behavioral marketing managers use to collect and store customer data and the importance placed on protecting the data were relevant to this study. Mishandling data may result in a security breach. Security breaches are costly to the organization the ecommerce consumer.

The topic of ecommerce privacy is relevant as an increasing number of consumers use the Internet to purchase products and services. In 2017, ecommerce sales increased $2.3 trillion USD, with a project increase of $4.8 trillion by 2021 (Statista, 2019). Behavioral marketers not focused on ecommerce consumer privacy may lose sales and loyal customers as the result of a security breach (Kude, Hoehle, & Sykes, 2017). Security breaches negatively affect the revenue and profits of the organization.

Background of the Problem

Behavioral marketing is the advertising process of targeting the consumer population based on an interest or topic (Milne Pettinico, Hajjat, & Markos, 2017). Targeting ecommerce consumers requires the collection, use, and sale of personal information (Milne et al., 2017). This relatively new phenomenon brings value and a competitive edge to the marketer's organization (Martin, 2016). Behavioral marketers increase sales and revenue by targeting potential customers based on the use of the

ecommerce consumer's personal information (Todor, 2016). The problem with the process of targeting consumers was the collection of personal information and the threat of a security breach. A security breach may decrease sales and revenue for the organization. Behavioral marketers must balance the benefits of targeted marketing with the risks to the consumer (Libaque-Saenz, Chang, Kim, Park, & Rho, 2016).

Behavioral marketing offers many benefits to the marketer, as an advertising strategy to increase revenue (Wu, Ke, & Nguyen, 2018). The online sales growth potential renders the phenomenon of behavioral marketing as profitable for the behavioral marketer (Todor, 2016). Behavioral marketers design advertising strategies to increase sales. Increased sales were the goal of targeted advertising (Wu et al., 2018). The results of this research project may add to the literature on ecommerce consumer privacy through the marketing lens of the behavioral marketer. Unlike previous ecommerce privacy concerns, which offer the ecommerce consumer's point of view, in this study, I focused on the viewpoint of the behavioral marketer.

Problem Statement

Although behavior marketing is a profitable low-cost advertising method, when compared with traditional marketing methods, there may be a threat of security breach, for organizations (Milne et al., 2017). In 2014, data breaches cost the organization approximately $5.9 million per incident (Sen & Borle, 2015). The general business problem that I addressed in this study is that behavioral marketers may have placed more importance on organizational profits than the risk of a security breach (Choong, Hutton, Richardson, & Rinaldo, 2017). The specific business problem that I addressed is that

some behavioral marketers may not understand the correlation social norms, and PBC concerning the collection of ecommerce consumer's personal information, resulting in a possible security breach.

Purpose Statement

The purpose of this quantitative correlational study was to examine the correlation between the behavioral marketer's intention to protect ecommerce privacy, as it relates to their attitude, SNs, and PBC, as measured by the TPB tool regarding the collection of ecommerce consumer's personal information. The dependent variable was the behavioral marketer's intention to protect ecommerce consumer privacy. The independent variables include the behavioral marketer's attitude, SNs, and PBC. The targeted population for this study was behavioral marketing managers from the American Marketing Association (AMA) located in the USA. A study of privacy from the behavioral marketer's viewpoint within ecommerce organizations was meaningful based on the expected growth of ecommerce sales and the risk of a security breach (Milne et al., 2017; Sen & Borle, 2015). In this study, I have contributed to social change by helping marketing leaders understand the correlation between their attitudes, SNs, and PBC concerning an organization's ecommerce information collection processes. This awareness may lead to strategies, which reduce the amount of information collected or policies to safeguard the consumer's personal information.

Nature of the Study

In this research study, I used input from the behavioral marketing manager's perspective to determine the importance of ecommerce privacy and the degree of

relationship between the dependent and independent variables. The selected research

method must be appropriate to answer the research question (Sukamolson, 2016).

Conducting quantitative and qualitative research studies provides answers to phenomena

related questions, but researchers can convert the data into numerical values, which allow

statistical analysis in quantitative designs (Sukamolson, 2016). The quantitative approach

allows the representative population to provide responses not readily available from other

sources (Sukamolson, 2016). Qualitative designs give meaning to the data from a

personal perspective with face-to-face interviews and participant observations, which

leads to the identification of trends (Echambadi, Campbell, & Agarwal, 2006). The

identification of trends in the data assists the researcher with conclusions. Qualitative

research was beneficial for a study when the researcher desires to add flexibility and have

direct contact with the study population (Farah, 2017). The direct contact of qualitative

research was useful in understanding phenomena. Echambadi et al. (2006) wrote that

researchers using a quantitative design alone might miss essential elements of the

phenomena due to bias and incomplete conclusions. A mixed methods approach may

bring out the best in both methods. Mixed methods have the capacity to answer more than

one type of research question (Frels & Onwuegbuzie, 2013). Echambadi et al. (2006)

suggested that researchers look for opportunities to combine qualitative and quantitative

methods. A mixed methods approach will allow researchers to identify new variables, not

studied in previous research (Echambadi et al., 2006). The three methodologies,

quantitative, qualitative, and mixed methods have merit but the best research design

allows the researcher to answer the research question successfully. I eliminated

qualitative and mixed methods because the two methodologies did not meet the need of the research question, which establishes the relationship between variables. The research question for this study renders quantitative methods the best methodology for this research project.

The research design was the method of collecting data (Sukamolson, 2016). Several designs exist for collecting data. The designs include survey research, correlational, experimental, and causal-comparative research (Vogt, Gardner, & Haeffele, 2014). A correlational nonexperimental design is most common in social and behavioral studies, when the researcher examines the participant's attitudes, beliefs, or values (Vogt et al.). The correlational design allows researchers to make comparisons between the constructs and was useful for predicting an outcome from one or more variables (Sukamolson, 2016). Ajzen and Sheikh (2013) were successful in predicting behavioral intentions with a correlational design. My purpose in this study was to predict the behavioral marketer's intention toward ecommerce consumer privacy based on their attitude, SNs, and PBC. A correlational design was appropriate for this study based on predicting the behavioral marketer's intention to protect ecommerce consumer privacy.

Research Question

The data from the research question for this doctoral study may provide knowledge of the behavioral marketer's role in maintaining the ecommerce consumer privacy by understanding the manager's behavioral intentions using the TPB. The primary research question was:

What was the correlation between behavioral marketer's attitudes, SNs, and PBC, regarding the collection of ecommerce consumer's personal information?

Hypotheses

H_{01}: There was not a significant correlation between the behavioral marketer's attitudes concerning the collection of ecommerce consumer's personal information.

H_{a1}: There was a significant correlation between the behavioral marketer's attitudes concerning the collection of ecommerce consumer's personal information.

H_{02}: There was not a significant correlation between the behavioral marketer's SNs concerning the collection of ecommerce consumer's personal information.

H_{a2}: There was a significant correlation between the behavioral marketer's SNs concerning the collection of ecommerce consumer's personal information.

H_{03}: There was not a significant correlation between the behavioral marketer's PBCs concerning the collection of ecommerce consumer's personal information.

H_{a3}: There was a significant correlation between the behavioral marketer's PBCs concerning the collection of ecommerce consumer's personal information.

Theoretical or Conceptual Framework

The theoretical framework for this study was the TPB first introduced by Ajzen (2011), in the 1980s. The TPB is an expanded construct of Ajzen's theory of reasoned action (TRA) (Ajzen & Sheikh, 2013). Ajzen identified an individual's propensity to perform a behavior, determined by the individual's SNs and their behavioral intent (BI), or attitude toward the behavior with TRA (Ajzen & Sheikh, 2013). Building on the TRA, Ajzen (1991) added PBC. PBC is the best predictor of future behavior (Ajzen, 1991). The

behavioral manger's attitudes, SNs, PBCs, and their intention to protect ecommerce consumer privacy was the focus of this study. The TPB variables, attitude, SNs, and PBC form the foundation of this study. Although previous researchers used the TPB to study psychological and health care issues, use of the TPB helped understand the intentions of behavioral marketers.

The TPB has more applications in the psychological and health care industry (Ajzen & Sheikh, 2013). Ajzen and Sheikh (2013) used TPB to understand individual behavior in the social science industries with excellent results. In the business world, TPB was a reliable predictor of online managerial behavior when behavior was volitional and the manager has the required information to form a stable online decision (Shin & Hancer, 2016). The TPB was useful for understanding online consumer behavior. Choong et al. (2017) used the TPB to identify ecommerce, privacy protection measures. Choong et al. revealed that 47% of ecommerce consumers expressed concern about their privacy in ecommerce applications. Applying the TPB to the current study contributed to the literature of ecommerce consumer's privacy with the collection, use, and sale of personal information by providing behavioral marketers additional insight into consumer's future ecommerce behavior. The principles of TPB provided behavioral marketer's introspection into their future behavioral intention and increased their understanding of safeguarding consumer privacy by reducing the collection, use, and sale of personal information.

Operational Definitions

Several terms were specific to the study of ecommerce privacy concerns. Definition of the key terms will aid in the understanding of this study. The terms used throughout this study listed in this section.

Behavioral intention: *Behavioral intention* is a predictor of behavior when the behavior is volitional, and the individual has the information to decide. (Kammer, Niessen, Schmid, & Schwendener, 2016).

Behavioral marketing: *Behavioral marketing* is the systematic process of collecting, storing, and selling personal information for use in targeting consumers. The practice of collecting and storing online consumer information for targeting advertisements for products or services, based on browsing history (Milne et al., 2017).

PBC: *PBC* represents a manager's perception of entering into strategic agreements as a representative of their firm or organization and the availability of resources (Kassim, Arokiasamy, Isa, & Ping, 2017).

Personal Information: Information, which directly or indirectly identify an individual. Personal information includes IP address, digital footprint, location, and online profile (Goddard, 2017).

Privacy concern: Ecommerce privacy concern is the unknown outcome of the collection and use of personal information (Milne et al., 2017).

Privacy paradox: *Privacy paradox* is the complex situation where consumers desire privacy in online settings but will provide personal information in exchange for a reward (Dienlin & Trepte, 2015; Lwin, Wirtz, & Stanaland, 2016).

Privacy violation: *Privacy violation* is the act of collecting, using, and selling an individual's personal information without the consent or knowledge, resulting in harm to the individual (Milne et al., 2017).

Right to privacy: The ability to control privacy by requesting marketers not collect, use, or sell personal information, to third parties (Walsh, Parisi, & Passerini, 2017).

SNs: Subjective or social norms are the effect reference groups have on the decision-making process (Kammer et al., 2016).

Assumptions, Limitations, and Delimitations

Assumptions, limitations, and delimitations were the parameters of the research study. They include the unverified truths or assumptions, the weak areas or limitations of the study and the boundaries or delimitations of the study. Together, assumptions, limitations, and delimitations set the expectations of the research study.

Assumptions

The assumptions of this study were concepts accepted as truths not but not verified (Simon, 2011). Leedy and Ormrod (2010) stated that assumptions are the basis of a doctoral study. The first assumption that I made was the population of behavioral marketing managers responding to the survey will possess the information required to answer the questionnaires truthfully. A second assumption that I made was the number of valid survey responses will result in a sample size representative of the population of behavioral marketing managers. Research validity depends on the response rate of the questionnaires (Vogt et al., 2014). A high response rate yields a sample size

representative of the population. The third assumption that I made was consumer privacy

concerns were important to behavioral marketers. The importance of consumer privacy

research in the literature focused on the consumer. The topic of this research study on

consumer privacy concentrated on the managerial perspective.

Limitations

The limitations of a study are the things that the researcher cannot control, which

may affect the validly of the research (Simon, 2011). Essentially, limitations are the weak

points of the research study. The first limitation based on the TPB was, that knowledge is

not a consistent predictor of behavior (Ajzen, 2011). A manager may be aware of a

knowledge point but choose to ignore it if his or her actions negatively affect

organizational profits. The second limitation was the anonymity of the survey responses.

The respondents or participants represented several industries. Focusing on one industry

may produce different results. For example, behavioral marketers within the elevator

industry may have a different perspective on privacy concern compared to the behavioral

marketer representing an online retailer. Related to industry was the geographic region.

Concentrating on one geographic region outside of the USA will yield different results.

Behavioral marketers in European countries have different viewpoints of privacy (Fortes

& Rita, 2016). Third, the TPB specific variable, attitude, SNs, or PBC, which will

motivate behavioral marketing managers to protect personal information online was

unknown. Fourth, there was not a concrete definition of privacy. Previous researchers

used differing terminology for the same privacy concepts (Milne et al., 2017). For the

purpose of this study, I defined *consumer privacy* as the privacy the behavioral marketers

can affect, by their information collection, use, and sale strategies. Last, there was a 2-week time constraint for collecting data. The populations of marketing managers are busy and many may delete the survey link without opening. This action may influence the number of qualified survey results returned.

Delimitations

Delimitations shape the structure of a research study. The delimitations function as the boundaries of the study (Leedy & Ormrod, 2010). The first delimitation was the defined specific problem (Simon, 2011). Some behavioral marketers may not realize the relationship between their attitudes, SNs, and perceived behavior toward the protection of ecommerce consumer privacy, resulting in possible security breach (Shin & Hancer, 2016). The target population of this study includes marketing managers with knowledge of targeted or behavioral advertising and will not include ecommerce consumers who are not behavioral marketers. The behavioral marketers with ecommerce behavioral marketing experience are the subject of this study regardless of their years of experience or size of their organization. Behavioral marketers from a large behavioral marketing organization, such as Amazon or Target may yield different results (Craciun, 2018).

My focus in this study was the behavioral intention of ecommerce or behavioral marketing managers on protecting ecommerce consumer's online privacy. The participants, behavioral marketers form the boundaries of this research. I included behavioral marketing managers who have experience with targeted advertising and collecting, storing, and selling consumer's personal information in the study. Behavioral marketing managers who have experience with targeted advertising and collecting,

storing, and selling consumer's personal information were included in the study. Behavioral marketing managers who were members of the AMA, within the USA received a survey. Surveys distributed directly to behavioral marketing managers using their company email address may yield different results. The results may vary in the number of surveys returned, due to changes in job classifications, promotions resulting in a different marketing role, and email message recognized as spam.

Significance of the Study

The growth of ecommerce provides the backdrop for a study of ecommerce privacy from the behavior marketer's perspective. Increased sales from the use of ecommerce consumer's personal information were the driving force for behavior marketers (Wu et al., 2018). At the same time, concern for consumer privacy should also be a factor to prevent a possible security breach.

A limited amount of literature was available concerning the behavioral marketer's role in protecting consumer privacy. As a relatively new phenomenon, most of the information readily available concerning ecommerce consumer privacy was from the ecommerce consumer's perspective (Kude et al., 2017). The significance of this study was the importance of ecommerce privacy from the behavioral marketer's point of view. The amount of ecommerce privacy information from the behavioral marketer's perspective was limited. As the number of ecommerce platforms continues to grow, the rise in ecommerce sites prompted a need to understand the behavioral marketer's perspective on ecommerce privacy (Kude et al., 2017). The results of this doctoral study may add to the limited research on ecommerce consumer privacy from the behavioral

marketer's perspective. The results of this research may lead to an increased knowledge of the behavioral marketer's attitude, SNs, and PBC concerning the collection of ecommerce consumer's personal information as this relates to ecommerce privacy.

Contribution to Business Practice

The growth of online shopping necessitates behavioral marketers understand and operate within the consumer privacy concern. Statista (2019) listed ecommerce sales in North America at 8.1% of global sales. The acceptance of social media and the amount of personal information on social media led scholars to suggest privacy was dead, and privacy concern was not relevant to ecommerce consumers (Weinberg, Milne, Andonova, & Hajjat, 2015). An effective behavioral marketing strategy will continue to increase revenue and profits for the organization without putting the ecommerce consumer at considerable risk of a security breach (Choong et al., 2017). The results of this study provided insight into the correlation between the behavioral marketer's attitude, SNs, and PBC concerning the collection of ecommerce consumer's personal information and ecommerce privacy. In short, this study provided insight into the importance behavioral marketers place on ecommerce privacy.

Implications for Social Change

The social implication of this study provided behavioral marketers an increased awareness of the ecommerce consumer privacy based on the collection of personal information. Behavioral marketer's attitude, SNs, and PBC as measured by the degree of importance placed on ecommerce privacy determines if the ecommerce organization was at high risk for a security breach. Behavioral marketers may align this awareness to the

profits and revenue of ecommerce transactions and take the appropriate action to protect the collected personal information. This awareness and subsequent action may prevent future security breaches. Social change aligned with shareholder interests has a greater chance for implementation (Sonenshein, 2016). An awareness of consumer privacy concerns with the collection of personal information assisted with differentiating an organization's ecommerce site from the ecommerce sites, which choose not to address consumer privacy concerns about the collection of personal data (Weinberg et al., 2015). Consumers will be more willing to provide personal information, and shop, if behavioral marketers were actively pursuing safeguards to protect ecommerce consumer's personal information (Acquisti, Taylor, & Wagman, 2016). Increased knowledge of behavioral marketer's attitude, SNs, and PBC toward the collection, and use of personal information drove social change through behavioral marketer's intentions.

A Review of the Professional and Academic Literature

My purpose in this quantitative correlational study was to understand the strategic intention of behavioral marketing managers when developing ecommerce advertising strategies, which collect, use, and sell ecommerce consumer's personal information. The process of collecting, using, and selling ecommerce consumer's personal information may put the information at risk for a security breach. Using TPB to frame the study, I examined the behavioral marketer's strategic intentions to understand the attitudes, social norms, and perceived behavioral control of the marketing manager. Studying the attitudes, social norms, and perceived behavioral control of the marketing manager who develop targeted ads with ecommerce consumer's personal information will add to the

existing literature. The results of this study contributed to the existing literature by adding

the element of consumer privacy, from the behavioral marketing manager's perspective.

This literature review was composed of references from three subject areas,

behavioral marketing, ecommerce consumer privacy, and the TPB. Together the articles

allowed an in-depth study of the concepts of ecommerce behaviors, attitudes, intention,

and ecommerce consumer's privacy concerns. The literature retrieved from electronic

database searches including Business Source Complete, ABI/INFORMS Complete,

Emerald Management, Sage Premier, and PsycINFO comprised most of the references.

The keywords included *consumer privacy, the theory of planned behavior, behavior*

marketing, target marketing, digital privacy, database marketing, Internet marketing,

personalized advertising, identity marketing, market research, online advertising, the

theory of reasoned action, and ecommerce transactions for years 2006 to 2019. The

collection of peer-reviewed journals collectively addresses the role of behavioral

marketers and their attitude, social norms, and PBC regarding ecommerce consumer

privacy concerns, ecommerce consumer privacy, and TPB, which frames this study. This

study includes 89% peer reviewed studies published within 5 years of CAO approval.

This literature review consists of 76 peer-reviewed articles.

TPB has limited applications in the ecommerce industry. The TPB theory evolved

from the psychology and health care construct thus identifying a gap in the literature and

a need for further study in the ecommerce environment. The limited information for TPB,

applications in ecommerce, and business decisions necessitated this literature review to

consist of three major sections. The three sections include the TPB framework, the

importance of consumer privacy, and behavioral marketing as a strategy. Each of the major areas includes a history and current state of the topic.

The Theory of Planned Behavior

The TPB was the theoretical framework used to study the behavioral marketer's future intentions toward consumer privacy on ecommerce sites. According to the TPB an individual's intention toward an action consists of three constructs; attitude, SNs, and PBC (Ajzen & Sheikh, 2013). Central to the theory was an individual's capability to perform the action (Shin & Hancer, 2016). Shin and Hancer (2016) stated that perceived behavioral control was an individual's confidence that he or she can perform the action. The focus of this study was twofold; the importance placed on behavioral marketer's role in protecting consumer privacy and the behavioral marketer's capacity to make the necessary changes to protect ecommerce consumer privacy. Behavioral marketers may understand the importance of protecting ecommerce consumer privacy and have a positive attitude toward TPB but lack the capacity to make changes.

The TPB was a reliable fit for this study. It has predictive validity for determining how an individual will perform a future action based on attitude, social norms, and PBC (Shin & Hancer, 2016). The behavioral marketer's intentions toward ecommerce privacy were necessary to answer the research question. TPB helped to understand how the behavioral marketer's attitude, social norms, and perceived behavior influence the marketer's intention. Behavioral marketers were instrumental in designing protective privacy controls in the initial phases of the ad design process. What was not clear is the

importance behavioral marketer's place on ecommerce privacy and the need to protect the privacy from security breaches.

Ajzen (1991) developed the TPB, from the TRA, which had more applications in social and behavior research. Ajzen stated that an individual's intention depends on the individual's attitude toward the behavior and the SNs within TRA (Ajzen, 2011). Users of the TRA tool measured an individual's intention to perform a behavior with the person's attitude as the barometer of the behavior's importance (Woolley, 2015). TPB had an additional component, PCB. Ajzen (2011) defined *PCB* as the perceived capability of performing the behavior or action and assumed the effect of prior experiences. Kassim et al. (2017) stated PCB was a significant factor in predicting intention. Based on the TPB an individual's behavioral intention was dependent on attitude, SNs, and perceived behavioral control (Ajzen, 2014;).

