The Role of Privacy Management in Brand Protection and Brand Value

By
Elizabeth-Anne McLeod

A Thesis Submitted to
Saint Mary's University, Halifax, Nova Scotia
In Partial Fulfillment of the Requirements for
the Degree of Doctor of Philosophy in Business Administration.

June, 2017, Halifax, Nova Scotia

Approved: Dr. Dawn Jutla
Supervisor

Approved: Dr. Ajax Persaud
External Examiner

Approved: Dr. Tom Stafford
Committee Member

Approved: Dr. Anthony Yue
Committee Member

Date: June 14, 2017

TABLE OF CONTENTS

LIST OF TABLES

Table

LIST OF FIGURES

Figure

LIST OF ABBREVIATIONS

AGFI ..... The Adjusted Goodness of Fit Index

AIC ..... The Akaike Information Criterion

AIPPA ..... Access to Information and Protection of Privacy Act

BCC ..... The Browne-Cudeck Criterion

BIC ..... The Bayesian Information Criterion

CAIC ..... The Consistent Akaike Information Criterion

CFI ..... The Comparative Fit Index

CMIN/DF ... Minimum of discrepancy function / Degrees of freedom

df …… Degrees of freedom

ECVI ..... The Expected Cross-Validation Index

FIPPs ..... Fair Information Practices Principles

FMIN ..... Minimum of discrepancy function F

FOIPOP ..... Freedom of Information and Protection of Privacy Act

FOIPPA ..... Freedom of Information and Protection of Privacy Act

GFI ..... The Goodness of Fit Index

IFI ..... The Incremental Fit Index

MGA ..... The Municipal Government Act Part XX

NFI ..... The Normed Fit Index

NCP ..... The Noncentrality Parameter

PA ..... Privacy Act

PbD ..... Privacy by Design

PCFI ..... The Parsimony Comparative Fit Index

PCLOSE ..... Process Close

PGFI ..... The Parsimony Goodness of Fit Index

PHIA ..... The Personal Health Information Act

PHIPA ..... The Personal Health Information Protection Act

PHIPAA ..... The Personal Health Information Privacy and Access Act

PIAs ..... Privacy Impact Assessments

PIIDPA ..... Personal Information International Disclosure Protection Act

PIPA ..... The Personal Information Protection Act

PIPEDA ..... Personal Information Protection and Electronic Documents Act

PNFI ..... The Parsimony Normed Fit Index

PRATIO ..... The Parsimony Ratio

PRO Act ..... Privacy Review Officer Act

RFI ..... The Relative Fit Index

RMR ..... The Root Mean Square Residual

RMSEA ..... The Root Mean Square Error of Approximation

RMSR ..... The Root Mean Square Residual

RTIPPA ..... Right to Information and Protection of Privacy Act

SRMSR ..... The Standardized Root Mean Square Residual

TLI ..... The Tucker-Lewis Index

χ^2 ……. Chi square

ACKNOWLEDGEMENTS

I would like to thank my Faculty Advisor, Dr. Dawn Jutla, Scotiabank Professor of Technology Entrepreneurship and Program Director of the Master of Technology Entrepreneurship and Innovation Program in the Department of Finance, Information Systems and Management Science at the Sobey School of Business at Saint Mary's University. Dawn has provided continued support, friendship, and great advice over the years. I met Dawn taking a course for my MBA. She supervised me through my MBA research project, E-Business Security and Privacy Practices in 2004.

I want to thank Dr. Albert Mills, Ph.D. Director, at Saint Mary's University and Dr. Jean Helms Mills. I met Albert taking Organizational Behaviour for my MBA. Albert and Jean taught me courses in the Ph.D. program. They have always made the Ph.D. program feel like a close family even with students from different cohorts. I would also like to thank Dr. Tom Stafford and Dr. Anthony (Tony) Yue for being on my Ph.D. committee, Dr. James O'Brien and Dr. George Deitz for their advice on SEM results presentation, and Dr. Ajax Persaud for being my External Examiner. I would like to thank Dr. Diane Crocker, Associate Dean, Student Affairs for her support.