Understanding the behavioral marketer's attitude toward ecommerce privacy was not enough if the capability to change was not present. Ajzen and Sheikh (2013) stated that the capacity to make changes reflects the behavioral marketer's intentions. The application of TPB to the study of ecommerce privacy was relatively new. There were many theories linked to the study of consumer privacy. The theories focused on the customer's behavior rather than the marketer's behavior.

Kassim et al. (2017) used TPB to understand car purchase decision intentions among potential car purchasers. The research results for Kassim et al. indicated social norms, reference groups, or individuals who influence decisions have a positive effect on the decision to purchase a safe car. Whereas Shin and Hancer (2016) found that PBC was

a predictor for intentions. The focus on the behavioral intention of the student population

provides insight into the decision-making process before the adoption of the behavior

(Shin & Hancer, 2016).

Fortes and Rita (2016) realized a significant correlation between ecommerce

purchase intention and a positive attitude. They concluded a positive attitude toward a

behavior leads a greater intention to participate in ecommerce. Last, Fortes and Rita

found differences in the ecommerce consumer's intention to purchase products compared

to services. Participants were less likely to purchase services online if a brick and mortar

retail store was available (Tabari & Abroud, 2017). This phenomenon was explained by

Tabari and Abroud (2017) as an adverse reaction to risk among ecommerce consumers.

Choong et al. (2017) and Fortes and Rita used a modified version of TPB survey tool to

examine online behaviors. The results indicated a positive correlation between social

norms and intention. The relationship between social norms and intention suggests

external influence affects an individual's intention to engage in a protective online

behavior. Choong et al. indicated peer influence had a positive effect on the participant's

intention to implement ecommerce protective actions. Like Choong et al., the research

studies of Fortes and Rita shared the similar results between the correlation of SNs and

the intention to perform the behavior. In each study, the SNs of the individual had a

positive impact on the behavior of the individual. Consistent with TPB, peers, and

significant relationships influence a managerial decision.

Brahmana, Brahmana, and Memarista (2018) used TPB to research psychological

drivers toward attitudes, SNs, and PBC for purchasing life insurance. The results of

Brahmana et al. revealed a positive relationship between the consumer's attitude toward purchasing health insurance and the intention to purchase. Also, Brahmana et al. found a positive correlation between the managers' PBC and their intention to purchase health insurance. In contrast, Libaque-Saenz et al. (2016) found that education and professional network influenced their social norms, for refusing to provide personal information for secondary use. Brahmana et al. suggested the social norm component of the TPB was a positive influence toward the purchase of health insurance. In each of the studies, the individual had the capability to carry out the action. Their results were consistent with the principles of the TPB; the individual must have the capacity to perform the behavior (Ajzen, 2011). Like Brahmana, the results of Hegner, Fenko, and Teravest (2017) suggested an individual's attitude significantly affected intention toward brand loyalty and their social circle provided the stimulus toward brand loyalty.

Fortes and Rita (2016) found a negative relationship between SNs and the propensity to disclose personal information in exchange for incentives or rewards, among Internet users. The results reflect the influence peers had on Internet users and the tendency to disclose personal information online (Fortes & Rita, 2016). If the peer group suggested online disclosure of personal information is safe, then the Internet users in the study would be more willing to disclose their personal information. Fortes and Rita suggested ecommerce consumers might be comfortable with disclosing personal information, but a security breach may result in negative reviews and negatively impact revenue. Seungsin, Younghee, Joing-in, and Jungkun (2015) confirmed Fortes and Rita's statement; a security breach may result in negative reviews and lost revenue, sales, and

profits. Rita and Fortes revealed the discomfort level of Internet users and publishing personal information.

Choong et al. (2017) and Fortes and Rita (2016) found a significant a relationship between the TPB variables, and the capacity to perform the behavior. Although, Chong et al. and Fortes and Rita used the TPB to frame their research they cited a positive experience, with the ability to perform the action. Along with the positive aspects of the TPB, there were limitations. Scholars used TPB research with varying results, often citing the limitations of the theory.

The shortcomings of the theory included differing viewpoints of the PCB construct, individual attitudes, and the critics of the theory. Ajzen (2011) and Han and Stoel (2017) used TPB with positive results but identified the deficiencies of the theory related to the SN construct. The subjective norm was found to be the weakest construct in the model for understanding socially responsible behavior. The inability to link behavior to the intention was fundamental with the TPB (Ajzen, 1991). The three constructs, attitude, SNs, and PBC must align with the intention, and the individual must have the capacity to perform the behavior (Ajzen & Sheikh, 2013). The essence of the perceived control component was a concern for a person's ability to follow through with the identified behavior (Ajzen & Sheikh, 2013).

Han and Stoel (2017) suggested that the TPB did not determine the beliefs associated with a defined behavior. Ajzen (2011) countered this by stating that TBP does not indicate where the beliefs originate, but the theory identified some constructs, which may influence beliefs, such as education, age, gender, income, exposure to media, and

personality. Han and Stoel identified the intention-behavior gap as a limitation of TPB. Shin & Hancer (2016) revealed the gap between intention and behavior concerning PBC, the type of behavior, and the individual's environment. This gap between intention and behavior corresponds to the participant's perception of the behavior.

An individual's perception of the behavior, whether positive or negative, was a factor between intention and behavior accomplishment, as well as the level of difficulty in performing the behavior (Ajzen & Sheikh, 2013). The intention to behavior gap may be more difficult when the sample populations were diabetics who require a diet modification (Caro-Bautista et al., 2015). The diabetic has knowledge a diet modification was required for sustained good health but may not be able to accomplish the behavior (Caro-Bautista et al., 2015). Similar to Caro-Bautista et al. (2015) Moghavvemi, Sellah, Sulaiman, and Abessi (2015) found intention alone was not a strong predictor for determining behavior. Moghavvemi et al. suggested a set of related events or changes were required for behavior changes. In addition to events or changes, Hassan, Shiu, and Shaw (2016) suggested adequate planning assists with the intention to perform a specific behavior, thus closing the behavior to intention gap. The individual's attitude was also a concern for the intention to behavior gap.

Shin and Hancer (2016) found social norms to be a shortcoming of TPB. The attitude component determines the individual's viewpoint of the behavior. The research of Shin and Hancer revealed that social norms were not significant toward the purchase of local food products and PBC to be significant influence on attitude to purchase. The attitude toward the behavior can be either positive or negative. If the attitude toward the

behavior was favorable and the intention to perform the behavior was present, then the capacity to carry out the behavior will be present (Shin & Hancer, 2016). In accordance with the TPB, an individual's attitude toward a behavior was a predictor of behavior (Ajzen & Sheikh, 2013). The attitude component relates to how an individual feel about the behavior or a tendency based on prior experience (Kammer et al., 2016). Kammer et al. (2016) found that the manager's attitude toward the behavior was a stronger indicator of behaviors compared to PBC. Shin and Hancer (2016) determined attitude were an influence on PBC.

Sniehotta, Presseau, and Araújo-Soares (2015) commented on additional variables to explain the intention to behavior gap. Sniehotta et al. indicated demographics, age, socio-economic status, and income affected the outcome of behavior. Choong et al. (2017) found demographic characteristics were insignificant in understanding the gap between intention and behavior. Age was an influencer of behavior intentions based on the behavior. Studies concerning personal information disclosure on social network sites will result in a positive correlation between age and intention to disclose with student populations than with baby boomer participants (Wu et al., 2018). Dismissing an individual's age as a determiner for the intention to behavior gap, Ajzen (2011) wrote knowledge or information was the link between intention and behavior and that knowledge does not have to be accurate as a predictor of behavior. Along with the shortcomings related to PBC and attitude, there were critics of the TPB. The critics state the theory was too old for contemporary studies, and the theory was not an acceptable predictor of future behavior.

Armitage (2015), Hall (2015), Ogden (2015), and Sniehotta et al. (2015) criticized the TPB. The most profound criticism was the theory was outdated and past usefulness for behavioral research. Hall advocated the retirement of TPB based on the age of the theory and three shortcomings. First, Hall stated, the TPB was not useful for developing interventions to change behavior although the intention of TPB was to predict behavior. Second, participant self-reporting as the default methodology for assessing predictive construct was a weakness for the theory. Last, the lack of understanding for boundary conditions leading to research results, which the researcher accepts or rejects based on the situation. Hall was correct in his assessment of the TPB. The TPB does not provide interventions to the behavior. Researchers using the TPB can identify the attitudes, SNs, and PBCs, which contribute to the intentions of performing the behavior and the intentions to accomplish the behavior (Ajzen & Sheikh, 2013). Armitage, Hagger (2015), Hall, and Trafimow (2015) understood the importance of TPB but acknowledged the theory may have reached the end of usefulness and time to retire the theory. A researcher should base the theory's usefulness on the research results and not the age of the theory. The TPB continues to have favorable results as it transitions from the health care and psychological studies to business decisions (Hagger, 2015; Hall, 2015; Trafimow, 2015).

Sniehotta et al. (2015) scrutinized the research designs and selection of sample populations used for examining the behavioral intentions in TPB studies. Sniehotta et al. indicated that the TPB was not an acceptable predictor of behavior when research studies used different designs and when participants were not college students. Contrary to Sniehotta et al. (2015) the study design must be able to answer the research question

(Ajzen & Sheikh, 2013). Gurung and Raja (2016), Han and Stoel (2017), Hegner et al. (2017), and Shin and Hancer (2016) found favorable success with both qualitative and quantitative research methods using a sample population of participants with knowledge of the subject and willingness to participate, for a reward. The sample of knowledgeable participants was important

Shin and Hancer (2016) and Yeh et al. (2018) indicated the participant's knowledge of the behavior was important when conducting TPB studies. The sample population must have knowledge of and the capability to perform the behavior (Choong et al., 2017). Once the sample participants meet this condition, the TPB was a useful tool to examine intentions (Shin and Hancer 2016; Yeh et al., 2018). For approximately 30 years, researchers have used the TPB to frame their research and used the TBP survey tool to extract data on behavior intentions (Ajzen, 2014). Although the criticisms were valid, future researchers should know the TPB was a useful theory for understanding behavioral intentions in both the business and health care realms.

While Armitage (2015) and Hall (2015) stated the TPB should be retired, they recognized the theory for its 30 years of contributions. They agreed the theory framed many research projects over the past 30 years with success, in the psychology, health, and social science disciplines. Trafimow (2015) admitted the problems with the theory but recognized the theory for the contributions the theory provided in the study of health related issues. If the TPB has outlived its psychology, health and social science disciplines, the theory can be useful for business decisions. The limited number of research projects for business decisions using the TPB as a theoretical framework

indicates an opportunity to understand manager's intention toward specific business decisions (Liu, Wang, Wang, Xia, & Xu, 2019). Although managers make business decisions based on the availability of data or financial reasons, understanding the attitudes, SNs, and the PBC added a new element to the decision-making process.

I measured the relationship between the independent variables, attitude, SNs, and PBC, with the dependent variable, the behavioral marketer's intention to protect ecommerce consumer's personal information. The assumption was the behavioral marketer's rational behavior influence their actions and behaviors (Ajzen, 2011). The independent variables or predictors for this study include attitude toward ecommerce privacy, SNs, and PBC. The predictors will determine the intentions toward the behavior, of protecting ecommerce consumer's behavior. While behavioral marketers may have good intentions to reduce the amount of personal information collected, stored, and sold, the results of this study may confirm the behavioral marketer's attitude, SNs, and PBC as well as their capacity to change behaviors, with PBC.

The TPB formed the framework for this behavioral research study regarding the behavioral marketer's intention to protect ecommerce consumer privacy. The behavioral marketer's intention to increase or reduce privacy protection may affect the sales, revenue, and profits of the organization (Acquisti et al., 2016). The collection of ecommerce consumer's personal information contributes to the success of behavioral marketing (Martin, 2016). The collection and storage of ecommerce consumer's personal information presented the double edge problem. Jai and King (2016) stated that a disconnection of expectations was visible between the ecommerce consumer and the

behavioral marketer concerning privacy. While the collection and storage of personal information drive ecommerce sales and revenue, the collection of ecommerce consumer's personal information also subjects the information to the risk of a security breach (Choong et al., 2017). Based on the amount of personal information on social media websites, for data mining, understanding the behavioral marketer's intention toward ecommerce consumer privacy was important (Acquisti et al., 2016). The literature contains mixed opinions on the importance of privacy from the ecommerce consumer's perspective. Ecommerce consumer's desire privacy but will readily provide personal information voluntarily at the point of purchase (Cracium, 2018).

Behavioral marketers can answer the questions regarding the importance of ecommerce consumer privacy and whether ecommerce privacy requires protection. Although the financial aspects of protecting ecommerce consumer privacy cost will not be a question on the TPB research tool, behavioral marketers may need to consider the economic aspects of privacy changes. Choong et al. (2017), Liu et al. (2019), and Zhang (2014) examined the cost of security breaches for the consumer and the organization. The organization loses about $191 per transaction and the ecommerce consumer's loyalty (Zhang, 2014). Choong et al. and Zhang noted the high cost of resolution to the organization for security breaches. Zhang noted consumers are more likely to remain with the retailer while the organization remedies the security breach because of the high cost associated with switching ecommerce retailers. Liu et al. suggested behavioral marketers compare the added cost of ecommerce privacy protection with the estimated cost of repairing the damage from a security breach. The worst-case scenario was a

security violation, which reaches far beyond the financial implications of the issues of consumer trust and negative word of mouth advertising (Choong et al., 2017).

Consumer Privacy

Since 1890, consumer privacy studies have been of interest to consumers and marketers (Walsh et al., 2017). While the topic of consumer privacy was not new, it was a complex subject based on the various definitions of consumer privacy. The different definitions of privacy render the subject difficult to study and compare results, across studies (Milne et al., 2017). New to the collection of consumer privacy studies was ecommerce privacy from the behavioral marketer's point of view. Literature devoted to ecommerce consumer privacy within the behavioral marketing strategy was limited because this phenomenon was relatively new (Kude et al., 2017). Privacy from the consumer's perspective forms the majority of consumer privacy literature (Barbu, 2015). Milne et al. (2017 and Cracium (2018) suggested personal information on the Internet assists marketing managers in targeting consumers. Targeting consumers was profitable for corporations (Milne et al., 2017). An ecommerce privacy viewpoint from the behavioral marketer's perspective would provide a different perspective on the topic of ecommerce privacy.

A study of ecommerce privacy from the behavioral marketer's perspective includes an examination of the behavioral marketer's attitude, SNs, and PBC toward ecommerce privacy (Choong et al., 2017). Comparing the behavioral marketer's importance of ecommerce privacy from three different constructs, attitude, SNs, and PBC may determine the behavioral marketer's intent to protect ecommerce consumer privacy

(Choong et al., 2017). Privacy from the behavioral marketer's perspective was difficult to define based on the differing definitions of privacy and the ecommerce consumer's expressed concern for privacy (Barth & de Jong, 2017). Fortes and Rita (2016) stated that privacy and security appear as one variable. Another difficulty to the study of consumer privacy was the various degrees of ecommerce privacy concerns (Milne et al., 2017). The privacy paradox adds to the difficulty of studying ecommerce privacy (Barth & de Jong, 2017; Dienlin & Trepte, 2015). The use of social media platforms implies privacy was not a concern for ecommerce consumers (Weinberg et al., 2015). Whereas, security breach victims may view ecommerce privacy as important (Choong et al., 2017). This section includes a history of consumer privacy, an overview of the various definitions of privacy, the definition of privacy used for this study, and a review of previous research on consumer privacy.

Consumer privacy concerns due to technological innovations were an ongoing trend. The issue of consumer privacy dates to Warren and Brandeis (1890), as cited by Walsh et al. (2017), were the first authors to address privacy related to technical devices. In 1890, Warren and Brandeis approached privacy as a need for protection from surveillance technology or cameras (Walsh et al., 2017). Warren and Brandeis sought privacy protection from photographers who photographed individuals without prior permission. Warren and Brandeis viewed this action as a breach of privacy for the individual. According to Warren and Brandeis, privacy was an inherited right of every citizen. In their viewpoint, the photographers were responsible for requesting permission before taking photos.

The present Internet technology makes ecommerce consumer's personal information available. The existing literature included a mixture of viewpoints, which indicate two schools of thought. One viewpoint was consumers were not comfortable with the collection and use of their personal data for marketing purposes (Fortes & Rita, 2016). The second position relates consumer's wiliness to provide personal information for compensation in the form of a reward, discount, or another monetary reward (Milne et al., 2017).

Milne et al. (2017) revealed that ecommerce consumers have mixed opinions regarding consumer privacy protection. Some researchers identified the importance of protecting the privacy whereas other researchers advocated privacy was not an issue based on the amount of personal information on the Internet and the amount of personal information provided for frequent purchase and loyalty cards applications (Milne et al., 2017). An aspect of the research was the behavioral marketer's intention toward protecting ecommerce consumer privacy and the capability to make a decision regarding the privacy of ecommerce consumer privacy. Although behavioral marketers may have the capability to reduce the amount of information collected on ecommerce consumers, they may not have the incentive. The profits realized because of behavioral marketing may be the driving force to continue with collecting vast amounts of personal information (Campbell, Goldfarb, & Tucker, 2015). Kude et al. (2017) suggested the tradeoff of reducing the amount of information collected and the incremental increase in profits realized from behavioral targeting compared to traditional methods may not be incentive enough to reduce the amount of personal information collected. Cracium, (2018)

suggested that behavioral marketers consider the competitive environment and weigh the benefits of collecting personal information with the detrimental effects of a security breach.

The common theme among privacy literature was the control over personal information (Markos, Milne, & Peltier, 2017). Ecommerce consumers want control over who collects, stores, and sells their personal information (Barth & de Jong, 2017). Barth and de Jong (2017) reviewed 35 theories to better understand the privacy paradox, in an online environment. They concluded ecommerce consumers were concerned about their privacy when providing personal information but the ecommerce consumer desired control over who sees the information (Barth & de Jong, 2017). Milne et al. (2017) offered a differing opinion from Barth and de Jong; ecommerce consumers do not have rights to their personal information. There was an implied contract that marketers may use the information ecommerce consumers provided to expand sales revenue (Milne et al., 2017). Milne et al. 2017 referenced a study where 91% of consumers believe control over personal information was lost to marketers.

The definition of privacy changes with the introduction of new data collection technology based on the Internet of things (IoT) (Weinberg et al., 2015). The definitions evolve as the technological devices evolve. Personal information can be collected from Fit Bit devices, Polo tech shirts, self driving cars, and climate control devices (Markos et al., 2017). There were several definitions of privacy based on the different consumer situations and various technological devices. Ecommerce consumers may be more concerned about the collection, use, and sale of their personal information and have a

higher expectation for behavior marketers to avoid or reduce the amount of collected

information (Markos et al., 2017). Three ecommerce privacy definitions include the

unauthorized use of personal information, as a consumer right, a tradeoff for obtaining

discounts, and a right to be left alone.

Existing literature provides several definitions of privacy. Hallam and Zanella

(2017) suggested *privacy* can be defined as a commodity, state, or right. Milne et al.

(2017) defined *consumer privacy* as consumers concern with the unauthorized collection,

use of personal information and a desire for control. Milne et al. separated privacy into

two components, privacy and regulation of access to self. Their definition of privacy

included the unauthorized use of personal information and security as the protection of

personal information. Based on Milne's et al. privacy definition, privacy was not an issue

if the retailer requests authorization for the personal information before collection. The

request for personal information provides the ecommerce consumer with a degree of

control. Milne et al. suggested the ecommerce consumer had an expectation the requester

would protect their personal information. Walsh et al. (2017) agreed with Milne et al. that

marketers obtain permission prior to the collection of personal information but they

expanded the privacy definition by adding privacy was a consumer right, not to be

violated.

Lowry, Dinev, and Willison (2017) viewed privacy with traditional marketing as

a consumer right. As a consumer right, marketers obtained authorization prior to

collecting personal information (Lowry et al., 2017). If behavioral marketers apply the

definition of privacy used by Lowry et al., then ecommerce privacy was a consumer

right, and the behavioral marketer must view ecommerce privacy as important. Identification of the importance of ecommerce privacy results in measures to protect consumer privacy by requesting permission before collecting, using, and selling the ecommerce consumer's personal information (Milne et al., 2017). The use of mobile devices and the popularity of social network sites made consumer information readily available (Milne et al., 2017). Unlike traditional market research methods, asking for permission to use personal information was not required when personal information was available on public Internet sites (Borgesius, 2015).

Traditional marketing researchers asked the consumer's permission before requesting the information (Milne et al., 2017). In this case, the consumer provided only the information they were comfortable with sharing (Milne et al., 2017). Milne et al. (2017) suggested that consumers will provide information they were comfortable with sharing; usually demographic information. In other instances, the consumer would fabricate the responses and provide the information they thought the researcher wanted to know (Milne et al., 2017). The difference between traditional market research and current market research methods was the behavioral marketer obtains reasonably accurate information on consumer preferences based on browser histories and other information readily available (Borgesius, 2015). The present problem was whether extracting ecommerce consumer's personal information from browsers and other databases for use in behavioral marketing strategies leads to privacy concerns of accountability and security for the behavioral marketer (Weinberg, et al, 2015).