I would like to thank Michael Steckling and Kyle Francis at Qualtrics and all the participants who completed the surveys. I would like to thank Chris Lutz, Verney Conference Management Inc., who let me volunteer and attend The Maritime Access, Privacy, Security, Records Management and Health IM Conference for many years.

It was a wonderful opportunity to network and meet so many people involved with Privacy from the Atlantic Provinces. Thank you Chris for letting me distribute my surveys at your conferences. I want to thank the High Technology Crime Investigation Association (HTCIA) for letting me distribute my surveys and present my research findings at your Annual Professional Development Day Conferences.

I would like to thank so many people who I have met over the years who have reviewed my survey and gave me their expert opinion and insightful comments, which I incorporated into my survey and who also helped me to distribute my survey. To name a few: Ms. Catherine Tully, Information and Privacy Commissioner of Nova Scotia; Ms. Carla Heggie, Past Information Access & Privacy Manager, Government of Nova Scotia; Mr. Bob Doherty, Owner, Robert P. Doherty Access and Privacy Services; Mr. Doug Stephen, Information & Privacy Coordinator at Alberta Health Services; Mr. David Hayes, Government of New Brunswick; Mr. Greg Bembridge, Senior Computer Forensic Instructor, Canadian Police College and Mr. Steve Prosser, Senior Consultant at CGI.

I would like to thank Trent McGill at the Saint Mary's University Centre for Academic Technologies (CAT) who helped me build my survey in LimeSurvey and Moha Jad who helped me with AMOS.

I would like to thank my loving and supportive family and friends. My husband, Ron, for his love, dedication and insight into security matters. I would like to thank my wonderful children, Connor and Kaleigh, my parents, Anne and Ron McCulloch, my late

mother-in-law, Margaret (Peggy) Johnson, and my sister, Mary, and her family Stephen, Kristen and Kelsey for their love, support and encouragement to finish my PhD.

Many times while I was running factor analyses, I was amazed at how SPSS could create components that made so much sense. I later discovered that there is a term for this called the “wow” criterion, “If, while scrutinizing the factor analysis, the investigator can shout 'Wow, I understand these factors,' the application is deemed successful” (Johnson and Wichern, 1998, p. 565 in Meyers, Gamst and Guarino, 2006, p. 513). This thesis gave me many wonderful wow moments.

ABSTRACT

The Role of Privacy Management in Brand Protection and Brand Value

By Elizabeth-Anne McLeod

There are more privacy issues and concerns with the use of a growing number of invasive technologies. This research determines if there is a role that privacy management plays on brand protection and brand value. An extensive literature review was conducted and a proposal for a new *privacy-brand model*, with hypotheses connecting 4 constructs: privacy practices (PP), brand protection (BP), experienced harms (EH), and brand value (BV) was proposed and then enhanced with the privacy concerns (PC) construct. A preliminary survey was conducted to capture up-to-date privacy concerns from experts in security and privacy. The findings informed a formal survey instrument, Privacy Management Survey, which included both new and existing scales for the constructs that were subsequently validated.

Study 1 contributes major themes for privacy concerns related to private information, using NVivo to analyze the qualitative data: (1) unauthorized access (2) misuse, particularly financial information, which is the area that is most harmed in identity theft (3) unauthorized disclosure (4) huge scope of privacy loss, and (5) need for better privacy protections. Two versions of the privacy-brand models were studied: one without privacy concerns (study 2) and one with privacy concerns (study 3). The constructs for all models were extracted using principal components analysis in SPSS, and their relationships confirmed using structural equation modeling in AMOS. The Privacy Management Survey was widely deployed to collect empirical data (N = 315) and (N = 205 holdout sample) to test the hypotheses of the *privacy-brand model* related to an organization. This work contributes a new model connecting privacy practices, experienced harms, privacy concerns, brand protection, and brand value to the management, management information systems, marketing and risk literatures. Empirical testing of the hypotheses has confirmed that privacy management plays a significant role in brand protection and brand value.