Cracium (2018) defined *consumer privacy* as a trade-off between the amount and type of information provided and security. The premise was that consumers increase their privacy by limiting the amount of information they disclose (Cracium, 2017). In some situations, ecommerce consumers provide incorrect personal information to protect their identity (Milne et al., 2017). Milne et al. (2017) referenced Goodwin (1991) in stating the desire to provide incorrect information may be based on judgements from peers. Increased ecommerce consumer privacy, in the form of nondisclosure of personal information, ultimately results in increased security and a reduction in the probability of a security breach (Cracium, 2018). Applying the privacy definition of Cracium suggests behavioral marketers view ecommerce consumer's personal information as important, and the need to protect the ecommerce consumer's personal information was necessary. Although the ecommerce consumers were willing to share personal information in exchange for something tangible, they remain cautious with the handling of their personal information (Cracium, 2018). When ecommerce consumers limit the amount of information they share the need for privacy concern and tighter security decrease. Restricting the amount of personal information ecommerce consumers disclose also limits the available useable information for the behavioral marketer (Milne et al., 2017). Like Milne et al., Mikhed and Vogan (2018) stated the collection of personal information was useful but security breaches have a devastating impact for the ecommerce consumer and the retailer. Milne et al. described the personal information tradeoff in terms of monetary value. Milne et al. stated ecommerce consumers were not concerned about

information privacy per se, when the consumer's trade personal information for a discount or monetary reward.

The dominant theme of privacy for Hallam and Zanella (2017) and Thompson, Tuzovic, and Braun (2019) was accountability. Accountability was a concern for the ecommerce consumer when they desire privacy but disclose personal information. Their attitudes were not in line with their intentions to disclose (Hallam & Zanella, 2017). Accountability may be a concern for the behavioral marketer, when stereotypical targeted ads may result in tarnished reputations and reduced sales based on *word of mouth* (WOM) from ecommerce consumers (Haryani & Motwani, 2015). The security of the ecommerce consumer's personal information was a primary concern for ecommerce consumers (Choong et al., 2017). Understanding the importance behavioral marketers place on the security and the privacy of the information collected forms the basis of this study. Thompson et al. (2019) stated accountability was important because the collected information was required for ecommerce growth. The behavior marketer's intention to protect ecommerce privacy was evident in the behavioral marketer's attitude toward ecommerce privacy. Their SNs, or how peers view privacy, and subjective behavior control will also be evident (Tamimi & Sebastianelli, 2015).

The ecommerce consumer's information was Internet-based in data files based on browser preferences, email address, and social media (Milne et al., 2017). The widespread use of social media sites suggests users were not concerned about the security of privacy. Milne et al. (2017) identified this phenomenon, the widespread use of social media as the privacy paradox. The privacy paradox may be controversial for the

behavioral marketer based on the assumption; information readily available on social websites was public information (Barbu, 2015). Fortes and Rita (2016) suggested ecommerce consumers did not know how their personal information found on social media sites was used. Ecommerce consumers provide personal information with the understanding this information was secure and only selected individuals will have access to the information (Lowry et al., 2017). Technological innovations such as the Internet made it possible for third parties to access ecommerce consumer's personal information (Choong et al., 2017). To this end personal information found on social media sites was public and accessible by behavioral marketers.

Milne et al. (2017) supported situations where consumers will provide personal information in exchange for a reward. The position of Milne et al. was contrary to the research findings of Fortes and Rita (2016), which suggested ecommerce consumers do not want to share their personal information. Milne et al. suggested the presence of a discount or reward blurs the lines between personal use and privacy concerns. When ecommerce consumers express concern for privacy but provide personal information for a specified reward, this results in a privacy paradox (Walsh et al., 2017). When Milne et al. suggested consumers were willing to trade their personal information for a reward; the reward included all the common incentives, such as discounts, travel points, merchandise, and monetary rewards. Milne et al. suggested ecommerce consumers do not have privacy concerns regarding providing personal information when rewards were available, in exchange for the information. In this situation, behavior managers do not need to view ecommerce consumer's personal information protection, as important. Contrary to the

findings of Milne et al., Barbu (2015) advocated for consumers to protect their personal

information by controlling the amount of information shared and made available to

marketers, regardless of offered incentives.

This research study on privacy focused on the behavioral marketer's intentions to

protect ecommerce consumer's personal information. The behavioral marketer can access

the ecommerce consumer's information from email accounts, browsing histories, and

social media (Milne et al., 2017). This activity was valuable for the behavioral marketer

as it results in an increase in sales, revenue, and profits (Kude et al., 2017). The opposite

of increased sales revenue is a security breach, whereby ecommerce consumers may face

identify theft (Kude et al., 2017). Security breaches result in large expenses for the

corporation, the behavioral marketer represents (Benson, Saridakis, & Tennakoon, 2015;

Choong et al., 2017). The impact of security breaches includes the costs for consumer

support, data security improvements, and incident investigation costs (Choong et al.,

2017). If the behavioral marketer has a positive attitude toward ecommerce privacy and

their intentions to protect or safeguard the collected information were high, then

ecommerce consumers should have a minimal concern or worry about the misuse of the

personal information (Lwin et al., 2016).

Researchers defined consumer privacy in several ways and placed varying

degrees of importance to consumer's privacy (Milne et al., 2017). The *privacy* definition

for this study was the protection of personal information gathered from email accounts,

browser histories, purchase histories, and social network sites, for targeted advertising

purposes (Weinberg et al., 2015). Understanding the importance behavioral marketers

place on the collection and use of ecommerce consumer's personal information was important to understanding the behavior marketer's perspective on ecommerce privacy. The behavioral marketer increases sale and revenue by using personal information to target advertising to the ecommerce consumer most likely to purchase the goods and services (Milne et al., 2017; Weinberg et al., 2015). The collected personal information adds value to the targeted marketing strategy (Walsh et al., 2017; Milne et al., 2017). Targeted advertising provides a financial benefit to the organization or corporation from the use of personal information (Walsh et al., 2017). Although the benefits of behavioral marketing were profitable, the value added benefit may have negative consequences if the information was hacked or stolen resulting in a security breach (Benson et al., 2015). The behavioral marketer must balance the risks of obtaining the personal information with the increased revenue benefits along with the possibility of a security breach (Choong et al., 2017). In order to balance the risks of collecting ecommerce personal information for targeted advertising, the behavioral marketer must understand the two privacy themes, promotion focus and prevention focus (Cracium, 2018).

Two privacy themes of ecommerce privacy appear in the literature; the consumer's promotion focus and the consumer's prevention focus (Lwin et al., 2016). Acquisti et al. (2016), Jai and King (2016), and Milne et al. (2017) provided support for the promotion focus viewpoint. Ecommerce consumers will provide personal information for a reward. Acquisti et al. suggested consumers have a threshold for monetary incentives, whereas Milne et al. suggested ecommerce consumers would provide personal information for any incentive or discount. The prevention focus includes ecommerce

consumers who prefer not to disclose personal information. Barbu (2015), Fortes and Rita (2016) and Weingerg et al. (2015) stated ecommerce consumers were inclined to protect their privacy by not disclosing personal information. Barbu and Fortes and Rita agreed ecommerce consumers should protect their personal information by not participating on social Internet sites. Cracium (2018) suggested ecommerce consumers protect themselves through education regarding the disclosure of personal information on the Internet as a method of protection. While the two privacy themes tend to contradict each other, the promotion focus includes ecommerce consumers who trade personal information for a reward. The prevention focus consumers would prefer not to disclose personal information without a clear picture of who was collecting the information and the intentions for the collected information (Lwin et al., 2016; Milne et al., 2017).

Promotion focus. The promotion focus aspect of privacy illustrates the consumer's willingness to provide personal information for a reward (Acquisti et al., 2016; Fortes and Rita, 2016). Behavioral marketers describe the situation as the privacy calculus (Aguirre, Roggeveen, Grewal, & Wetzels, 2016; Fortes & Rita 2016; Lwin et al., 2016). In this situation, ecommerce consumers regard their personal information as a commodity, which they trade or sell for promotional rewards, such as a percentage discount (Cracium, 2018). Milne et al. (2017) suggested consumers who provide personal information for a reward or discount were not concerned about their privacy. Barbu added to Milne et al. and described the ecommerce consumer as providing their personal information in exchange for a reward as selling their personal information. Cracium (2018) further stated privacy concerns were part of the ecommerce consumer's value

system. The privacy calculus suggests ecommerce consumers may have privacy concerns but will quickly sell their personal information for a reward (Lwin et al., 2016); Milne et al., 2017). Once the ecommerce consumer releases their personal information, the consumer does not have a claim on the information after accepting a reward or discount in exchange for the information (Milne et al., 2017). Using consumer information to target advertising appears to be a win-win situation for both the behavioral marketer and the ecommerce consumer (Walsh et al., 2017). The additional discounts for the ecommerce consumer translate into an increase in sales for the retailer and increased information for the behavioral marketer (Barbu, 2015). In some cases, the consumer was willing to provide the information but wants to maintain control over who uses the information (Walsh et al., 2017).

Veltri and Ivchenko (2017) suggested privacy concerns related to promotion focus or privacy calculus relates to the ecommerce consumer's control of their personal information. If the ecommerce consumer believes they have control over their information, they may provide the requested information for a reward or discount (Benson et al., 2015). Ecommerce consumers lose control over their information when they post information on social media sites (Weinberg et al., 2015). This loss of control led Markos et al. (2017) to state privacy was dead in the digital age. While accessing personal information from social network site is not the only means for obtaining ecommerce consumer's personal data, behavioral marketers may obtain personal information from frequent flyer cards, membership cards, and other loyalty cards or other tangible incentives (Lwin et al., 2016; Milne et al., 2017)

The use of loyalty cards was widespread (Milne et al., 2017). Ecommerce consumers using loyalty cards for discounts on products and services provide a certain amount of information for the retailer to customize advertising ads (Milne et al., 2017). American Airlines established the first documented loyalty program in 1981 (Meyer-Waarden, 2015). Loyalty cards were a convenient method for collecting personal information from ecommerce consumers (Milne et al., 2017). The ecommerce consumer provides personal information when they sign up for the loyalty or frequent users card (Meyer-Waarden, 2015). The behavioral marketer uses this information, to target advertising ads to the consumer (Meyer-Waarden, 2015). In exchange for the information, retailers provide discounts, which translated into monetary benefits (Cracium, 2018). Lwin et al. (2016) suggested consumers were aware of the risks but were willing to provide personal information in exchange for rewards. Cracium (2018) concluded ecommerce users were knowledgeable concerning personal privacy, understand the privacy risks, and will assume a certain degree of risk for a reward, compensation, or promotion. Contrary to Cracium, Milne et al. (2017), and Weinberg et al. (2015) implied ecommerce consumers were not aware of the dangers of providing personal information for a discount and ecommerce retailers should self-regulate themselves when collecting personal information. Meyer-Waarden suggested ecommerce consumers engaged in ecommerce purchasing and use loyalty cards were not overly concerned with ecommerce privacy. The fine print on the loyalty card indicates marketers may use the information provided for marketing purposes (Cracium, 2018). Milne et al. 2017 took a different view; they stated ecommerce consumers were aware of the personal

information they provide on loyalty card applications and provide the information voluntarily, in exchange for a monetary benefit. If ecommerce consumers were conscious of the risk and trade their personal information as a commodity, for compensation or discount, there is no need for behavioral marketers to make the effort to protect the ecommerce consumer's personal information (Walsh et al., 2017). The ecommerce consumer provided the information as a part of doing business with the ecommerce retailer. The widespread use of loyalty cards would confirm the privacy calculus; ecommerce consumers were willing to disclose personal information for compensation (Walsh et al., 2017). The use of loyalty cards indicated ecommerce consumers will assume the risk of a security breach in exchange for a benefit (Barbu, 2015). Although privacy statements were present when the consumer applies for a loyalty card, few consumers read the fine print, which explains how behavioral marketers may use the information (Barbu, 2015).

Walsh et al. (2017) used privacy calculus to understand why consumers disclose personal information. The privacy calculus states a consumer will disclose personal information for a perceived benefit, regardless of the risk (Aguirre et al., 2016). Contrary to the privacy calculus, Barbu (2015) found a weak link between privacy concerns and willingness to disclose personal information for loyalty programs. This weak link may suggest ecommerce consumers may try to protect their privacy once they understand the process of collecting, using, and selling their personal information. There were disadvantages concerning the use of loyalty cards for commerce consumers, which may

cause concern for the ecommerce consumer (Acquisti et al., 2016). Situations may arise with inaccurate targeting and the sale of personal information to third parties.

A known problem with loyalty cards was inaccurate consumer targeting (Walters, Wiese, & Bruce, 2018). Inaccurate targeting occurs when the wrong ad reaches the ecommerce consumer. Behavioral marketers identify incorrect targeting as a message backfire because the recipient did not identify with the message (Walters et al., 2018). Walters et al. (2018) attributed the identification problem to behavioral marketers obtaining information from data miners selling outdated information. Understanding the role of data brokers for behavioral marketers will determine if behavioral marketers were purchasing outdated or fraudulent consumer data. Data brokers turn random pieces of personal information into a sought after commodity (Weinberg et al., 2015). Data mining was easier with a large amount of data on the Internet (Weinberg et al., 2015). The use of consumer data from third-party sources including social media sites may result in erroneous ecommerce consumer targeting (Corrigan, Cracium, & Powell, 2014). Erroneously targeting the ecommerce consumer was a reason for concern.

The Target Corporation found a solution for message backfire, when an ad for baby products went to a family loyalty card prior to the young woman disclosing her pregnancy (Corrigan, et al, 2014). The behavioral marketers at Target Corporation use a 3-prong approach to deliver targeted advertising (Corrigan et al., 2014). In addition to gathering data from data brokers, Target provides a 5% discount on each purchase with the loyalty card, and they mix the ads to avoid message backfires (Campbell et al., 2015; Corrigan et al., 2014). Because ecommerce consumers do not want to filter through ads

for products, they have little interest in, Campbell et al. (2015) suggested the need to target the correct ad to the correct customer.

Inaccurate consumer targeting provides a reason for the ecommerce consumer to discontinue use of the card, thus leaving the behavioral marketer without a convenient source for obtaining consumer information (Campbell et al., 2015). Behavioral marketers on behalf of corporations do not notify ecommerce consumers when they collect and use personal information for marketing purposes (Cracium, 2018). For example, the Target Corporation marketers do not notify ecommerce consumers, the information consumers provide was for marketing purposes (Cracium, 2018). The site designers buried the privacy information in the fine print without a statement of how the information was utilized (Cracium, 2018). The security breach in 2013 impacted 41 million customers (Lowry et al., 2017). The debate continues with the pros and cons of ecommerce privacy concerns with the use of loyalty cards. Ecommerce consumers enjoy the benefits of the loyalty cards and do not perceive a problem with providing personal information to obtain a discount or monetary reward (Milne et al., 2017). The amount of information accessible from the Internet renders ecommerce privacy difficult to protect (Weinberg et al., 2015). The last problem ecommerce consumers may incur with the uses of a loyalty card was the sale of personal information to a third party broker or data miner (Jai & King, 2016; Spiekermann, Acquisti, Bohme, & Hui, 2015). Spiekermann et al. (2015) stated selling personal information to third party broker or data miner presents the problem of identifying where the security breaches occurred.

Retailers sell personal consumer information to third parties on a regular basis (Jai & King, 2016). The information was readily available from social network sites, browser histories, and previous experience with ecommerce retailers (Jai & King, 2016). Jai and King (2016) discovered consumers were willing to provide personal information for loyalty programs but do not want the information sold to third parties. The problem with loyalty card retailers purchasing and selling ecommerce consumer's personal information was the lack of knowledge to explain the third parties' intended use of the personal information (Acquisti et al., 2016). This lack of knowledge results in inaccurately targeting the ecommerce consumer (Acquisti et al., 2016). The behavioral marketer can review the data for the relevancy of the information to ensure correctness (Cracium, 2018). Ecommerce consumers with strong privacy concerns can avoid providing personal information (Barbu, 2015). The prevention method relies on opting out of all loyalty card promotions, no interaction with social network sites and limited ecommerce sales (Choong et al., 2017). The action of protecting personal information from the collection, use, and sale incorporate the prevention focus aspect of ecommerce consumer privacy.

Prevention focus. The second theme for ecommerce privacy was prevention focus. Campbell et al. (2015) defined privacy prevention focus as the process of reducing privacy concerns by reducing the amount of personal information provided to ecommerce retailers, through regulation. Ecommerce consumers fail to understand the process of using personal information to increase ecommerce profitability (Libaque-Saenz et al., 2016). Ecommerce consumers protect their privacy by engaging in protective behaviors and not providing personal information (Taylor, Ferguson, & Ellen, 2015). There were

conflicting schools of thought regarding the need for consumers to protect their privacy and minimize the collection, use, and sale of personal information.

Campbell et al. (2015) indicated ecommerce consumers require protection through prevention and ecommerce education regarding the collection, use, and sale of personal information. Education was the ecommerce consumer's best defense for reducing the amount of personal information provided to ecommerce retailers (Campbell et al., 2015). Declining invitations for loyalty cards was only one source for preventing the behavioral marketer from obtaining ecommerce consumer's personal information (Choong et al., 2017). Contrary to Taylor et al. (2015), Milne et al. (2017) indicated consumers cannot stop the widespread use of personal information based on the numerous data collection devices in use by e commerce consumers. The personal information was available from several sources. Choong et al. and Cracium (2018) iterated opting out of requests for personal information might not solve the privacy prevention situation, due to lack of transparency and the availability of personal information via the Internet. Also, the behavioral marketer has several sources for obtaining personal information for ad targeting. The sources include data mining, previous purchase histories, cookies, and social network sites (Kayhan & Davis, 2016). The availability of personal information may be available from several sources (Kayhan & Davis, 2016). The ecommerce consumer cannot avoid leaving an information footprint (Milne et al., 2017). Therefore, declining requests for personal information may not be enough to prevent security breaches.

The ecommerce privacy researchers Campbell et al. (2015) voiced a different opinion concerning privacy through prevention compared to Taylor et al. (2015). Campbell et al. argued privacy concerns were part of a consumer's value system and do not require protection by prevention, but through regulation. Contrary to Campbell et al., Cracium (2018) suggested ecommerce consumers do not need privacy prevention, and ecommerce consumers should maintain control of their personal data, through the options provided by the ecommerce websites, such as opt in and opt out opportunities as well as privacy notices.

Based on the TPB model behavioral marketers who have a strong correlation between ecommerce privacy and attitude will view ecommerce privacy as important requiring protection or through a reduction of information requested (Seungsin et al., 2015). If the intention of behavioral marketers was the protection of ecommerce consumer's personal information, then ecommerce consumers do not have to be overly protective of the information provided to ecommerce retailers (Campbell et al., 2015). The behavioral marketer will focus their attitudes on protecting consumer's personal information. Behavioral marketing peers who share similar personal information protection strategies will influence their SNs (Kammer et al., 2016). Last, the behavioral marketers will have the capability to modify the personal information security strategies, where required as part of their PBC (Tiwari, Bhat, & Tikoria, 2017).

The best overall solution to protecting ecommerce consumer privacy was through education (Barbu, 2015; Kammer et al., 2016). Cracium (2018) suggested ecommerce consumers do not require protection through prevention. There was an implied contract

between the ecommerce consumer and the behavioral marketer on behalf of the

organization and the request for personal information. Seungsin et al. (2015) noted

ecommerce consumers know how to protect their privacy. Ecommerce consumers were

aware of the risks and how to minimize the risks of a security breach based on public

information regarding previous security breaches (Seungsin et al., 2015). Acquisti et al.

(2016) found that consumers were more likely to reject requests for personal information

in exchange for reward if they believed their personal information was at risk.

If Cracium (2018) was correct and an implied contract exists then, the behavioral

marketer on behalf of the retailer has an obligation to store ecommerce consumer's

personal information in a method, which will protect the personal information. There

were several options behavioral marketers can utilize to manage the ecommerce

consumer's information in a sensitive manner (Cracium, 2018). The literature contains a

few examples of methods for handling the ecommerce consumer's information in a

sensitive way. One method was by setting the ecommerce consumer's expectation. Peer

and Acquisti (2016) implied the prevention of personal information misuse was best if

addressed by the manager to set the consumer's level of expectation. Setting the

consumer's expectation through open disclosure was a good method for reducing the

ecommerce consumer privacy concerns (Choong et al., 2017). Another approach was a

time stamp on the personal information. Campbell et al. (2015) and Craciun (2018)

suggested ecommerce retailers provide consumers with an element of control for their

privacy with an opt-out clause in their privacy statement to reduce the amount of

information a consumer was required to provide. Another retailer self-regulating process

was the development of an easy to read and understand privacy clause (Cracium, 2018). The privacy clause should contain an informed consent section and an expiration date for the collected information (Campbell et al., 2015). Behavioral marketers have an opportunity to take the lead by informing the ecommerce consumer with information regarding what information they collect, how they use the information, and at what point the information the behavioral marketer sells the information (Choong et al., 2017). The flow of information from behavioral marketers will aid the ecommerce consumer in understanding how their personal information fit into the behavioral marketers advertising strategy (Walsh et al., 2017). Last, a well-constructed privacy statement located at the point where ecommerce consumers provide their personal information will aid in the ecommerce consumer's education of how the behavioral marketer will use the provided information (Cracium, 2018). An expiration date will ensure the ecommerce consumer when the information will no longer be available (Cracium, 2018). If the request for personal information was a social contract then having as much information regarding how the behavioral marketer uses the personal information was helpful in easing the ecommerce consumer's prevention privacy concerns (Campbell et al., 2015). The behavioral marketer's intentions toward ecommerce consumer privacy will determine the need to protect ecommerce privacy through prevention or education (Tiwari et al., 2017).