June 14, 2017.

CHAPTER 1 - INTRODUCTION

Dr. Alan Westin (2003) stated that "privacy is a quality-of-life topic worth the best scholarship, thoughtful advocacy, and continuing attention of us all" (p. 32). It is a human necessity to have our privacy.

Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada (2011) stated that it is "flawed logic that the strengthening of one interest (connecting online) will invariably lead to a reduction in an 'opposing' interest (privacy)." Cavoukian suggests that, "You can reverse this mistaken view by substituting a positive-sum, win-win strategy in its place – one that allows us to interact online and exercise control over our personal information. We can, and must, have both – the future of privacy … the future of freedom, may well depend on it."

In the information age we live in, our private information is being collected in digital format. This makes it easier to accumulate, compile and combine personal information, which on its own may not be damaging to an individual but if accessed by the wrong parties may lead to detrimental results such as identify theft and financial consequences. "Nearly half of Canadian businesses that handle customers' personal information in digital form fail to use appropriate tools and practices to protect sensitive data, according to a survey commissioned by the Office of the Privacy Commissioner of Canada" (Arellano, 2012).

With the proliferation of technology in the information society in which we live it is now easier than ever to access, collect, store and distribute personal information. Technology in workplaces has created a new digital platform domain and with this new domain there are new problems and concerns related to the privacy of information. We live in an environment with surveillance, e-mail, smart phones, ubiquitous wireless access and social networking. The privacy challenges we face today are more complex. Only one incident involving a breach of customer privacy and security could have a "significant detrimental financial impact on your business" (Herold, 2005, p. 98) and could negatively impact the lives of the individuals involved.

I believe that protecting our personal information is extremely important. I have had experiences when my personal information was compromised and corrective actions had to be taken to rectify each situation. Our local banking machine was compromised by attaching a skimmer to gather the magnetic strips and PINs. As a result, we were required to get new client cards. The customer database at retailer TJX Cos. Inc., owner of Winners and HomeSense, was compromised. As customers of Winners we were required to get new credit cards. As a result of this data breach I have paid cash for all purchases made at Winners. In March 2016 Rosen Hotels and Resorts Inc. reported that their payment network had malware on it and could impact any cards they used between September 2, 2014 and February 18, 2016 (Ragan, 2016; Rosen Hotels and Resorts Inc.,

2016). Since we stayed at Rosen in Florida once again it may be necessary to verify credit card statements, obtain new credit cards and change automatic payments.

Problem Statement

Online hacking and identity theft are growing problems for organizations and consumers with anecdotal connections to how they affect brand value. This research seeks to understand what role privacy practices, privacy concerns, and brand protection practices play in preserving brand value.

The purpose of this research is to empirically evaluate the relationships among privacy practices, brand protection, brand value, and any mediators among them.

The research examines privacy concerns given present-day technological contexts, privacy regulations, principles in privacy policies, and practices embraced in privacy management programs, the various online security and privacy defenses that extend brand protection programs, and the components of brand value. The research intends to measure whether brand protection, involving online security and privacy defenses, will help prevent privacy breaches and experienced harms and the impact this has on an organization's brand value.

Gaps

To the best of my knowledge, the intersection of the management, management of information systems, and marketing literatures do not have empirical studies investigating

the relationships between privacy management and an organization's brand value. The hypotheses and studies in this thesis are original and will cover a real gap in those literatures.

Overview

The goal of this research is to empirically show relationships between organizations' privacy concerns, privacy practices, brand protection, experienced harms, and brand value. A real outcome of this research is to have the theoretical research results transformed into pertinent actions that relevant end-users can apply in practice.

Research Question

The research question is to determine *what relationships among privacy concerns, privacy practices, and brand protection positively impact an organization's brand value*?