TPB Variables and the Marketer. Behavioral marketers know the advantages of behavioral marketing. Behavioral marketers increase organization sales and revenue by obtaining information supplied by data mining (Tamimi & Sebastianelli, 2015). The

capability to access and use this data was advantageous to the behavioral marketer (Lwin et al., 2016). What were not clear were the behavioral manger's attitudes, SNs, and PBC toward ecommerce privacy concerns. Lwin et al. (2016) and Milne et al. (2017) argued against the need to protect the consumer's personal information based on the widespread use of promotional rewards. Research was required to understand the behavioral marketer's intention toward the collection, use, and sell of ecommerce consumer's personal information based on the behavioral marketer's attitude, SNs, and the ecommerce manager's PBC. Internet usage provides a challenging argument for the protection of ecommerce consumer privacy.

The behavioral manger's attitude toward the ecommerce consumer privacy includes the behavioral marketer's capability to form a positive or negative evaluation of consumer privacy. Ajzen and Sheikh (2013) stated beliefs about a behavior's consequences determine attitudes concerning the behavior. In this case, the use, collection, and storage of ecommerce consumer's personal information in a database may result in a security breach (Cracium, 2018). The behavioral marketer's previous experience with consumer privacy will shape their attitudes regarding ecommerce consumer privacy (Vasalou, Joinson, & Houghton, 2015). Previous experience includes the behavioral marketer's personal experience with Internet privacy and the behavioral marketer's participation in a group or organization, which was the target of a security breach (Clemons & Wilson, 2015).

SNs of the behavioral marketer measure the effect peer groups have in shaping the importance of protecting ecommerce consumer privacy. Ajzen and Sheikh (2013)

related SNs to the perceptions of significant outside individuals. Featherman and Hajli (2016) extended the thought of Ajzen and Sheikh to include the experience level of manager, which affects the manager's subjective norm. If the manager was inexperienced, then the manager may depend on their peer group because they lack confidence in their knowledge of consumer privacy (Fortes & Rita, 2016). Experienced managers tend to trust their knowledge of ecommerce privacy, while collecting information from several sources (Moore, Moore, Shanahan, Horky, & Mack, 2015). Moore et al. (2015) referred to the process of collecting information personal from several sources, as *creepy marketing*.

The PBC component to the TPB determines the behavioral marketer's capacity to perform the task of protecting ecommerce consumer's behavior (Ajzen, 1991). PBC determines the capability to perform the behavior (Ajzen & Sheikh, 2013). The PBC component allows the manager to perform or not perform the intended behavior (Ajzen, 1991). The behavioral marketer will either perform the behavior of protecting ecommerce consumer privacy with ease or difficulty. The two perspectives on consumer privacy promotion and prevention suggest differing approaches to consumer privacy. Increased Internet usage and the popularity of social networks supports the argument consumer privacy on ecommerce websites was not important and security breaches were not important to ecommerce consumers (Weinberg et al., 2015). Based on the limited information regarding behavioral marketer's intent to protect ecommerce consumer privacy, the outcome of this study may add to the literature concerning ecommerce privacy on websites using a behavioral theoretical framework, TPB.

Behavioral Marketing

The study of behavioral marketing was beneficial based on the amount of

personal information that was required to make this strategy successful and the

profitability (Cracium, 2018). Behavioral marketing was successful as a marketing

strategy because it increases revenue from online sales, lowers overall marketing costs,

and positively influences the profitability of the organization (Cracium, 2018). As an

effective strategy, behavioral marketing increase sales and overall profits for the

organization (Cracium, 2018). Summers, Smith, and Walker-Reczek (2016) defined

behavioral marketing as the practice of collecting and storing online consumer

information, to target advertisements for products or services to consumers who showed

interest in the product or service from the browsing history and other information

sources. Moore et al. (2015) expanded on the definition of behavioral marketing by

defining the behavioral portion of behavioral marketing to mean the type of ecommerce

consumer's personal information behavioral marketers collected. Similarly, Campbell et

al. (2015) narrowed the information used by behavioral marketing managers to

consumer's personal information derived from past online activity. The use of personal

information leads to a successful behavioral marketing strategy (Lwin et al., 2016).

Behavioral marketers were successful when ecommerce consumer information was

available for designing targeted marketing messages (Cracium, 2018). In addition, the

collection of personal ecommerce consumer's information from social sites allows the

behavioral marketer to obtain current consumer information (Weinberg et al., 2015). The

availability of consumer information for use in marketing strategies evolved from a product based to consumer-based strategies (Barbu, 2015).

In the 1920s through 1940s, manufacturers made products first then advertised the product based on a perceived need of the consumer (Barbu, 2015). The consumer did not provide input into the product design, nor the advertising message (Barbu, 2015). As time evolved, advertising collateral included several mediums, including print ads, radio spots, television spots, and billboard advertising (Barbu, 2015). The challenge for marketers was matching the product to the customer. To know and understand the consumer's likes and dislikes, marketing researchers gathered consumer information related to consumer behavior through research projects (Barbu, 2015).

Prior to the Internet marketers collected consumer information through surveys mailed to random homes, in prepaid envelopes for returning the survey (Barbu, 2015). In some situations, researchers conducted in-person interviews or focus groups. In each of these information-gathering cases, the researcher never knew how the participant's external environment affected the responses. Behavioral marketing evolved from traditional advertising methods as a means for marketing organizations to recover ecommerce sales lost to increased retail competition and online comparison-shopping (Cracium, 2018). Increased technological innovations contributed to the availability of ecommerce consumer's personal information (Milne et al., 2017). Access to the Internet opened the door to ecommerce retail sales and shortened the distance between the ecommerce consumer and the retailer (Weinberg et al., 2015). Consumers and marketers benefited from the technological advancements (Milne et al., 2017).

Technological innovations were the core of a successful behavioral marketing strategy. The expanded technologies of the Internet increased the knowledge of consumers as they interacted with ecommerce retailers (Milne et al., 2017). Access to the Internet allows for communication beyond geographical boundaries and browsing activity (Milne et al., 2017). Ecommerce consumers were part of the technological changes related to how ecommerce consumers interact with and access the Internet (Milne et al., 2017). The desire to have the convenience of information available prompts the use of the Internet (Milne et al., 2017).

The average consumer evolved through the technological phase; from a desktop computer to laptops and tablets to handheld devices, such as phones (Milne et al., 2017). The widespread adoption of digital devices provides fertile ground for behavioral marketing (Vasalou et al., 2015). The modern consumer has Internet access readily available, day and night. The easy access to the Internet prompted an interest from researchers to understand the ecommerce consumer (Campbell et al., 2015). Marketing through the Internet gives marketers the ability to level the playing field between large and small organizations (Milne et al., 2017).

Acquisti et al (2016) called behavioral marketing a tool of choice for online advertisers. The information found on the Internet allows behavioral marketers an opportunity to target consumers directly based on previous purchase history (Milne et al., 2017). The difference between online and offline advertising was the ability to target consumers effectively (Campbell et al., 2015). Although, behavior marketing increases the efficiency of advertising by targeting ads toward consumer preference, privacy

concerns were present (Campbell, et al, 2015; Walters et al., 2018). Behavioral marketing requires data mining to collect consumer information, to be effective (Cracium, 2018). Internet technology has allowed marketers an opportunity to refine the process of collecting personal customer information regarding buying patterns (Milne et al., 2017). Data mining allows marketers to gain access to the personal data based on technological advances, of the Internet (Milne et al., 2017). Data mining presents the significant risk to behavioral marketing. Obtaining personal information from ecommerce consumer's personal information may present a risk to behavioral marketing managers.

The profitability of behavioral marketing for organizations was encouraging for organizations (Wu et al., 2018). The benefits of behavioral marketing include increased revenue by targeting products and services based on the consumer's preferences and allow for a reduction in marketing costs to reach the target consumer segment (Wu et al., 2018). Behavioral marketing as a strategy increases the competitive advantage, of an organization, which lead to increased revenue and improved consumer-targeting strategy (Walsh et al., 2017). While Walsh et al. (2017) discovered targeted marketing creates a positive relationship between the advertiser and the consumer there were disadvantages to collecting, using, and selling ecommerce consumer's personal information. Conversely, behavioral marketing may have a negative effect when identity marketing backfires and behavioral marketers target ads to incorrect consumers (Clemons & Wilson, 2015). Behavioral marketing may also backfire when the marketer uses the ecommerce consumer's information for the purpose of price discrimination (Clemons & Wilson, 2015). The largest concern for behavioral marketers was the issue of consumer

privacy and the threat of privacy breaches (Choong et al., 2017). The question regarding

ecommerce privacy was the importance behavioral marketers place on ecommerce

consumer's personal information. An increase in ecommerce transactions year over year

lends creditability to the theme of consumer privacy concern with the behavioral

marketer's process for collecting, using, and storing consumer's personal data (Choong et

al., 2017). Although behavioral marketing was profitable and contributes to increased

revenue for the corporation, there were disadvantages and risk associated with behavioral

marketing (Steijn & Vedder, 2015).

While behavioral marketing was profitable and contributed to increased revenue

for the corporation, there were disadvantages to the implementation of a behavioral

marketing strategy. The disadvantages included incorrectly targeting the ecommerce

consumer and security breaches (Walters et al., 2018). Liu et al. (2019) suggested

ecommerce retailers could lose a portion of their existing market if behavioral marketers

mishandle consumer information. Lwin et al. (2016) added to this by stating discovered

privacy concerns would prompt the consumer to change retailers. From the consumer's

standpoint, Campbell et al. (2015) added to Lwin et al. (2016) by stating that improved

technology may result in lower switching costs and advertising avoidance tools for

consumers. Conversely, Walters et al. (2018) stated ecommerce consumers might view

targeted advertising as annoying and have increased concerns regarding targeted

advertising. The personal information component of behavioral marketing, personal

information, which leads to a successful strategy for increasing organizational revenue

can alienate consumers using outdated information or targeting by body type and shape

(Walters et al., 2018). Outdated information incorrectly targets the consumer and presents

the greatest challenge to consumer privacy (Steijn & Vedder, 2015). Incorrectly targeting

the ecommerce consumer based on outdated information results in a frustrated

ecommerce consumer (Clemons & Wilson, 2015). The behavioral marketer requires

current ecommerce consumer data for a successful behavioral marketing strategy.

Incorrectly targeting the consumer presents a problem, resulting in a mismatch between

the targeted consumer and the brand, and the possible risk of privacy breaches (Walters et

al., 2018)

Walters et al. (2018) revealed a weak link between behavioral marketing and the

collection of personal data based on a lack of correlation due to the collection of personal

information without a significant relationship to the brand. Walters et al. further stated

the successful behavioral marketing strategy would associate targeted brands to the

lifestyle of the consumer, like the Harley Davidson and Apple brands. To achieve a better

understanding of consumer targeting, Campbell et al. (2015) suggested companies

develop a positive relationship with consumers to target the best products to the

consumer. A relationship between the retailer and the ecommerce consumer is required

for correctly targeting brands, products, and services (Campbell et al., 2015). The

behavioral marketer's intention to safeguard the ecommerce consumer's personal

information will lower the risk of a security breach (Steijn & Vedder, 2015).

The second risk to behavioral marketing profitability was security breaches. The

potential of behavioral marketing is the misuse of personal information or a security

breach (Sen & Borle, 2015). Moore et al. (2015) discussed the fine line between

advertising and privacy invasion. As additional retailers incorporate behavioral marketing strategies into their advertising programs, the risk of security breaches will continue to grow (Steijn & Vedder, 2015). Security breaches have a cost associated with each breach for the retailers and the ecommerce consumer. Choong et al. (2017) explored security breaches from the marketer's viewpoint. In 2013, 43% of American companies reported data breaches (Choong et al., 2017). Target, Home Depot, and JP Morgan Chase were a few of the high-profile companies affected by breaches (Choong et al., 2017). Consumers who have privacy concerns tend to limit on line purchase activities, resulting in lost sales (Choong et al., 2017). Additionally, lost sales due to customer loyalty were approximately 3 million dollars (Campbell et al., 2015). Security breaches were not only costly to the organization, but consumers display less than desirable reactions to targeted advertising (Campbell et al., 2015). Behavioral marketers understand the risks of behavioral marketing. The benefits of behavioral marketing tend to outweigh the risks and disadvantages.

Walsh et al. (2017) examined the benefits of behavioral marketing while addressing the issue of consumer privacy. The inherent benefits of behavioral marketing were lower advertising costs and increased marginal profits (Walsh et al., 2017). Tabari and Abroud (2017) found the success of behavioral marketing depended on the assurance the ecommerce retailer or behavioral marketer provided to protect personal information used for marketing purposes. Cracium (2018) expanded on this by stating behavior marketers should balance the benefits of behavioral marketing with the risks. Choong et al. (2017) stated a specific personalized behavioral marketing strategy

worked best to minimize the risk of security breaches. The personalized strategy used the ecommerce consumers name in the ad. Personalized advertising brings a level of comfort to the consumer that the ecommerce retailer will use their personal information for the intended purposes (Walsh et al., 2017). Ecommerce retailers must understand the frequency of personalizing ads to the consumer (Fortes & Rita, 2016). A high frequency may result in ad avoidance, which negatively affects organizational revenue (Fortes & Rita, 2016). Campbell et al. (2015) agreed with Walsh, behavioral marketers should monitor the frequency of the targeted ads.

The ecommerce consumer information was available for both domestic and global ecommerce retailers (Milne et al., 2017). The challenge for global marketers was the development of business to consumer relationship. The development of a relationship was beneficial for global ecommerce retailers (Weinberg et al., 2015). Milne et al. (2017) indicated the ecommerce consumer was willing to share personal information with global retailers provided there was familiarity. Global consumers develop familiarity through repeat purchases and relationship management (Weinberg et al., 2015).

Craciun (2018) and Weinberg et al. (2015) agreed based on their research, that behavioral marketing may increase revenue and reduce marketing costs but at a significant cost to the ecommerce consumer privacy. As researchers, Cracium and Weinberg et al. advocated for ecommerce consumers to exercise control over their personal information. Ecommerce consumers were more willing to provide personal information when they felt in control of their personal information (Walsh et al., 2017).

Walsh et al. suggested a disconnection between the ecommerce retailer's use of personal information and the expectation of privacy protection. Although control over personal information allows ecommerce consumers to take risks with their personal information, control does not lead to privacy protection (Walsh et al., 2017). This disconnection may damage the relationship between the retailer and the consumer resulting in lost sales and reduced profitability (Cracium, 2018).

Behavioral marketing has benefits for the organization and to the consumer (Todor, 2016). The marketing managers can target a consumer with an interest in the product or service and the consumer's exposure to targeted advertising directed to a product or service may increase the likelihood of a sale. Although behavioral marketing increased revenue, behavioral marketing was not beneficial for all organizations. Todor (2016) revealed behavioral marketing increases revenue if the organizations were similar in size and the competition was sufficient. For smaller organizations with small demand for the product or service, traditional advertising methods may be more profitable (Todor, 2016).

There was a cost associated with behavioral marketing (Choong et al., 2017). Choong et al. stated behavioral marketing was profitable for all organizations. While behavioral marketing was profitable there was a down side in the event of a security breach (Hallam & Zanella, 2017). A security breach can have a negative impact on stock prices and result in large cash expenditure to repair the damage to the affected consumers (Hallam & Zanella, 2017). For example, the data breach at Target in 2013 resulted in a 40% loss of profits (Kude et al., 2017).

The information found in the literature demonstrated the importance of collecting and using ecommerce consumer's personal information as it related to increasing sales and revenue for the business or corporation (Choong et al., 2017). What was not clear was the behavioral marketer's attitude toward protecting ecommerce consumer privacy. Additionally, it was not clear if behavioral marketers intended to protect ecommerce consumer privacy. What was widely known was how ecommerce consumers view online privacy.

My purpose in this quantitative correlational study was to understand the strategic intention of behavioral marketing managers when developing ecommerce advertising strategies, which collect, use, and sell ecommerce consumer's personal information. The process of collecting, using, and selling ecommerce consumer's personal information may put the information at risk for a security breach. Using TPB to frame the study, I examined the behavioral marketer's strategic intentions to understand the attitudes, social norms, and perceived behavioral control of the marketing manager. Studying the attitudes, social norms, and perceived behavioral control of the marketing manager who develop targeted ads with ecommerce consumer's personal information will add to the existing literature. The results of this study contributed to the existing literature by adding the element of consumer privacy, from the behavioral marketing manager's perspective.

Transition

In Section 1, I defined behavioral marketing and how behavioral marketing benefits the organization. The central component of behavioral marketing was the

collection, use, and sale of ecommerce consumer's personal information. The ecommerce

consumer's perspective maintains two schools of thought regarding personal information

privacy, promotion focus, and prevention focus. The promotion focus group maintains

consumer privacy was not an issue and will trade personal information for a reward. The

second group maintains information privacy was a right and requires protection from,

behavioral marketers. The TPB tools were instrumental in gathering behavioral

information from the behavioral marketing managers regarding ecommerce consumer

privacy and the need to protect the privacy by limiting or ceasing the collection of

personal information without the consumer's consent.

In Section 2, I provided detailed information concerning details of this research

project, a description of the role of the researcher, the research method and design,

population and sampling, data analysis, ethical consideration, and issues concerning

validity and instrumentation. Section 2 contains the clarification for the methodology.

Section 3, I highlighted results of the data analysis; included implications for social

change, recommendations for further research, summary, reflections and the conclusion.

Section 2: The Project

In Section 2, I provided the research components to this doctoral study. This section includes my purpose of the doctoral study redefined and the steps taken to complete the research process. The steps included the identification of the sample population, data collection from the sample population and the measures taken to protect the identity of the sample population based on the *Belmont Report*. This section also identified the research method and design and a systematic process for data analysis. The results of the data analysis provided an answer to the research question.

Purpose Statement

My purpose in this quantitative correlational study was to examine the correlation between the behavioral marketer's intention to protect ecommerce privacy, attitude, SNs, and PBC as measured by the TPB tool regarding the collection of ecommerce consumer's personal information. The dependent variable was the behavioral marketer's intention to protect ecommerce consumer privacy. The independent variables included the behavioral marketer's attitude, SNs, and PBC. The targeted population for this study was behavioral marketing managers, from the AMA located in the USA. A study of privacy from the behavioral marketer's viewpoint within ecommerce organizations was meaningful based on the expected growth of ecommerce sales and the risk of a security breach (Sen & Borle, 2015). This study contributed to social change by helping marketing leaders understand the correlation between their attitudes, SNs, and PBC concerning an organization's ecommerce information collection processes. This awareness may lead to

strategies, which reduce the amount of information collected or policies to safeguard the consumer's personal information.

Role of the Researcher

Researchers focused on the statistical interpretation of the collected data, and tend to hold the positivist worldview (Mukhopadhyay & Gupta, 2014). Positivists use the logical nature of quantitative data collection to advance knowledge (Mukhopadhyay & Gupta, 2014). Although, Mukhopadhyay and Gupta (2014) used quantitative research to advance knowledge, Dinev, Xu, Smith, and Hart (2013) stated the uniqueness of the variables was lost when the logical order of quantitative research was applied. The analysis of the collected data leads to knowledge (Smith, 2014). I incorporated a cross-sectional correlational research design, to study behavior marketer's intention to protect ecommerce consumer's personal information. Han and Stoel (2017), Shin and Hancer (2016), and Walters et al. (2018) experienced success with their quantitative studies framed with TPB.

In my role, as the researcher, I assumed the responsibility of distributing the Internet-based survey to subject matter professionals, behavioral marketers. Dienlin and Trepte (2015), Schaller, Patil, and Malhotra (2015), and Walters et al. (2018) used an Internet survey tool targeted to a population with prior knowledge of the study subject. Lim (2015) administered an online survey to participants who had experience in ecommerce purchasing. Segmenting in accordance to knowledge or skillsets allows a good presentation of behavioral intentions (Lim, 2015).

Although I am a member of the AMA and the Connecticut chapter of AMA, I was not aware of members with behavioral marketing experience. AMA members from Connecticut may recognize my name from the events I attended or the survey pilot. The letter of introduction asked them to disqualify themselves and opt out of the survey if an association with me existed. If a behavioral marketer from the Connecticut Chapter of AMA received a request to participate in the survey, the risk of bias was low due to the anonymous nature of the survey (Tiwari et al., 2017).

In accordance with the *Belmont Report* protocol, I adhered to the ethical principles of the *Belmont Report*, which includes informed consent, fairness, beneficence, volunteerism, and justice (Bromley, Mikesell, Jones, & Khodyakov, 2015). I did not request personally identifiable information, such as name, employer, or other sensitive information. I was respectful of the participant's time commitment with the convenience of an online survey tool. The online survey tool allows the participants to participate in the survey at a convenient time. The population of behavioral marketers was not part of a protected classification for research purposes. Each participant was over the age of 21 and parental, state, or government permission for participation was not required. Han and Stoel (2017), Tiwari et al. (2017), and Walters et al. (2018) used mature participants for their research with success.

Participants

Identifying individuals with knowledge of the research topic was essential to the success of this study. The participants in this study, behavioral marketers were eligible to participate in this study based on their knowledge of behavioral marketing. This

participant selection was similar to Brahmana et al. (2018), Han and Stoel (2017), and

Raza, Bakar, & Mohamad (2018) who targeted their sample population from individuals

with knowledge of the subject. Tiwari et al. (2017) stated participants with knowledge of

the topic ensured collected data based on business experience.

The AMA provided access to the behavioral marketers by emailing the survey

package to behavioral marketers, who were members of the AMA. The survey package

included consent letter, letter of introduction, and survey document. The survey and letter

of introduction contained my identity as a researcher studying behavioral marketer's

intentions toward ecommerce consumer privacy. A working relationship between the

survey participants and me did not exist.

Describe the sample adequately. Remember, the sample is the subset selected

from the broader population. Thus, it may differ from the targeted population discussed

in Section 1. Detail the major demographic characteristics, for example the type of

business, leader, manager, or title of the participants within the business. As a rule,

describe the groups as specifically as possible, with emphasis on characteristics that may

have bearing on the interpretation of results/findings. Follow the guidance on

requirements for this section provided in the DBA rubric.

Research Method and Design

This section contains a detailed discussion of the research method and design used

to study behavioral marketer's attitude, SNs, and the PBC in relationship to ecommerce

privacy concerns. A study of the behavioral marketer's attitudes, SNs, and PBC regarding

the collection of ecommerce consumer's personal information will contribute to the topic

of consumer privacy. The uniqueness of this study was consumer privacy information was from the behavioral marketer's perspective rather than the consumer.

Research Method

Quantitative methodology was a useful research method when examining behavior and attitudes of a population through sampling (Norris, Plonsky, Ross, & Schoonen, 2015). I selected a quantitative research method to form the basis of this study. Hegner et al. (2017), Norris et al. (2015), and Walters et al. (2018) used quantitative methods to study the behavior and attitudes, of the sample population. A quantitative research project answers the research question and allows replication of the study (Norris et al., 2015). The quantitative method was effective for business related phenomena, whereas interpretation of the data rendered quantitative research sufficient for enterprise applications (Sukamolson, 2016). In enterprise applications, quantitative data allow the researcher to make decisions based on the statistical results of the data analysis (Sukamolson, 2016).

A researcher can add a subjective element with the use of elicitations and coding of published data concerning attitudes, subjective norm, and PBC when performing a phenomenological approach (Ajzen, 1991). The qualitative research method was beneficial for the researcher if the researcher desires to add flexibility and has direct contact with the study population (Farah, 2017). In comparison, a quantitative research study revealed the relationships between the variables and provided the benefit of statistical analysis and a measurement of the three TPB predictors. A sole qualitative method was not suitable for the study of planned behavior based on the analysis of the

three predictors of intention, attitude, SNs, and perceived behavioral control (Ajzen, 1991).

A mixed methods approach works well with TPB. A qualitative design with in-person interviews or focus groups allows the identification of trends in the data (Herrero & San Martin, 2012). The qualitative portion enables the researcher to develop patterns with a new phenomenon whereas the quantitative portion or questionnaire enables the researcher to concentrate on the correlations of the participant's attitude, social norms, and perceived behavioral control (Ajzen, 1991; Ajzen, 2011; Ajzen & Sheikh, 2013). A mixed methods approach was not suitable for this study based on the research question, structured to establish relationship between the variable (Dienlin & Trepte, 2015; Frels & Onwuegbuzie, 2013; Sukamolson, 2016).

In this research study, the quantitative method was suitable to allow the representative sample from the behavioral marketer population to provide answers not readily available from other marketing manager sources. Raza et al. (2018), Shin and Hancer (2016), and Tiwari et al. (2017) targeted participants with experience in the research topic to participate in the survey. The responses from the behavioral marketers will seek to answer the research question regarding the intent to protect the privacy of ecommerce consumers. The effectiveness of quantitative research lies in the diversity and complexity of the research questions (Aiken, West, & Millsap, 2008). Last, the quantitative aspects of the TPB model provided a predictive quality when examining behavioral intentions (Dienlin & Trepte, 2015).

Research Design

The research design is the basis for collecting and analyzing data. The purpose of this quantitative study was to understand the correlation between the behavioral marketer's attitudes, SNs, and PBC regarding the collection of ecommerce consumer's personal information. Although multiple research projects address the issue of consumer privacy, the topic was generally from a consumer's perspective. Researchers Ajzen and Sheikh (2013) used nonexperimental quantitative designs with the TPB survey tool to uncover the participants' attitudes, SNs and PBC. I did not use an experimental design based on the research question. In an experimental design study, the researcher was comparing the effects of one treatment to a no treatment control group (Gonzalez, Lopez, Marcos, & Rodriguez-Marin, 2012; Sánchez, 2013).

Population and Sampling

Marketing managers with experience in behavioral marketing, e-marketing, or target marketing who were members of the AMA located in the USA have the knowledge to complete the survey. The AMA was the largest marketing organization in North America with an international membership of 30,000 marketers in 118 countries (Ormiston, 2014). Only the members from the USA received an invitation to participate in the survey.

The sample of participants came from the population of behavioral marketing managers. Behavioral marketers have knowledge of the subject, ecommerce privacy protection. Raza et al. (2018), Shin and Hancer (2016), and Tiwari et al. (2017) achieved favorable results by focusing on subject matter experts. Each member identified as a

behavioral, target, or e-marketing manager was invited to participate in the Internet-based email questionnaire via Surveymonkey.com. Phillips (2015), Ryan (2017), and Soon and Wallace (2017) used Survey Monkey to administer online surveys effectively. A question at the beginning of the survey identified the participation sample of e-marketing managers with experience in behavioral marketing. Marketing managers, who have behavioral, e-marketing, or target marketing experience will have the necessary knowledge of ecommerce consumer privacy as it relates to behavioral marketing and be able to respond to the questionnaire from a knowledge base of behavioral marketing.

Convenience sampling a nonprobability sampling technique was the preferred sampling method for this study. Hegner et al. (2017), Mikhed and Vogan (2018), and Shin and Hancer (2016) identified a sample population based on the nonprobability sampling technique of convenience sampling. Convenience sampling was useful for both quantitative and qualitative research method because it allows the researcher to select the sample from a population of individuals with knowledge or experience of the research topic (Hegner et al., 2017; Mikhed & Vogan, 2018; Shin & Hancer, 2016). Convenience sampling was similar to purposive sampling, but the two sample methods differ in sample size determination (Walters et al., 2018).

Like convenience sampling, purposive sampling was a random process useful for targeting the desired sample from a larger population (Farah, 2017). Purposive sampling method also focuses on the subject matter professionals (Jayaraman, Arumugam, Kumar, & Kiumarsi, 2018; Walters et al., 2018; Wu, 2015). Purposive sampling was useful for successfully recruiting research participants from a professional organization based on

their expertise (Walters et al., 2018). Comparing purposive sampling to convenience sampling rendered one disadvantage. It takes longer to acquire the appropriate sample size with purposive sampling (Jayaraman et al., 2018). Both convenience and purposive sampling methods were suitable for this research study, but the determination of the sample size rendered convenience sampling the best sampling method to collect data from behavioral marketers. Convenience sampling required a sample size determination because convenience sampling was a nonprobability selection process (Jackson, 2018).

The sample size was critical for quantitative research studies (Xiao & Askin, 2014). The appropriate sample size reduces type II errors and ensures the sample size results in an adequate confidence interval (Davcik, 2014). The sample size for this study was estimated with the G*Power 3.1.9. software program. Davcik (2014), Faul, Erdfelder, Buchner, and Lang (2009), and Liu (2013) used the G*Power software package to determine the appropriate sample size. The sample selection presented a clear view of reality, in the population (Davcik, 2014). A sample with less than the required participants will not return the desired research results (Liu, 2013).

Bosco, Singh, Aquinis, Field, and Pierce (2015) stated a medium effect size related to behaviors such as attitude and intentions were between $/r/$ .10 and .25. The effect size for this study was .15. Based on parameters of the power of $1 - \beta = .80$, the error probability of 95% ($\alpha = .05$), and the number of predictor variables set at three, the appropriate study sample size was 54. I estimated a sample size using G*Power 3.1.9.2 based on assumptions for alpha err probability, power (1-β err probability), and effect size. Davcik (2014), Faul, Erdfelder, Buchner, and Lang (2009), and Haenlein and

Kaplan (2011) used G*Power software to obtain an appropriate sample size. The correct

sample size reduces the risks of error and allows accurate analysis of the data (Bosco et

al., 2015; Faul et al., 2009).
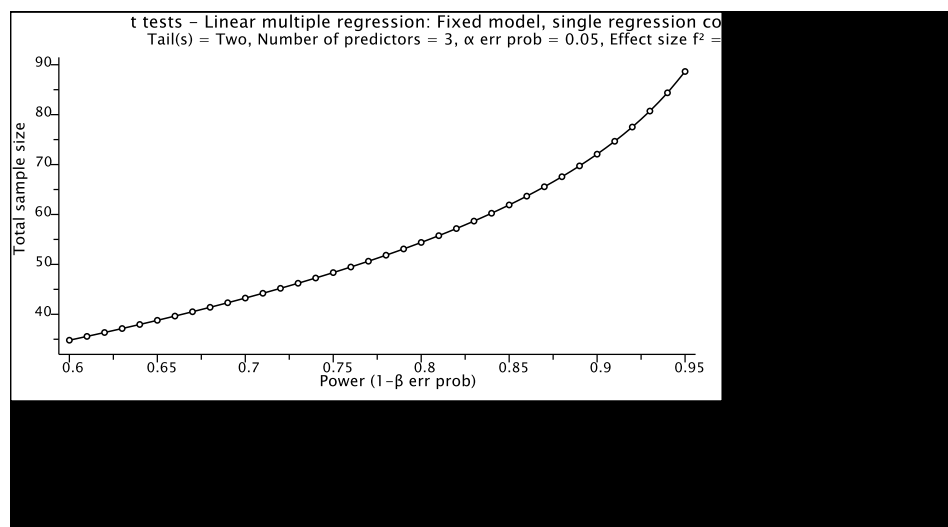
Figure 1. Power as a function of sample size

The premise of a two-tailed t-test, using the parameters of the power of error

probability of 1- β = .80, the error probability of 95% (α =.05), and the numbers of

predictors set at three, the appropriate study sample size was 54 as shown in figure 1.

Increasing the power of error to .95 (1 – β = .95 would yield a higher sample size of 98.

The effect size of .15 was suitable for this research study. Bosco et al. (2015), Davcik

(2014), and Liu (2013) realized a medium effect size of .15 to be suitable for similar

research projects. Understanding the sample size as it relates to the effect size determines

the correct sample size to reduce type II errors (Davcik, 2014).

Ethical Research

The *Belmont Report* is a standard guideline for human research participants

(Rogers & Meek Lange, 2013). The *Belmont Report* identifies several vulnerable

categories for human research (Bromley et al., 2015; Health & Human Services (HHS), 1979; Rogers & Meek Lange, 2013). The vulnerable groups included racial minorities, economically disadvantaged, and institutionalized individuals. The target participant population may have included racial minorities, but the participants were not vulnerable or underage. Decision trees within the *Belmont Report* assisted in the determination of whether pending research projects involved protected individuals (Bromley et al., 2015; HHS, 1979; Rogers & Meek Lange, 2013). Ethical research procedures in the *Belmont Report* provide a safe and protective environment in which to conduct research. The two areas of concern in the *Belmont Report* included informed consent and fairness for research participation (Bromley et al., 2015; Rogers & Meek Lange, 2013). This section included the ethical process I followed to gather data for this ecommerce privacy study.

Informed Consent

Walden University requires students obtain Institutional Review Board (IRB) approval for research projects. I obtained approval from Walden University's IRB to comply with the standards and principles of ethical research as outlined by Walden University. A copy of the consent form was available on the survey link. Each participant had an opportunity to read the consent form. The form contained a description of the ecommerce privacy study, background information regarding the study, and the purpose for the research. The consent form contained the approval from the IRB to conduct the research by the assignment of IRB approval number 02-02-18-0329556. Each participant had the capacity to give consent and fell within the principle of fairness (Rogers & Meek Lange, 2013). The participants received a contact email address and a contact phone

number for questions regarding the study. Hegner et al. (2017), Mikhed and Vogan (2018), and Shin and Hancer (2016) used this form of contact effectively in their research studies.

Participation was voluntary. Each participant had the option to opt out of completing the survey. Hegner et al. (2017), Mikhed and Vogan (2018), and Shin and Hancer (2016) allowed the participants to opt out of the survey maintaining voluntary status. Each participant had opportunity to decline the invitation (Hegner et al., 2017; Mikhed and Vogan, 2018; and Shin and Hancer, 2016). The survey contained a button to opt out of the survey. When the participant clicked the button to opt out, a thank-you message appeared, and the survey closed. Incentives were not included as a tool to encourage participation (Curras-Perez, Ruiz-Mafe, & Sanz-Blas, 2014). I based the decision not to use a stimulus or incentives on personal finances, although incentives increase survey participation rates (Cavazos, 2013; Cavazos & Varadarajan, 2012; Holliman & Rowley, 2014).

Ethical protection of each participant was adequate. The survey design protected the identities of participant. Hegner et al. (2017), Mikhed and Vogan (2018), and Shin and Hancer (2016) used the TPB survey tool to examine behaviors and attitudes of individuals without revealing their identities. Using the TPB survey tool provided protection in three ways: First, the survey was anonymous. The identities of each participant were unknown. Second, the demographic information requested at the beginning of the survey was for classification purposes. Last, each participant was not

part of a vulnerable group and participants were not required to provide sensitive information.

The consent form contained a statement regarding the safe storage and destruction of the pertinent research documents required by the IRB. Carr (2015), Gubrium and Holstein (2002), Moreno, Goniu, Moreno, and Diekema (2013) referenced the importance, the informed consent process and handling of research documents play in scholarly research. A safety deposit box at a local bank, in Enfield, CT provided a safe location for the research documents for 5 years. The Enfield, CT location provided local access for easy retrieval.

Data Collection Instruments

Quantitative research designs require a reliable instrument to collect data. I elected to use the TPB questionnaire survey instrument developed by Ajzen as a useful survey tool to capture an individual's future intention toward a behavior (Ajzen, 2006). Hegner et al. (2017), Walters et al. (2018), and Wu et al. (2018) used the TPB survey tool to examine behaviors and attitudes of individuals who can implement changes. I incorporated responses from behavioral marketers, individuals who can implement changes. An understanding of ecommerce consumer privacy from the behavioral marketer's perspective rather than the ecommerce consumer allowed the behavioral marketer an opportunity to make the needed changes to protect ecommerce consumers from privacy invasion or security breach.

The instrumentation used for this research project was useful for understanding the future intentions of the participants, behavioral marketers. My survey tool contained 4 sections and 15 total questions. Fortes and Rita (2016), Tiwari et al. (2017), and Zampetakis, Bakatsaki, Litos, Kafetsios, and Moustakis (2017) designed their TPB survey tools in a similar manner. The questions solicit responses related to the variables, intentions, attitude, social norms, and PBC. Tiwari et al. (2017) used the TPB tool to study the correlation between the independent variables, attitude, SNs, and PBC and the dependent variable intention. The TPB survey tool measured the degree of correlation between the variables, which resulted in behavioral marketer's intention to limit the amount of personal information collected or seek strategies to safeguard the personal information. Intention toward a future action was a function of the behavioral marketer's attitude, SNs, and PBC (Fortes & Rita, 2016; Tiwari et al., 2017; and Zampetakis et al., 2017). The TPB variables attitude, subjective norm, and PBC influence the degree to which an individual's intent to perform the behavior (Ajzen & Sheikh, 2013). Behavioral marketers adopted favorable or unfavorable attitudes automatically as new information about the subject was acquired (Sanne & Wiese, 2018). The three variables worked together to determine the manager's intention toward a future action (Ajzen & Sheikh, 2013). The variable attitude measured the extent behavioral marketers were concerned about ecommerce consumer privacy (Sanne & Wiese, 2018). A behavioral marketer's ambivalence toward ecommerce consumer privacy will affect the manager's attitude toward protective measures (Jackson, 2018). For example, a strong ambivalence toward a subject results in a weak attitude toward the subject (Jackson, 2018). A behavioral

marketer's weak attitude was associated with a weak association between behaviors and intentions (Ajzen & Sheikh, 2013; Tiwari et al., 2017). A manager with a strong attitude toward ecommerce consumer privacy exhibits behaviors or intentions to protect the personal information (Ajzen & Sheikh, 2013; Tiwari et al., 2017).

SNs were social practices based on the expectations or opinions of other individuals regarded as important (Shin & Hancer, 2016). Behavioral marketer's base their SNs on the beliefs or interests of peers (Tiwari et al., 2017). The views of the behavioral marketer's peer or reference group influence whether the behavioral marketer's intention will limit the amount of collected information, if the peer group approved of the behavior (Shin & Hancer, 2016). The behavioral marketer based his or her SNs on the degree of relationship the manager has with his or her peer group (Shin & Hancer, 2016).

The last variable perceived behavioral control measured the behavioral marketer's judgment of how well he or she can accomplish the course of action (Ajzen, 2011). Perceived behavioral control measures the behavioral marketer's degree of difficulty or ease of limiting ecommerce consumer's personal information (Shin & Hancer, 2016). A high degree of perceived behavioral control added strength to the behavioral marketer's intention to limit the amount of ecommerce consumer's personal information (Ajzen, 2011). Perceived behavioral control was the behavioral manger's intention to implement the behavior of limiting the amount of ecommerce consumer's personal information (Shin & Hancer, 2016). A study of the three variables, attitude, social norms, and PBC

provided insight into the behaviors and intentions toward safeguarding ecommerce consumer's personal information.

The survey tool based on the 7-point Likert scale contained 15 questions with seven options. Fortes and Rita (2016), Tiwari et al. (2017), and Zampetakis et al. (2017) used the same 7-point Likert scale survey format. I programmed the survey tool to accept only one response per question. This design reduced the number of disqualified surveys due to entering more than one answer per question. Tiwari et al. used this approach to reduce the number of disqualified survey forms. Each response to the survey question corresponded to a numerical value. For example, each response had a quantifiable value ranging from *strongly disagree* (1) to *strongly agree* (7). This scale allowed variance between the constructs, attitude, SNs, and PBC (Fortes & Rita, 2016). Fortes and Rita (2016), Sanne and Wiese (2018), and Tiwari et al. (2017) used this scale for variance between the constructs. The higher the score, the more favorable the participants were to protecting ecommerce privacy concerns. This data allowed the calculation of descriptive statistical analysis, Cronbach's alpha, and regression analysis.

The scales of measurement that described the attributes of the data included scale data, ratio and interval, nominal, and ordinal data. Nominal and ordinal data was required to collect text information and numerical data for analysis. Han and Stoel (2017), Shin and Hancer (2016), and Walters et al. (2018) used text data to identify categories and numerical data for analysis. The nominal data included the name of categories and variables. The scale data, which included the numerical responses from the participants using the 7-point Likert scale formed the basis of analysis using multiple regression

analysis. Jayaraman et al. (2018), Kassim et al. (2017), and Wolf, Weibenberger, Wehner, and Kabst (2015) achieved favorable results with multiple regressions to analyze data for each variable. The scores for each question range from 1 to 7, with 1 equal to *strongly disagree* and 7 equal to *strongly agree*. I calculated a raw score for each participant, in each of the four sections using a weighted average formula (Ajzen, 1991).

This research study was one of few studies, which viewed ecommerce consumer privacy from the behavioral marketer's perspective. The existing literature revealed ecommerce privacy from the consumer's point of view. A division exists in the importance of privacy among ecommerce consumers resulting in two schools of thought (Milne et al., 2017). The first school of thought states privacy protection was not necessary based on the amount of information on social media and the use of loyalty cards (Lwin et al., 2016; Milne et al., 2017). The second school of thought states privacy was a consumer right in need of protection or regulation from security breaches (Campbell et al., 2015). The goal of this study was a better understanding of ecommerce consumer privacy from the behavioral marketer's perspective in an environment where security breaches were common.

Reliability in quantitative research was a measure of internal consistency of the research tool (Caramelli & Van De Vijver, 2013). There were several methods for determining reliability, including Cronbach's alpha, McDonald's omega, and test and retest (Caramelli & Van De Vijver, 2013). The reliability and validity of the TBP survey tool required testing. Although TPB was a valid widely used survey tool, modifications to

the survey tool to adapt the tool to the study of behavior marketers required reliability and validity testing (Kassim et al., 2017; Liu et al., 2019; Tiwari et al., 2017;).