The specific research objectives are to:

(1) Determine whether a model, based on new hypothesized relationships among privacy concerns, privacy practices, brand protection (the extended definition), brand value, and experienced harms, exists and to scientifically test its validity.

(2) Propose the extension of the brand protection construct with online security and privacy defenses, and determine whether this extended concept is positively and significantly correlated to brand value on a go-forward basis.

Importance of this Research

This topic is worth investigating because the findings may incent trainers and educators to develop privacy programs for employees, and policy makers in developing policies that facilitate privacy education for employees to help protect the privacy rights of citizens and customers as well as the organization's brand and its associated value. Thus, privacy management may be important to shareholders and stakeholders in marketing, finance, and risk management alike. "Information privacy is of growing concern to multiple stakeholders including business leaders, privacy activists, scholars, government regulators, and individual consumers" (Smith, Dinev, and Xu, 2011, p. 990). It is desired that my *Privacy-Brand Model* will "prove useful across disciplines and contexts" (Smith et al., 2011, p. 1008) and that this thesis will make a contribution to the literature by providing "actionable steps for individuals, managers, and regulators" (p. 1008) as Smith et al. (2011) recommended for future research in privacy.

CHAPTER 2 - LITERATURE REVIEW, PRIVACY-BRAND MODEL AND HYPOTHESES

A review of the literature provides the necessary background to understanding the constructs in my proposed *Privacy-Brand Model*, the basis for my new model proposal, as well as motivation for key hypotheses of this research work. Journal articles, online resources, videos, magazine articles, textbooks and conference proceedings were included in the literature review. A subset of the attached bibliography that I extensively reviewed is summarized in this chapter, and my new hypotheses are developed and presented from this review.

Smith, Dinev and Xu (2011) have classified the privacy literature into "normative, purely descriptive, and empirically descriptive" which has been explored on an "individual, group, organizational, and societal" (p. 989) level of analysis. My qualitative research can be classified as purely descriptive utilizing interpretive methods. My quantitative research is empirically descriptive, which tests theories, models, and relationships between constructs utilizing positivist, scientific methods. My research includes both an individual and organizational level of analysis. Smith et al. (2011) identified that previous information privacy research contributions fall into three major areas: "the conceptualization of information privacy, the relationship between information privacy and other constructs, and the contextual nature of these relationships" (p. 989).

My research examines the relationships between information privacy and other constructs.

Connection between Legislation and Organizational Policy for Privacy Protection

The Freedom of Information and Protection of Privacy (FOIPOP) Act protects the privacy of Canadians' interactions with government. The FOIPOP Act establishes guidelines for the collection, use, and disclosure of individual information for public bodies and municipalities. Enforcing Canada's FOIPOP Act falls to a Privacy Commissioner or equivalent and a team with roles such as a Review Officer, Director, Investigator, Portfolio Officer, and Intake Analyst, who together uphold the confidence of the public around citizen privacy.

Canada's federal privacy legislation for its private sector, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) is based on Fair Information Practice Principles (FIPPs). Other countries, such as the USA, also use the core 8 principles of FIPPS: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, and Security to underlie organizations' frameworks to create and maintain organizational privacy policy (Teufel, 2008). The Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, the Children's Online Privacy Protection Act and Section 222 of the Homeland Security Act have also been formed on the basis of the FIPPs principles (Teufel, 2008).

Further legislative guidance may be available on a provincial basis. For example, in 2006 the Nova Scotia Government passed the Personal Information International Disclosure Protection Act (PIIDPA) and gave it teeth. Violation of this Act may cause organizations to incur substantial fines of up to $500,000. The Act addresses concerns about data sharing and foreign access to citizens' personal information.