As an internal validity measure, Cronbach's alpha related to the variance and covariance of the survey questions. Bonett and Wright (2015), Fortes and Rita (2016), and Kassim et al. (2017) used Cronbach's alpha to measure internal consistency with a reliability of 0.7 or greater. The closer the results were to one the higher the degree of reliability (Ajzen, 2011). The Cronbach's alpha statistic was popular with social and behavior research (Bonett &Wright, 2015; Hegner et al., 2017; Tiwari et al., 2017). A Cronbach's alpha reliability of greater than 0.7 is indicative of high reliability, whereas a researcher should reject a reliability of less than 0.50 (Jayaraman et al., 2018). Jayaraman et al. (2018) suggested that reliability 0.50 had a moderate consistency whereas a reliability of 0.7 or greater represented a high reliability. A reliability of 0.70 or greater was suitable for this research project. Inclusive with reliability, a second quality feature was validity.

A research project has several validity checks, construct validity, internal validity, and, external validity. Construct validity with the TPB research tool was present until a modification of the survey tool takes place, which changed the measurement structure (Ajzen, 1991). Ajzen (1991) designed the research survey to maintain construct validity. I maintained the same structure of the original survey tool. I modified the wording to address the research questions of this project, thus maintaining construct validity.

Internal validity involves the number of participants in the study and the number of valid responses (Gonzalez et al., 2012). I determined internal validity by controlling

for the threats to internal validity. The threats include history, regression, selection, mortality, and diffusion of treatment. I controlled most of the threats, history, selection, mortality, selection, and diffusion of treatment by administering the survey twice; once as a pilot and the actual survey distribution. Randomization of the sample selection eliminated the threats to internal validity (Keele, McConnaughy, & White, 2012). Gonzalez et al. (2012), Keele et al. (2012), and McGrath and Brinberg (1983) argued randomization or generalization of the sample population was one method for controlling external validity. There was the risk of extremely high and low scores with the regression process, but the threat was minimal. I would have repeated the survey if extremely highs and lows occur. Liu et al. (2019), Shin and Hancer (2016), and Tiwari et al. (2017) measured internal validity between the constructs with confirmatory factor analysis (CFA). CFA was suitable for samples size greater than 30 but less than 500 (Zolait, 2014). Last, I achieved internal validity with the appropriate sample size and randomization of the sample.

External validation was related to drawing incorrect inferences from the sample (Gonzalez et al., 2012). The threats to external validity include generalizations to sample population based on a different set of circumstances (Lynch, 1982). Lynch (1982) identified three threats to external validity, statistically generalizability, conceptual replicability, and realism. Statistical generalizability relates to the use of probability sampling to select a sample population that represents the general population. Conceptual replicability indicates a different researcher can replicate the experiment at a different time, with a different sample (Lynch, 1982). Last, Lynch indicated the more realistic the

experiment, the easier to generalize the results of the experiment. I controlled external validity by removing the threats of statistical generalizations by using a random sampling process and maintain replicability by following similar experiments. Lynch, McGrath and Brinberg (1983), and Wijnhoven and Bloemen (2014) found the two aspects random sampling and replicability to be important in the control of external validity.

The perspective researcher adjusts the TPB survey tool based on the research topic (Ajzen, 2011). The tool modification or adjustment considers the various behavioral subjects (Kassim et al., 2017; Jayaraman et al., 2018; and Wolf et al., 2015). The same formats of the questions appear for each administration of the survey tool (Kassim et al., 2017). Ajzen (1991) designed the questions to collect information related to behavioral intentions, attitudes, SNs, and PBC. For example, a question to collect data related to the participant's intention toward an evidence-based practice or behavior follows. I plan to employ evidence-based practices into my treatment practices for clients. The same question for behavioral marketer's ecommerce privacy concern: I plan to implement ecommerce privacy practices into my daily work with ecommerce advertisement development. This interchangeability made the TPB tool an easy and consistent tool for researchers (Kassim et al., 2017; Jayaraman et al., 2018; and Wolf et al., 2015). Although the TPB survey was a widely used survey tool, I applied Cronbach's alpha to confirm validity and reliability of the tool in my application.

The permission to use the TPB survey tool was included in Appendix A. The tool does not require formal approvals, only a citation when referencing the tool. Ajzen (2006) provided the conditions for incorporating the TPB survey into student research.

Ajzen also provided instruction for constructing the survey tool based on obtaining

behavioral information from the variables, intention, attitude, SNs, and PBC. A copy of

the survey tool was in Appendices B. I stored the raw data in a safety deposit box located

in Enfield, Connecticut for 5 years. The data was available upon request.

Data Collection Technique

The importance of data collection for quantitative studies cannot be understated.

Data collected from a sample not representative of the population may result in erroneous

conclusions (Xiao & Askin, 2014). The capability of numerically analyzing data in

quantitative studies allows inferences concerning the data (Sukamolson, 2016). I

collected the data through an online survey directed toward the subject matter

professionals. Fortes and Rita (2016), Kassim, et al (2017), and Shin and Hancer (2016)

reached accurate conclusions by collecting survey data from individuals with knowledge

of the subject. An online survey was less intrusive on the participant's busy schedules

than face-to-face interviews (Jackson, 2018). The subject matter professionals were busy

professionals; therefore, an online survey allowed the participants to complete the survey

when their schedule allows free time. Hegner et al. (2017), Shin and Hancer (2016), and

Walters et al. (2018) noted the convenience of an online survey for the participants. The

major advantage of an online survey compared to face-to-face questionnaires was that

participants had privacy when they completed the survey and not feel pressure to comply

(Hegner et al., 2017; Shin & Hancer, 2016; Walters et al., 2018).

A pilot survey ensures functionality, wording, and clarity of the survey document

(Sanne & Wiese, 2018). I conducted a pilot study to ensure functionality of the survey

document. Liu et al. (2019), Peiris, Kulkarni, and de Silva Mawatha (2015), and Sanne and Wiese (2018) conducted pilot studies to test the reliability of the questionnaire. Members of the Connecticut chapter of AMA participated in the pilot survey to ensure functionality of the questionnaire. The pilot survey period was approximately 2 weeks. The population of AMA members based in Connecticut was small and this population was not included in the survey distribution. A month was the average time required to conduct a pilot survey (Guarte & Barrios, 2006). Although, Liu et al., Peiris et al., and Sanne and Wiese allowed longer survey completion times, I elected to open the pilot survey for 2 weeks in the interest of time. Required adjustments to the survey tool took place based on the feedback of the pilot survey (Liu et al., 2019; Peiris et al., 2015; Sanne & Wiese, 2018).

Data Analysis

The purpose of the data collection was to answer the research question using statistical methods. The research question drove the data analysis. The statistical tests and methods utilized during research answered the research question and provided a basis to accept or reject the hypothesis. The research question for this study was:

What was the degree of correlation between behavioral marketer's attitudes, SNs, and PBC, as measured by the TPB tool, regarding the collection of ecommerce consumer's personal information?

H_{01}: There was not a significant correlation between the behavioral marketer's attitudes concerning the collection of ecommerce consumer's personal information.

H_{a1}: There was a significant correlation between the behavioral marketer's attitudes concerning the collection of ecommerce consumer's personal information.

H_{02}: There was not a significant correlation between the behavioral marketer's SNs concerning the collection of ecommerce consumer's personal information.

H_{a2}: There was a significant correlation between the behavioral marketer's SNs concerning the collection of ecommerce consumer's personal information.

H_{03}: There was not a significant correlation between the behavioral marketer's PBCs concerning the collection of ecommerce consumer's personal information.

H_{a3}: There was a significant correlation between the behavioral marketer's PBCs concerning the collection of ecommerce consumer's personal information.

There were several software packages to analyze statistical data. I chose the Statistical Package for Social Science (SPSS), version 25, to provide the statistical analysis for this study. Farah and Maya (2017), Sanne and Wiese (2018), and Tiwari et al. (2017) used the SPSS software package to analyze the results of their quantitative research. I collected the survey data from Survey Monkey and downloaded the data into a spreadsheet in preparation for SPSS analyses.

A descriptive analysis for each of the constructs was the first statistical measurement to reveal the central tendencies of the sample. Tiwari et al. (2017) stated descriptive analysis data improves the understanding of sample frequencies. Han and Stoel (2017), Shin and Hancer (2016), and Tiwari et al. conducted a descriptive analysis of their collected data to reveal the central tendencies. This descriptive analysis included a calculation of the mean, standard deviation, and the correlation between the variables.

Knowing the mean (μ) assisted in the understanding of the relationship between the behavioral marketer's attitude toward protecting ecommerce consumer privacy, SNs, PBC, and the behavioral marketer's intentions toward protecting ecommerce consumer privacy. A score higher than four would indicate study participants were familiar with ecommerce consumer privacy and have positive attitudes toward ecommerce consumer privacy (Walters et al., 2018). The standard deviation (SD) for the sample provided information on the variance or dispersion of the data (Riquelme & Roman, 2014). The next statistical measurement will be Cronbach's alpha statistic.

Cronbach's alpha was one of several reliability measures. The list of possible reliability measures included confirmatory factor analysis (CFA), exploratory factor analysis (EFA), and the goodness of fit measures, (GFI), adjusted goodness of fit (AGFI), normed index fit (NFI), comparative fit index (CFI), root mean index (RMR), and, root mean square error of approximation (RMSEA). I utilized Cronbach's alpha for internal validity and reliability of the questionnaire. Fortes and Rita (2016), Kude et al. (2017), and Liu et al. (2019) used Cronbach's alpha and CFA to evaluate the quality of each question. Quantitative researchers use the EFA in psychological and educational research (Williams, Brown, & Onsman, 2010).

The sample size was a factor in EFA. EFA requires a sample size of 100 to 300 useable responses (Williams et al., 2010). Due to the estimated sample size of 54 for this study, EFA was not suitable for this study. I used Cronbach's alpha to determine the reliability of the variables. Fortes and Rita (2016), Kude et al. (2017), and Wolf et al. (2015) experienced good results with Cronbach's alpha and CFA reliability measures.

The next statistical measure was a multiple regression analysis. I made the decision to use multiple regression analysis based on the results of previous research. Ajzen and Sheikh (2013), Liu et al. (2019), and MacCann, Todd, Mullan, and Roberts (2015) used multiple regression analysis to calculate the degree of relationship or correlation between the dependent variable and two or more independent variables. The one-way analysis of variance (ANOVA) tested the hypothesis (Ajzen & Sheikh). The ANOVA measured the means of each construct to determine if the means were equal (Ajzen & Sheikh). If the means were equal then the null hypothesis would be accepted (Ajzen & Sheikh, 2013). Ajzen and Sheikh, MacCann et al., and Liu et al. used ANOVA to test their hypotheses.

The largest barrier to obtaining reliable responses was the response rate (Milne et al., 2017). An adequate response rate was indicative of the sample quality (Jackson, 2018). My target response rate was 50%. Hegner et al. (2017), Soon and Wallace (2017), and Tiwari et al. (2017) realized adequate response rates 50% or greater. Whereas a 50% response rate was desirable, Mine et al. stated a response rate of 12% was typical for Internet surveys.

The second largest barrier for obtaining reliability was a construct reliability of less than 0.70. Tiwari et al. (2017), Walters et al. (2018), and Wolf et al. (2015) stated the construct reliability should have a Cronbach's alpha 0.70 or greater. A reliability of less than 0.70 required deletion from the study (Ryan, 2017). A reliability of less than 0.70 may be a significant barrier. Weak constructs compromise the integrity of the data and produce incorrect correlations (Wolf et al., 2015). Incorrect correlations result in Type I

and Type II errors (Wolf et al., 2015). Haenlein and Kaplan (2011) defined *Type I errors* as the probability of incorrectly rejecting the null hypothesis or finding a relationship between the variables, which do not exist, whereas Type II errors include failing to find a relationship between the variables, when a relationship exists, respectively. Echambadi et al. (2006) stated inadequate construct measurement leads to divergent findings in research. Achieving good research results begins with a reliable and valid survey tool (Ajzen, 2011; Wolf et al., 2015). The validity of the constructs allows the researcher to match the sample population to the overall population (Wolf et al., 2015).

Avoiding errors in the analysis process require data cleaning (Karam & Ralston, 2016). Data cleaning was a step researchers overlooked prior to transferring data from data collection tool to a statistical database (Karam & Ralston, 2016). I reviewed the data in Excel format to identify missing information and delete the missing data or entries. Cole (2008), Karam and Ralston (2016), and O'Reilly & Kumar (2016) used the screening process prior to inputting the information into the SPSS database. The data process includes checking for missing data and incomplete survey forms. A 5% ratio for missing data was common (Karam & Ralston, 2016). It was possible to identify missing data by a default setting in SPSS called case wise or pairwise deletion. Deletion by case wise or pairwise may negatively affect the sample size by deleting the entry or record (Karam & Ralston, 2016). Another solution for missing data involved the researcher filling in the missing blanks (Karam & Ralston, 2016). This method may skew the results and underestimate the sample parameters (Karam & Ralston, 2016). I avoided sample size reduction by programming the survey tool, which required the participants to answer

all questions. Reduction of the sample size leads to power loss and miscalculation of the population and sample parameters (DeSimone, Harms, & DeSimone, 2015; Karam & Ralston, 2016).

The three assumptions of the study included behavioral marketers will have the information required to answer the survey questions, the response rate will yield an adequate sample size which was representative of the population and protecting ecommerce privacy was important to behavioral managers. I addressed the first assumption of behavioral marketers possessing the required information to complete the survey based on the responses from the behavioral marketers. If the sample of behavioral marketer's responses resulted in a sample size of less than 54, I would re administer the survey until an adequate sample size is obtained. The second assumption was the population of behavioral managers producing a sample size of 54 participants or greater. I addressed this assumption by sending weekly reminders to behavioral marketer within the AMA until an adequate sample size was present. Bootstrapping is a method for resampling and normalizing the distribution (Psaradakis, 2016).

The process of bootstrapping takes a sample from the sample population and calculates the samples mean (Psaradakis, 2016). The bootstrapping method was useful when assumptions of normality arise, the size of variance was large, and the sample size may not be large enough for statistical testing (Karam & Ralston, 2016; O'Reilly & Kumar, 2016; Psaradakis, 2016; Xu, Yang, Chen, & Yu, 2015). Although resampling was more appropriate for ANOVA procedures rather than regression analysis, I did not use

the bootstrapping method because the sample size of 84 was adequate for analysis

(DeSimone et al., 2015).

The third assumption relates to the importance behavioral marketers place on

protecting ecommerce consumer's personal information. If the intentions of behavioral

marketers placed a high value on protecting ecommerce consumer's personal information

then the relationships between the variables will be significant (Ajzen & Sheikh, 2013).

On the other hand, if the responses from the behavioral marketers indicated ecommerce

consumer privacy was not important, then another study may be useful to understand the

intentions of behavioral marketer's risk factors for preventing a security breach (Benson

et al., 2015).

A test for the assumptions included a positive correlation. A positive correlation

in which the *R* value represents a value between 0 and + 1 (Ajzen & Sheikh, 2013;

MacCann et al., 2015). An R value of 0 was indicative of no relationship (MacCann et

al., 2015). The R^2 value indicates the strength of the effect size a predictor variable has on

the dependent variable (Moore, McCabe, Duckworth, & Sclove, 2003). Moore et al.

(2003) stated eta squared or η^2 for ANOVA procedures and *R2* for regression analysis

provide the direction of a correlation and an indicator of the effect size of the dependent

variable.

Conducting a multiple regression analysis required inputting data into the SPSS statistical

database. The statistical correlation between the dependent and independent variables

resulted in the effect size of the variables (Moore et al., 2003). The decision to accept or

reject included a comparison of the *p* value. The null hypotheses will be accepted if *p* >

.05 (Moore et al., 2003).

Study Validity

Control of internal and external validity threats increases the validity of research

findings and controls or eliminates Type I and Type II errors (Bonett & Wright, 2015).

The internal validity factor included the selection of participants (Campbell et al., 2015).

The convenience sampling method was a nonrandom process, whereby the participants

have an equal chance of selection (Walters et al., 2018). The survey tool distribution to

the population of behavioral marketing managers minimized the internal threat to

validity. Jayaraman et al. (2018), Kassim et al. (2017), and Walters et al. (2018) targeted

a sample population of individuals with knowledge of the study topic, to minimize the

internal threat. The external factors included survey standardization, sample size,

statistical conclusion validity, and construct validity (Bonett & Wright, 2015).

The TPB survey model was an established survey tool (Han & Stoel, 2017). An

established survey tool minimizes the external threat to validity (Ajzen & Sheikh, 2013).

The sample size was a core factor in survey administration (Liu, 2013). The sample size

determined the statistical power of the sample (Liu, 2013). The sample size of 54 based

on a G*Power analysis was small. A small sample size increased the size of the

confidence intervals and the effect of the statistical tests (Haenlein & Kaplan, 2011;

Nesterkin & Ganster, 2015; Rogelberg & Stanton, 2007). Nonresponse rates adversely

affect small sample sizes (Nesterkin & Ganster, 2015). Historically, low response rates to

email surveys have increased since 1989 (Nesterkin & Ganster, 2015). Low response

rates change the sample means and increase standard errors (Nesterkin & Ganster, 2015).

Attempts to increase the response rate included a cover letter and invitation to the survey,

which motivated the participants to open the survey, complete, and submit the survey

(Heerwegh & Loosveldt, 2009). In addition, reminders were sent to participants to

increase response rates (Nesterkin & Ganster, 2015). Increasing the sample size was

accomplished by motivating participants with a weekly reminder to take the survey which

explained the participant's participation to the value of the research (Nesterkin &

Ganster, 2015).

Statistical conclusion validity was the process of reaching false assumptions

(Haenlein & Kaplan, 2011). False assumptions include Type I and Type II errors,

reliability of the survey tool, data assumptions, and sample size. Quantitative researchers

reduce Type I and Type II errors by maintaining an adequate sample size that represents

the population and by the confidence interval. Conversely, decreasing the probability of a

Type I error increases the probability of a Type II error. Cronbach's alpha statistic

determined the reliability or constructs validity of the survey tool. An alpha statistic of

0.07 was adequate for studies framed in TPB (Liu et al., 2019). The error of incorrect

data assumptions occurs when the sample size was not large enough to produce correct

assumptions or the sample size does not represent the population (Haenlein & Kaplan,

2011). The right sample size was tantamount to reducing errors in statistical analysis

(Nesterkin & Ganster, 2015). I used a power analysis to determine the proper sample size

thus reducing statistical data analysis errors. A sample size that represented the

population will reduce Type I and Type II errors and data assumptions (Nesterkin &

Ganster, 2015).

The ability to generalize the findings to a larger population was dependent on

randomization of the sample, replicability, and realism of the study (Campbell & Stanley,

2015; Lynch, 1982). The sampling method was important to the generalization of

research (McGrath & Brinberg, 1983). I incorporated a random sample from the

population of behavioral marketer's responses to the online survey. The random sampling

of behavior marketing managers was representative of the population of behavioral

marketing managers. Another researcher will be able to replicate the study with a random

sample of behavioral marketing managers. Replicability was difficult when the

knowledge base of the population was varied (Lynch, 1982). Sampling a population of

marketing managers would not yield the same results. In this study, the population of

behavior marketing managers had similar backgrounds and knowledge bases. The similar

backgrounds will allow replication of the study. Lynch (1982) stated the more realistic

the study the easier to generalize the results. Ecommerce privacy from the behavioral

marketing manager's viewpoint was realistic as ecommerce sales increase each year

(Tamimi & Sebastianelli, 2015).

Transition and Summary

Section 2 included an examination of the quantitative research method and

correlational design. I included a comprehensive description of the population sample,

the location of the sample participants, and the number of participants required. A

method for determining reliability and validity of the research tool was present. Last, this

section contained data analysis information ensuring the applied research will answer the research question.

In Section 3, I provided a presentation of the research findings. An explanation of how the results will affect professional practice. A discussion of how this study may contribute to change social change was included and recommended action(s). The recommendations for future research were valuable to future scholars. The readers of this research project may identify gaps in the current literature resulting in expansion of the behavioral marketing topic. The last section contains my reflections. My reflections on the intentions of behavioral marketers were significant based on the lack of ecommerce privacy research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

My purpose in this quantitative correlational study was to examine the correlation between the behavioral marketer's intention to protect ecommerce privacy, as it relates to their attitude, SNs, and PBC, as measured by the TPB tool regarding the collection of ecommerce consumer's personal information. In Section 3 I address the results of the study. It begins with an introduction, followed by sections on (a) presentation of findings, (b) application to professional practice, (c) implications for social change, (d) recommendations for action, (e) recommendations for further research, and, (f) reflections

Presentation of the Findings

The research question that formed the base of this DBA study was: What was the correlation between behavioral marketer's attitudes, SNs, and PBC, regarding the collection of ecommerce consumer's personal information. I collected data for this quantitative DBA study through a survey (N = 84) of behavioral managers, who were members of the AMA. A pilot survey was administered to members of the Connecticut Chapter of AMA identify errors and opportunities for improvement. I corrected the pilot survey to remove a duplicated question. The administrative staff of the AMA distributed the corrected survey to behavioral marketers through Survey Monkey. The population of behavioral managers totaled 546. Total responses equaled 126, 42 responses were disqualified because the participant lived outside of the USA. The response rate was 23%.

Confidentially of the participants was maintained because I did not have access to email addresses or other member related data. The survey administrator sent the survey via email to each participant based on job title. Each participant received a copy of the consent form and allowed to opt out of taking the survey. The AMA administrators sent the survey twice, during the winter of 2019, in a 4-week period to ensure an adequate convenience sample.

I exported the data from Survey Monkey into SPSS. I analyzed the data using SPSS version 25. I conducted an analysis for each of the 3 hypotheses. The analyses included descriptive information, validity, correlational, multiple regression, and ANOVA. The descriptive analysis included a comparison of the means, standard deviation, and skewness. I measured each item on a 7-Liket scale with 1 representing "extremely disagree" or "unlikely" extremely and 7 representing "extremely agreeable" or "extremely likely".

Table 1

Demographics of Sample Population

Experience	%
10+	52%
5 - 9	21%
2 - 4	18%
≤ 1	10%

Table 2

USA Regions

Area	%
Midwest	36%
Eastern	29%
Southern	19%
Western	16%

The demographics of the participants are listed in table 1 and table 2. This

information included age as a qualifier. All participants were 21 years of age. Experience

in years as a behavioral marketer, including the city, and state where each participant

worked. More than half of the sample had 10 or more years of experience. The

descriptive data is shown in table 3. I averaged the means for each variable for simplicity.

The results of the descriptive analysis were summarized in table 3.

Table 3

Descriptive Statistics

	A	SN	PBC	I
Mean	5.00	4.7	4.25	4.87
SD	1.46	1.65	1.64	1.45
Skewness	-0.71	-0.73	-0.18	-0.78
Cronbach α	0.837	0.817	0.812	0.873

Note. n = 84.

The means were above 4 for the four variables however the distribution was

negatively skewed for the four variables due to the extreme values. The participant's

attitudes were more agreeable to protecting ecommerce consumer's privacy. The

participants were aware their social norms expected them to protect ecommerce

consumer's privacy and they have the capacity to implement ecommerce privacy

strategies into their work but were not strongly inclined to make the changes.

Reliability and validity of the variables were measured by Cronbach's alpha.

Dienlin & Trepte (2015) suggested a Cronbach's Alpha of 0.7 or greater using a 7-point

Likert scale was a fitting measure of reliability. The survey data resulted in a Cronbach's alpha of 0.8 indicating strong reliability of the variables used in the TBP survey tool. All variables were retained because there was not a lot of variance between the variables. The next statistical analysis included multiple regression analyses. The multiple regression analysis measures the degree of correlation between the dependent variable and two or more independent variables.

The multiple regressions statistical test resulted in a weak relationship between the variables. Attitude was the only variable with a positive correlation. Norms and PBC reflected a negative relationship. Ryan, 2017 indicated that as norm and PBC increases the intention to participate in ecommerce privacy control will decrease. The variables were not suitable predictors of the intention to safeguard ecommerce privacy.

The ANOVA measures the means of each construct to determine if the means were equal (Ajzen & Sheikh, 2013). If the means were equal then the null hypothesis was accepted. The results from the ANOVA test answered the research question: What was the correlation between behavioral marketer's attitudes, SNs, and PBC, regarding the collection of ecommerce consumer's personal information?

Separate ANOVA tests were conducted for the variables attitude, social norm, and PBC. The results of the ANOVA for the three categories listed in table 4.

Table 4

One-Way Analysis of Variance

	Sig (p)	F	R^2	Results
Attitude	0.879	0.683	0.641	Accept Null
Social norms	0.026	2.298	0.892	Reject Null

	0.048	4.263	0.986	Reject Null
Perceived behavior				

Note. n= 84.

H$_{01}$: There was not a significant correlation between the behavioral marketer's attitudes concerning the collection of ecommerce consumer's personal information.

H$_{a1}$: There was a significant correlation between the behavioral marketer's attitudes concerning the collection of ecommerce consumer's personal information. Based on the results for the first hypothesis, the attitude variable was significant, F (12,23) = .683, p = .879. The ρ value was greater than .05; therefore the null hypothesis was rejected.

Second Hypothesis

H$_{02}$: There was not a significant correlation between the behavioral marketer's SNs concerning the collection of ecommerce consumer's personal information.

H$_{a2}$: There was a significant correlation between the behavioral marketer's SNs concerning the collection of ecommerce consumer's personal information. The social norms variable was not significant, F (14,18) = 2.298, ρ = .026. The p value is less than .05; therefore the null hypothesis was accepted.

Third Hypothesis

H$_{03}$: There was not a significant correlation between the behavioral marketer's PBCs concerning the collection of ecommerce consumer's personal information.

H$_{a3}$: There was a significant correlation between the behavioral marketer's PBCs concerning the collection of ecommerce consumer's personal information.

The PBC was not significant, $F(78,5) = 4.263$, $\rho = .048$. The p value was less than .05;
therefore the null hypothesis was accepted.

The results of the study indicated behavioral managers were aware of the privacy
issues with the collection, use, and sell of personal information. The participants had a
positive attitude toward privacy protection, but attitude was not a determinant of
behavior. Dienlin and Trepte (2015) suggested extreme attitudes were more likely to
impact behavior. Also, experience with online security breaches or other privacy issues
may impact the behavioral marketer's attitude.

The results for social norms and PBC were statistically insignificant. Apparently,
the behavioral marketers did not have a strong motivation to follow group norms. Shin
and Hancer (2016) found social norms to be statistically significant. It was assumed
behavioral marketers would have volitional control to implement privacy controls in their
work. There may not be an opportunity for the behavior marketer to implement change
due to lack of support or resources. Decision makers in businesses and corporations were
accountable to the stockholders and ecommerce consume privacy may not be a focus for
the business. A social change agent may be needed to make the business case of being
proactive rather than reactive, of security breaches.

Applications to Professional Practice

The collection, use, and sell of personal information were beneficial to behavioral
marketers. The collected information assisted with targeting products to consumers,
which increased sales. The results of the research indicated skewness. The behavioral
marketer's attitude toward protecting consumer privacy was positive and social norms

were positive, whereas the PBC and intention were negative. The research results supported the privacy paradox. Ecommerce behavioral marketing managers were concerned about privacy but consistently collected data for profit.

Milne et al. (2017) indicated the collection of personal information continue to be a marketing strategy for behavior marketers, ecommerce consumers will have privacy concerns, and consumers will continue to provide personal information. There are process changes the behavioral marketer can implement. The changes for behavioral marketers include sensitivity to the ecommerce consumer information risk, implementation of information and privacy notifications.

Cracium (2018) suggested behavioral marketers beware of ecommerce consumer's sensitivity to the collection of personal information. Milne (2017) stated the consumer's perception of how their information was utilized influence privacy concerns. The willingness to provide personal information was positively impacted by trust in the business and negatively impacted by a potential security breach. Sensitivity to ecommerce consumer's privacy concern may be the first step toward avoiding the negative impact of a security breach.

Implementation of information includes personalized privacy policies. Personalized privacy policies allow the ecommerce consumers a degree of control regarding their personal information. The use of a personalized dashboard would provide ecommerce consumers control over their information Consumers would be able to choose how much information to share. Currently, privacy protection includes online privacy notifications, data usage disclosures, online tracking options, and default options.

Enhanced information collection methods would limit the amount of information

collected.

Improved information collection methods would limit the amount of information

needed to a minimum. This is accomplished by understanding what type of information

was useful. Last, the information collected should have an expiration date and erased

from the company's databases at a point in time. Businesses will continue to collect

personal information and consumers will have concerns regarding ecommerce privacy

therefore the best approach will be information privacy policies at the corporate or

business level.

Implications for Social Change

Behavior marketers are the best catalyst for social change. As social change

agents, behavioral marketers can drive the changes required to protect ecommerce

consumer privacy. The results of the study indicated behavioral marketers were aware of

ecommerce consumer's privacy concerns. The attitude and social norms were positive,

but the PBC and intentions were negative. This trend suggests behavioral marketers were

aware of ecommerce consumer's privacy concerns and their peers expect them to protect

ecommerce; although they do not have the volition to make changes. Behavior marketers

could propose strategies to protect ecommerce consumer's privacy to the appropriate

level of management. The easier changes would be the commitment to include changes to

the current small print privacy protection notifications. Implementation of robust privacy

protection activities may prevent the financial penalty of a security breach. Business

owners or managers who implement ecommerce privacy protection, at the request of the behavior marketer may positively contribute to brand loyalty.

Recommendations for Action

The first limitation of the study was; knowledge was not a consistent predictor of behavior. The results of this research study indicated the behavioral marketers had knowledge of ecommerce privacy protection, but attitude was not a predictor of behavior. Second limitation, the respondents or participants represented several industries. Future research may focus on one industry. The results may be different when the participants are from one industry. Third, there was an unknown regarding, which TPB specific variables attitude, SNs, or PBC, would motivate behavioral marketing managers to protect personal information online. It may be advantageous to study the variables separately. Administering one survey tool with the four variables may result in confusion. Fourth, there was not a concrete definition of privacy. The researcher's definition should be listed at the beginning of the survey. Last, there was a 4-week time constraint for collecting responses from the participants. Future research may consist of a qualitative focus to express the participants thoughts related to PBC and intentions. The qualitative nature will allow the participants more time to express comments related to the questions or variables.

There were many definitions of privacy. At the beginning of my DBA study, I shared the definition with Goodwin (1991), the right to be left alone (Milne et al., 2017). As I continued through the DBA process, I realized the *Internet of things* (IOT) provides personal information and preferences for every consumer (Milne et al., 2017). The

Internet of things makes it easier to collect personal information but harder to protect.

Information is collected from several platforms including social media, ecommerce

information, and personal devices, such as Fitbit trackers. It may be more advantageous

to protect and regulate personal information than eliminate the collection.

Recommendations for Further Research

The first limitation of the study was; knowledge was not a consistent predictor of

behavior. The results of this research study indicated the behavioral marketers had

knowledge of ecommerce privacy protection, but attitude was not a predictor of behavior.

Second limitation, the respondents or participants represented several industries. Future

research may focus on one industry. The results may be different when the participants

are from one industry. Third, there was an unknown regarding, which TPB specific

variables attitude, SNs, or PBC, would motivate behavioral marketing managers to

protect personal information online. It may be advantageous to study the variables

separately. Administering one survey tool with the four variables may result in confusion.

Fourth, there was not a concrete definition of privacy. The researcher's definition should

be listed at the beginning of the survey. Last, there was a 4-week time constraint for

collecting responses from the participants. Future research may consist of a qualitative

focus to express the participants thoughts related to PBC and intentions. The qualitative

nature will allow the participants more time to express comments related to the questions

or variables.

Reflections

There were many definitions of privacy. At the beginning of my DBA study, I shared the definition with Goodwin (1991), the right to be left alone (Milne et al., 2017). As I continued through the DBA process, I realized the *Internet of things* (IOT) provides personal information and preferences for every consumer (Milne et al., 2017). The Internet of things makes it easier to collect personal information but harder to protect. Information is collected from several platforms including social media, ecommerce information, and personal devices, such as Fitbit trackers. It may be more advantageous to protect and regulate personal information than eliminate the collection.

Conclusion

The theory of planned behavior was a popular theory for examining behaviors toward an activity. Researchers used the theory successfully to understand a variety of behaviors related to medical situations, purchasing green vehicles, and local food purchases. Based on the research, I conducted; behavior marketers have positive attitudes toward protecting ecommerce consumer's privacy, but negative impacts of SNs or PBC. The negative results may be indicative of behavioral marketers not having volitional control over changes to privacy strategies.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442-492. doi.10.1257/jel.54.2.442

Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing*, *33*, 98-110. doi:10.1108/jcm-06-2015-1458

Aiken, L. S., West, S. G., & Millsap, R. E. (2008). Doctoral training in statistics, measurement, and methodology in psychology. *American Psychologist, 63*(1), 32-50. doi:10.1037/0003-066x.63.1.32

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2006). Constructing a TPB questionnaire: Conceptual and methodical considerations. Retrieved from http://people.umass.edu/aizen/tpb.html

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113-1127. doi:10.1080/08870446.2011.613995

Ajzen, I. (2014). The theory of planned behaviour is alive and well, and not ready to retire: A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review*, *9*, 131-137. doi:10.1080/17437199.2014.883474

Ajzen, I., & Sheikh, S. (2013). Action versus inaction: Anticipated affect in the theory of planned behavior. *Journal of Applied Social Psychology*, *43*(1), 155-162. doi:10.1111/j.1559-1816.2012.00989.x

Armitage, C. (2015). Time to retire the theory of planned behavior. A commentary on

    Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review, 9*, 151-155.

    doi:10.1080/17437199.2014.892148

Barbu, A. (2015). Young customers loyalty. *FAIMA Business & Management Journal,*

    3(3), 12-23. Retrieved from http://faimajournal.ro

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies

    between expressed privacy concerns and actual online behavior: A systematic

    literature review. *Telematics and Informatics, 34*, 1038-1058.

    doi:10.1016/j.tele.2017.04.013

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social

    media users. *Information Technology & People, 28*(3), 426-441.

    doi:10.1108/ITP.10-2014-0232

Bonett, D. G., & Wright, T. A. (2015). Cronbach's alpha reliability: Interval estimation,

    hypothesis testing, and sample size planning. *Journal of Organizational Behavior,*

    36(1), 3-15. doi:10.1002/job.1960

Borgesius, F. J. Z. (2015). Personal data processing for behavioural targeting: Which

    legal basis? *International Data Privacy Law, 5*(3), 163-176.

    doi:10.1093/idpl/ipv011

Bosco, F. A., Singh, K., Aguinis, H., Field, J. G., & Pierce, C. A. (2015). Correlational

    effect size bench. *Journal of Applied Psychology*, *100*(2), 431-449.

    doi:10.1037/a0038047

Brahmana, R., Brahmana, R. K., & Memarista, G. (2018). The planned behavior in

    purchasing health insurance. *South East Asian Journal of Management*, *12*(1), 53-

    64. Retrieved from http:// http://www.journal.ui.ac.id/tseajm

Bromley, E., Mikesell, L., Jones, F., & Khodyakov, D. (2015). From subject to

    participant: Ethics and the evolving role of community in health research.

    American Journal of Public Health, 105, 900-908.

    doi:10.2015/AJPH.2014.302403

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs*

    for research. New York, NYC: Ravenio.

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure.

    Journal of Economics & Management Strategy, *24*(1), 47-73.

    doi:10.1111/jems.12079

Caramelli, M., & Van De Vijver, F. R. (2013). Towards a comprehensive procedure for

    developing measurement scales for cross cultural management research.

    Management International, 17(2), 150-163. Retrieved from

    http://managementinternational.ca/

Caro-Bautista, J., Martín-Santos, F. J., Villa-Estrada, F., Morilla Herrera, J. C., Cuevas

    Fernández-Gallego, M., & Morales-Asencio, J. M. (2015). Using qualitative

    methods in developing an instrument to identify barriers to self-care among

    persons with type 2 diabetes mellitus. *Journal of Clinical Nursing*, *24*(7-8), 1024-

    1037. doi:10.1111/jocn.12740

Carr, C. T. (2015). Spotlight on ethics: Institutional review boards as systematic bullies. *Journal of Higher Education Policy and Management, 37*(1), 14-29. doi:10.1080/1360080X.2014.991530

Cavazos, C. (2013). Entering into strategic alliances: An empirical test of the direct and interaction effects of managers' attitudes, Subjective Norms, and perceived behavioral control. *Journal of Strategic Marketing, 21*(1), 3-24. doi:10.1080/0965254X.2012.717539

Cavazos, C., & Varadarajan, R. (2012). Manager's intentions toward entering into strategic marketing alliances: An empirical investigation. *Journal of Strategic Marketing, 20*(7), 571-588. doi:10.1080/0965254x.2012.730544

Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *American Journal of Management, 11*(1), 59-68. Retrieved from: https://www.nabpress.com/american-journal-of-management

Clemons, E. K., & Wilson, J. S. (2015). Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications. *Journal of Management Information Systems, 32*, 40-70. doi:10.1080/07421222.2015.1063277

Cole, J. C. (2008). *How to deal with missing data: Best practices in quantitative methods.* Thousand Oaks, CA: Sage.

Corrigan, H., Craciun, G., & Powell, A. (2014). How does target know so much about its consumers? Utilizing consumer analytics to make marketing decisions. *Marketing Education Review, 24*, 59-165. doi:10.2753/MER1052-8008240206

Cracium, G. (2018). Choice defaults and social consensus effects on online information

  sharing: The moderating role of regulatory focus. *Computers in Human Behavior,*

  88, 89-102. doi:10.1016./j.chb.2018.06.019

Curras-Perez, R., Ruiz-Mafe, C., & Sanz-Blas, S. (2014). Determinants of user behavior

  and recommendations in social networks. *Industrial Management & Data*

  Systems, 114(9), 1477-5577. doi:10.1108/IMDS-07-2014-0219

Davcik, N. S. (2014). The use and misuse of structural equation modeling in management

  research: A review and critique. *Journal of Advances in Management Research,*

  11(1), 47-81. doi:10.1108/JAMR-07-2013-0043

DeSimone, J. A., Harms, P. D., & DeSimone, A. J. (2015). Best practice

  recommendations for data screening. *Journal of Organizational Behavior*, *36*(2),

  171-181. doi:10.1002/job.1962

Dienlin, T., & Trepte, S. (2015). Is privacy paradox a relic of the past? An in-depth

  analysis of privacy attitudes and privacy behaviors. *European Journal of Social*

  Psychology, 45, 285-297. doi:10.1002/ejsp.2049

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An

  empirical attempt to bridge and distinguish privacy related concepts. *European*

  Journal of Information Systems, *22*(3), 295-316. doi:10.1057/ejis

Echambadi, R., Campbell, B., & Agarwal, R. (2006). Encouraging best practice in

  quantitative management research: An incomplete list of opportunities. *Journal of*

  Management Studies, 43, 1801-1820. doi:10.1111/j.1467-6486.2006.00660.x

Farah, M. F. (2017) Consumers' switching motivations and intention in the case of bank

    mergers: a cross-cultural study. *International Journal of Bank Marketing, 35*(2),

    doi:10.1108/IJBM-05-2016-0067

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analysis

    using G*Power 3.1: Tests for correlation and regression analyzes. *Behavior*

    Research Methods, 41(4), 1149-1160. doi:10.3758/BRM.41.4.1149

Featherman, M. S., & Hajli, N. (2016). Self-service technologies and e service risks in

    social commerce era. *Journal of Business Ethics, 139*, 251-269.

    doi:10.1007/s10551-015-2614-4

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour:

    Towards an integrated model. *European Research on Management and Business*

    Economics, 22(3), 167-176. doi:10.1016/j.iedeen.2016.04.002

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with

    qualitative interviews: A mixed research approach. *Journal of Counseling &*

    Development, 91(2), 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Goddard, M. (2017). The EU general data protection regulation (GDPR): European

    regulation that has a global impact. *International Journal of Market Research,*

    59(6), 703-705. Retrieved from http://eur-lex.europa.eu/legal

Gonzalez, S. T., Lopez, C. N., Marcos, Y. Q., & Rodriguez-Marin, J. (2012).

    Development and validation of the theory of planned behavior questionnaire in

    physical activity. *The Spanish Journal of Psychology, 15*(2), 801-816.

    doi:10.5209/rev_SJOP.2012.v15.n2.38892

Goodwin, C. (1991). Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing*, *10*(1), 149–166. Retrieved from https://journals.sagepub.com/home/ppo

Guarte, J. M., & Barrios, E. B. (2006). Estimation under purposive sampling. *Communications in Statistics-Simulation and Computation, 35*(2), 277-284. doi:10.1080/0361091060091610

Gubrium, J. F., & Holstein, J. A. (2002). *Handbook of interview research: Context & method.* Thousand Oaks, CA: Sage.

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information & Computer Security, 24*(4), 348-371. doi:10.1108/ICS-05-2015-0020

Haenlein, M., & Kaplan, A. M. (2011). The influence of observed heterogeneity on path coefficient significance: Technology acceptance within the marketing discipline. *Journal of Marketing Theory and Practice, 19*, 153-168. doi:10.2753/MTP1069-6679190203

Hagger, M. S. (2015). Retired or not, the theory of planned behavior will always be with us. *Health Psychology Review, 9*, 125-130. doi:10.1080/17437199.2015.1034470

Hall, P. A. (2015). Re-establishing momentum in theory development: A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review, 9*, 172-175.

Hallam, C., & Zanella, G. (2017). Self-disclosure. The privacy paradox explained as a temporary discount balance. *Computers in Human Behavior, 68*, 217-227. doi:10.1016/j.chb.2016.11.033

Han, T. I., & Stoel, L. (2017). Explaining socially responsible consumer behavior: A meta-analytic review of theory of planned behavior. *Journal of International Consumer Marketing, 29*(2), 91-103. doi:10.1080/08961530

Haryani, S. J., & Motwani, B. B. (2015). Gender difference in consumer perception towards online viral marketing communication. *International Journal of Marketing and Business Communication, 4*(3), 28-37. Retrieved from http://www.publishingindia.com

Hassan, L., Shiu, E., & Shaw, D. (2016). Who Says There is an intention-behaviour gap? Assessing the empirical evidence of an intention-behaviour gap in ethical consumption. *Journal of Business Ethics*, *136*(2), 219-236. doi:10.1007/s10551-014-2440-0

Heerwegh, D., & Loosveldt, G. (2009). Explaining the intention to participate in a web survey: A test of the theory of planned behavior. *International Journal of Social Research Methodology, 12*(3), 181-195. doi:10.1080/13645570701804235

Hegner, S. M., Fenko, A., & Teravest, A. (2017). Using the theory of planned behavior to understand brand love. *Journal of Product & Brand Management, 26*, 26-41. doi:10.1108/jpbm-06-2016-1215

Herrero, A., & San Martin, H. (2012). Effects of the risk sources and user involvement on ecommerce adoption: Application to tourist services. *Journal of Risk Research, 15*(7), 841-855. doi:10.1080/13669877.2012.666758

Holliman, G., & Rowley, J. (2014). Business to business digital content marketing: Marketers' perceptions of best practice. *Journal of Research in Interactive Marketing, 8*, 269-293. doi:10.1108/JRIM-02-2014-0013

Jackson, J. R. (2018). A perfect fit: Personalization versus privacy. *Journal of Organizational Psychology, 18*(4), 33-42. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/job.515

Jai, T. M., & King, N. J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third party advertisers and brokers. *Journal of Retailing and Consumer Services, 28*, 1-8. doi:10.1016/j.jretconser.2015.01.005

Jayaraman, K., Arumugam, S., Kumar, K. M., & Kiumarsi, S. (2018). Factors Influencing the Purchase Decision of Non-National Cars in Malaysia: An Empirical Study. *Global Business & Management Research*, *10*, 150–162. Retrieved from https:// gbmr.ioksp.com

Kammer, A., Niessen, S., Schmid, L., & Schwendener, L. (2016). Finding ones way on the roads to social change: The impact metamodel of the impact FOPH communication campaigns. *Social Marketing Quarterly, 22*(2), 89-109. doi:10.1177/152450041385

Karam, C. M., & Ralston, D. A. (2016). A failure before analysis: The soup to nuts of preparing for multicountry analyses. *Cross Cultural & Strategic Management, 23*, 590-612. doi:10.1108/CCSM-05-2016-0105

Kassim, K. A., Arokiasamy, L., Isa, M. H., & Ping, C. H. (2017). Intention to purchase a safer car: An application of theory of planned behavior. *Global Business and Management Research: An International Journal, 9*, 188-197. Retrieved from http://www.universal-publishers.com

Kayhan, V. O., & Davis, C. J. (2016). Situational privacy concerns and antecedent factors. *Journal of Computer Information Systems, 56*, 228-237. Retrieved from http://www.scimagojr.com/journalsearch.php?q=12373&tip=sid

Keele, L., McConnaughy, C., & White, I. (2012). Strengthening the experimenter's toolbox: Statistical estimation of internal validity. *American Journal of Political Science, 56*(2), 484-499. doi:10.1111/j.1540-5907.2011.00576.x

Kude, T., Hoehle, H., & Sykes, T. A. (2017). Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management, 37*, 56-74. doi:10.1108/IJOPM-03-2015-0156

Leedy, P. D., & Ormrod, J. E. (2010) *Practical research: Planning and design*. New York, NY: Merri.

Libaque-Saenz, C. F., Chang, Y., Kim, J., Park, M. C., & Rho, J. J. (2016). The role of perceived information practices on consumers' intention to authorize secondary use of personal data. *Behaviour & Information Technology, 35*(5), 339-356. doi:10.1080/0144929X

Lim, W. M. (2015). Antecedents and consequences of e-shopping: An integrated model. *Internet Research, 25*, 184-217. doi:10.1108/IntR-11-2013-0247

Liu, X. S. (2013). Sample size determination for the confidence interval of mean

    comparison adjusted by multiple covariates. *Statistical Methods & Applications,*

    22(2), 155-166. doi:10.1007/s10260-012-0212-5

Liu, Y. N., Wang, Y. P., Wang, X. F., Xia, Z., & Xu, J. F. (2019). Privacy-preserving raw

    data collection without a trusted authority for IoT. *Computer Networks, 148*, 340-

    348. doi: 10.1016/j.comnet.2018.11.028

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at

    the centre of the information systems (IS) artefact: Proposing a bold research

    agenda. *European Journal of Information Systems, 26*(6), 546-563. Retrieved

    from http://www.palgrave.com/journals

Lwin, M. O., Wirtz, J., & Stanaland, A. J. S. (2016). The privacy dyad. *Internet*

    Research, 26, 919-941. doi:10.1108/IntR-05-2014-0134

Lynch, J. G. (1982). On the external validity of experiments in consumer research.

    Journal of Consumer Research, 9(3), 225-239. doi:10.1086/208919

MacCann, C., Todd, J., Mullan, B. A., & Roberts, R. D. (2015). Can personality bridge

    the intention-behavior gap to predict who will exercise? *American Journal of*

    Health Behavior, *39*, 140-147. doi:10.5993/AJHB.39.1.15

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information sensitivity and Willingness

    to provide Continua: A comparative privacy study of the USA and Brazil. *Journal*

    of Public Policy & Marketing, 36(1), 79-96. doi:10.1509/jppm.15.159

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551-569. doi:10.1007/s10551-015-2565-9

McGrath, J. E., & Brinberg, D. (1983). External validity and the research process: A comment on the Calder/Lynch dialogue. *Journal of Consumer Research, 10*(1), 115-124. doi:10.1086/208951

Meyer-Waarden, L. (2015). Effects of loyalty program rewards on store loyalty. *Journal of retailing and consumer services, 24*, 22-32. doi:10.1016/j.jretconser.2015.01001

Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking & Finance*, *88*(1), 192–207. doi:10.1016/j.jbankfin.2017.12.002

Milne, G. R., Pettinico, G., Hajjat, F., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data. *Journal of Consumer Affairs, 51*(1), 133-161. doi:10.1111/joca.12111

Moghavvemi, S., Sellah, N. A. M., Sulaiman, A., & Abessi, M. (2015). Effect of external factors on intention behaviour gap. *Behaviour & Information Technology, 34*(12), 1171-1185. doi:10.1080/0144929X.2015.1055801

Moore, D. S., McCabe, G. P., Duckworth, W. M., & Sclove, S. L. (2003). *The practice of business statistics using data for decisions*. New York, NY: Freeman and Company.

Moore, R. S., Moore, M. L., Shanahan, K. J., Horky, A., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation.

Marketing Management Journal, 25(1), 42-53. Retrieved from

http://www.tandfonline.com/toc/rjmm20/current

Moreno, M. A., Goniu, N., Moreno, P. S., & Diekema, D. (2013). Ethics of social media

research: Common concerns and practical considerations. *Cyberpsychology,*

Behavior & Social Networking, 16(9), 708-713. doi:10.1089/cyber.2012.0334

Mukhopadhyay, S., & Gupta, R. K. (2014). Survey of qualitative research methodology

in strategy research and implication for Indian researchers. *Vision, 18*(2), 109-

123. doi:10.1177/0972262914528437

Nesterkin, D. A., & Ganster, D. C. (2015). The effects of nonresponse rates on group

level correlations. *Journal of Management, 41*, 789-807.

doi:10.1177/0149206311433853

Norris, J., Plonsky, L., Ross, S., & Schoonen, R. (2015). Guidelines for reporting

quantitative methods and results in primary research. *Language Learning, 65*(2),

470-476. doi:10.111/lang.12104

O'Reilly, S., & Kumar, A. (2016). Closing the loop. *International Journal of Logistics*

Management, 27(2), 486-510. doi:10.1108/IJLM-03-2015-0050

Ogden, J. (2015). Time to retire the theory of planned behavior: One of us will have to

go. A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology*

Review, 9, 165-167. doi:10.1080/17437199.2014.898679

Ormiston, M. (2014). The American Marketing Association. Retrieved from

https://www.ama.org/search/pages/results.aspx

Peer, E., & Acquisti, A. (2016). The impact of reversibility on the decision to disclose personal information. *Journal of Consumer Marketing, 33*, 428-436. doi:10.1108/JCM-07-2015-1487

Peiris, P. M., Kulkarni, D., & de Silva Mawatha, C. R. (2015). An empirical study of customer adoption of e-commerce: A customer trust model to support the adoption of e-commerce among small and medium sized enterprises in Sri Lanka. *International Journal of Business and Information, 10*, 491-518. Retrieved from http://knowledgetaiwan.org/ijbi/

Phillips, A. (2015). OH research: How to conduct surveys. *Occupational Health, 67*(1), 27-30. Retrieved from https://www.researchgate.net

Psaradakis, Z. (2016). Using the bootstrap to test for symmetry under unknown dependence. *Journal of Business & Economic Statistics, 34*, 406-415. doi: 10.1080/07350015.2015.1043368

Raza, S. H., Bakar, H. A., & Mohamad, B. (2018). Relationships between the advertising appeal and behavioral intention: The role of mediating role of attitude towards advertising appeal and moderating role of cultural norm. *Journal of Business and Retail Management Research, 12*(2), 185-193. Retrieved from http://www.jbrmr.com

Riquelme, I., & Roman, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers. *Electronic Markets, 24*, 135-149. doi:10.1007/s12525-013-0145-3

Rogelberg, S. G., & Stanton, J. M. (2007). Introduction: Understanding and dealing with organizational survey nonresponse. *Organizational Research Methods, 10*(2), 195-209. doi:10.1177/1094428106294693

Rogers, W., & Meek Lange, M. (2013). Rethinking the vulnerability of minority populations in research. *American Journal of Public Health, 103*, 2141-2146. doi:10.2105/AJPH.2012.301200

Ryan, T. A. (2017). The role of beliefs in purchase decisions: A look at green purchase behaviour and altruism. *Journal of Research for Consumers,* (31), 25-56. Retrieved from https://JRconsumers.com/academic

Sánchez, J. C. (2013). The impact of an entrepreneurship education program on entrepreneurial competencies and intention. *Journal of Small Business Management*, *51*, 447-465. doi:10.1111/jsbm.12025

Sanne, P. N. C., & Wiese, M. (2018). The theory of planned behaviour and user engagement applied to facebook advertising. *South African Journal of Information Management, 20*(1), 1-10. doi: 10.4102/sajim.v20i1.915

Schaller, T. K., Patil, A., & Malhotra, N. K. (2015). Alternative techniques for assessing common method variance an analysis of the theory of planned behavior research. *Organizational Research Methods, 18*(2), 177-206. doi:10.1177/1094428114554398

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*, 314-341. doi:10.1080/07421222.2015.1063315

Seungsin, L., Younghee, L., Joing-in, L., & Jungkun, P. (2015). Personalized e-services: consumer privacy concern and information sharing. *Social Behavior & Personality: An International Journal*, *43*(5), 729–740. doi:10.2224/sbp.2015.43.5.729

Shin, Y. H., & Hancer, M. (2016). The role of attitude, subjective norm, perceived behavioral control, and moral norm in the intention to purchase local food products. *Journal of Foodservice Business Research*, *19*(4), 338–351. doi:10.1080/15378020.2016.1181506

Simon, M. K. (2011). *Dissertation and scholarly research: Recipes for success*. Seattle, WA: Dissertation Success.

Smith, T. A. (2014). Testing theory and related factors for influencing proficiency in quantitative research. *Academy of Educational Leadership Journal, 18*(4), 117-128. Retrieved from http://cetl.kennesaw.edu/journals/academy-educational-leadership-journal

Sniehotta, F. F., Presseau, J., & Araújo-Soares, V. (2015). On the development, evaluation, and evolution of health behavior. *Health Psychology Review, 9*, 176-189. doi:10.1080/17437199.2015.1022902

Sonenshein, S. (2016). How corporations overcome issue illegitimacy and issue equivocality to address social welfare: The role of the social change agent. *Academy of Management Review, 41*, 349-366. doi:10.5465/AMR.2013.0425

Soon, J. M., & Wallace, C. (2017). Application of theory of planned behavior in

    purchasing intention and consumption of Halal food. *Nutrition & Food Science,*

    47(5), 635-647. doi:10.1108/NFS-03-2017-0059

Spiekermann, S., Acquisti, A., R., & Hui, K. (2015). The challenges of personal data

    markets and privacy. *Electronic Markets, 25*(2), 161-167. doi:10.1007/s12525-

    015-0191-0

Statista (2019). Statistics and facts about online shopping. Retrieved from

    https://www.statista.com/topics/871/online-shopping/

Steijn, W. M. P., & Vedder, A. (2015). Privacy concerns, dead or misunderstood? The

    perceptions of privacy amongst the young and old. *Information Polity, 20*, 299-

    311. doi:10.3233/ip-150374

Sukamolson, S. (2016). *Fundamentals of quantitative research*. EJTR. Retrieved from

    https://independent.academia.edu/SSukamolson

Summers, C. A., Smith, R. W., & Walker-Reczek, R. (2016). An audience of one:

    behaviorally targeted ads as implied social labels. *Journal of Consumer Research*,

    43(1), 156-178. doi:10.1093/jcr/ucw012

Tabari, N. A. Y., & Abroud, E. (2017). Factors effecting consumer's tendency to online

    shopping. *International Journal of Economic Perspective, 11*(3), 549-556.

    Retrieved from http://econ-society.org

Tamimi, N., & Sebastianelli, R. (2015). The relative importance of e-tailor website

    attributes on the likelihood of online purchase. *Internet Research, 25*, 169-183.

    doi:10.1108/IntR-07-2013-0131

Taylor, J. F., Ferguson, J., & Ellen, P. S. (2015). From trait to state: Understanding privacy concerns. *Journal of Consumer Marketing, 32*, 99-112. doi:10.1108/jcm-07-2014-1078

The U.S. Department of Health & Human Services (HHS). (1979). The *Belmont Report*: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Thompson, M. F., Tuzovic, S., & Braun, C. (2019). Trustmarks: Strategies for exploiting their full potential in e-commerce. *Business Horizons, 62*(2), 237-247. doi:10.1016/j.bushor.2018.09.004

Tiwari, P., Bhat, A. K., & Tikoria, J. (2017). An empirical analysis of the factors affecting social entrepreneurial; intentions. *Journal of Global Entrepreneurialship Research, 7*(9), 1-25. doi:10.1186/s40497-017-0067-1

Todor, R. D. (2016). Blending traditional and digital marketing. *Economic Sciences, 9*(58), 51-56.Retrieved from http://webbut.unitbv.ro/Bulletin/Series%20V/Series%20V.html

Trafimow, D. (2015). On retiring the TRA/TPB without retiring, the lessons learned: A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review, 9*, 168-171. doi:10.1080/17437199.2014.884932

Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy as a fuzzy concept: A new

    conceptualization of privacy for practioners. *Journal of the Association for*

    Information Science and Technology, 66, 918-929. doi:10.1002/asi.23220

Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity

    on online privacy disclosure. *Computers in Human Behavior, 73*, 238-284.

    doi:10.1016/j.chb.2017.03.018

Vogt, W. P., Gardner, D. C., & Haeffele, L. M. (2014). *When to use what research*

    design. New York, NY: Guilford Press.

Walsh, D., Parisi, J. M., & Passerini, K. (2017). Privacy as a right or as a commodity in

    the online world: The limits of regulatory reform and self-regulation. *Electronic*

    Commerce Research, 17(2), 185-203. doi.10.1007/s10660-015-9187-2

Walters, H. D., Wiese, M.D., & Bruce, M.L. (2018). When retailors target women based

    on body shape and size: The role of ethical evaluation on purchase intention,

    Journal of Research for Consumers, 33, 1-37. Retrieved from http://

    http://www.jrconsumers.com/

Warren, S. V., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*,

    193-220. Retrieved from http://harvardlawreview.org/

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of

    things: Convenience vs. privacy and secrecy. *Business Horizons, 58*, 615-624.

    doi:10.1016/j.bushor.2015.06.005

Wijnhoven, F., & Bloemen, O. (2014). External validity of sentiment mining reports: Can concurrent methods identify demographic bias, event bias, and manipulation of reviews? *Decision Support Systems, 59*, 262-273. doi:10.1016/j.dss.2013.12005

Williams, B., Brown, T., & Onsman, A. (2010). Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine, 8*(3), 1-13. Retrieved from http://ro.ecu.edu.au/jephc/vol8/iss3/1

Wolf, S., Weibenberger, B. E., Wehner, M. C., & Kabst, R. (2015). Controllers as business partners in managerial decision-making. Attitude, subjective norm, and internal improvements. *Journal of Accounting & Organizational Change, 11*, 24-46. doi:10.1108/JAOC-10-2012-0100

Woolley, D. J. (2015). Two issues to consider in digital piracy research: The use of Likert-like questions and the theory of behavioral surveys. *Journal of Legal, Ethical, and Regulatory Issues, 18*(3), 63-67. Retrieved from http://www.alliedacademies.org

Wu, C. (2015). Using the theory of planned behavior to explain and predict behavior intentions in Taiwan. *Journal of International Education Research, 11*(3), 153-162. Retrieved from https:// https://www.journals.elsevier.com/international-journal-of-educational-research/

Wu, W. Y., Ke, C. C., & Nguyen, P. T. (2018). Online shopping behavior in electronic commerce: An integrative model from Utilitarian and Hedonic perspectives. *International Journal of Entrepreneurship, 22*, 1-16. Retrieved from

http://www.abacademies.org/journal/international-journal of entrepreneurship-home.html

Xiao, L., & Askin, N. (2014). Academic opinions of Wikipedia and open access publishing. *Online Information Review, 38*, 332-347. doi:10.1108/olir-04-2013-0062

Xu, L., Yang, F., Chen, R., & Yu, S. (2015). A parametric bootstrap test for two-way ANOVA model without interaction under heteroscedasticity. *Communications in Statistics-Simulation and Computation, 44*, 0361-0918. doi:10.1080/03610918.2013.818689

Yeh, C. H., Wang, Y. S., Lin, S. J., Tseng, T. H., Lin, H. H., Shih, Y. W., Lai, Y. H. (2018). What drives Internet users' willingness to provide information? *Online Information Review, 42*(6), 923-939. doi:10.1108/OIR-09-2016-0264

Zampetakis, L. A., Bakatsaki, M., Litos, C., Kafetsios, K. G., & Moustakis, V. (2017). Gender based differential item functioning in the application of the theory of planned behavior for the study of entrepreneurial intentions. *Frontiers in Psychology, 8*, 1-8. doi:10.3389/fpsyg.2017.00451

Zhang, J. (2014). Customer' loyalty forming mechanism of O2O E-commerce. *International Journal of Business and Social Science, 5*(5), 164-169. Retrieved from http://www.ijbssnetcom

Zolait, A. S. (2014). The nature and components of perceived behavioural control as an element of theory of planned behaviour. *Behaviour & Information Technology, 33*(1), 65-84. doi:10.1080/0144929X.2011.630419

Appendix A: TPB Survey Tool Authorization

The test content may be reproduced and used for non-commercial research and

educational purposes without seeking written permission. Distribution must be

controlled, meaning only to the participants engaged in the research or enrolled in the

educational activity. Any other types of reproduction or distribution of test content is not

authorized without permission from author and publisher. Always include a credit line

that contains the source citation and copyright owner when writing about or using test.

Appendix B: TPB Survey Tool

Questionnaire – Ecommerce Consumer Privacy Concern

Attitude toward the behavior:

1. For me to implement ecommerce consumer privacy strategy, in my work, would be:

Extremely unenjoyable – extremely enjoyable

2. For me to implement ecommerce consumer privacy strategy, in my work, would be:

Extremely worthless – extremely valuable

3. For me to implement ecommerce consumer privacy strategy, in my work, would be:

Extremely bad – extremely good

4. For me to implement ecommerce consumer privacy strategy, in my work, would be:

Extremely unpleasant – extremely pleasant

Subjective Norms:

1. Most people who are important to me would think I should implement consumer

   privacy protection into my daily work with ecommerce advertising.

Strongly disagree – strongly agree

2. People in my life whose opinions I value would approve of me implementing

   ecommerce consumer privacy practices into my daily work.

Strongly disagree – strongly agree

3. My coworkers/manager/important people whose opinions I value have implemented

   an ecommerce consumer privacy practices, in their daily work.

Strongly disagree – strongly agree

4. It is expected of me to implement ecommerce consumer privacy practices in my daily work with ecommerce targeted advertising.

Strongly disagree – strongly agree

Perceived Behavior Control:

1. It is mostly up to me whether I implement ecommerce consumer privacy practices into my daily work.

Strongly disagree – strongly agree

2. For me to implement ecommerce consumer privacy practices in my daily work is:

Extremely difficult – extremely easy

3. I am confident, that if I wanted to implement ecommerce consumer privacy practices at work.

Strongly disagree – strongly agree

4. For me to employ ecommerce consumer privacy practices into the ad design phase is:

Impossible - possible

Intentions:

1. I plan to implement ecommerce consumer privacy practices into my daily work with ecommerce ad development.

Extremely unlikely – extremely likely

2. I will make an effort to implement an ecommerce consumer privacy practice in my daily work.

Definitely will not – definitely will

3. I intend to employ ecommerce consumer privacy practices into my responsibilities.

Definitely will not – definitely will