Privacy policy guidance is also available on a sector basis in the US, Canada, and in many other countries. Ontario's Personal Health Information Protection Act (PHIPA) is a health sector privacy legislation that is substantially similar to Canada's federal private sector privacy legislation, *PIPEDA.* PHIPA establishes rules surrounding the collection, use, and disclosure of health information, codifies a client's right to confidentiality and establishes accountability and remedies for breaches (Cavoukian, 2010). The Privacy Commissioner of Canada's Office has investigated cases involving privacy issues with respect to the PIPEDA ranging across numerous industries including: Financial Institutions, Telecommunications industry, Health, Insurance, Transportation, Airline, School, Day care, Law firm, Retail, Restaurant, Internet service providers, E-mail provider, Telemarketing, Landlord/tenant and Real estate industries.

Privacy

"We've come to understand that privacy is the currency of our online lives, paying for petty conveniences with bits of personal information. But we are blissfully ignorant of what that means. We don't know what data is being bought and sold, because, well, that's

private" (Chase in Hess, 2017). "Privacy costs often become clear only after they've already been paid" (Hess, 2017).

Personal Information (PI)

Information considered to be personal includes names, birth dates, social insurance and social security numbers, home addresses, telephone numbers, email addresses, financial information, credit card information, or other contact information and personally identifiable data. Personal information may also include age, race, religion, financial and marital status and ethnic or national origin. PI is defined as "age, marital and financial status, race, national or ethnic origin, and religion" according to the Glossary of Canada Council Terms (2005). Personal information that

> (*a*) the organization collects, uses or discloses in the course of commercial activities; or
>
> (*b*) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

The definition this thesis uses for *personal information* is the "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Personal information that the organization "collects, uses or discloses in the course of commercial activities" or "is

about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business" (Office of The Privacy Commissioner of Canada, 2013).

According to the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) the definition of personal information also includes an applicant for employment with the organization.

Personally Identifiable Information (PII)

"Any (set of) data that can be used to distinguish or trace an individual's identity" is personally identifiable information (Sabo et al., 2012).

Personal Health Information

Personal health information is defined as "identifying information about an individual pertaining to that person's mental or physical health, family history or health care history. This includes:

- genetic information;
- registration information, including the Medicare number of the individual;
- information about payments or eligibility for health care or health-care coverage;
- information pertaining to a donation by the individual of any body part or bodily substance;
- information derived from the testing of a body part or bodily substance of the individual; and

- information that identifies the individual's health care provider or substitute decision maker" (Government of New Brunswick, 2013).

The form of information may be oral, photographed or written and applies to information recorded or stored in media such as electronic records, microfilm, paper, and X-rays (Government of New Brunswick, 2013).

Personal Information as an Asset

Some of the anecdotal connections among privacy and brand are revealed in a discussion of personal information as corporate assets. "If customers are typically considered a business' greatest asset, then their personal information must be considered one as well. Organizations will want to build and protect their assets, and personal information, as an asset, is no different" (Office of the Information and Privacy Commissioner of Alberta, n.d.).

The Privacy Commissioner of Canada's Office has stated, "Companies that cause consumers to feel as if their privacy has been invaded are in grave danger of losing the trust of their customers. And because brand has a lot, if not everything, to do with trust, the use of personal data has the power to make or break a brand—more power than anything that has ever come before it."

Privacy Concerns (PC)

Smith et al. (2011) recommended that researchers be mindful of their overarching macro model they call APCO, which stands for Antecedents → Privacy Concerns → Outcomes. Smith et al. (2011) believe that "positivist empirical studies will add the greatest value if they focus on antecedents to privacy concerns and on actual outcomes" (p. 989). Empirically descriptive studies have attempted to answer either: (1) "What is (and is not) privacy?" (2) "What is the relationship between privacy and other constructs?" (3) "To what extent does context matter in the relationships between privacy and other constructs? There is disagreement regarding the extent to which these relationships can be generalized across contexts, such as types of information, different industries, and new technological applications" (Smith et al., 2011, p. 992). I have done an extensive qualitative study of the types of information that are a concern for privacy (see Chapter 4).

Organizational Privacy Practices (PP)

Privacy practices within organizations are governed by their privacy policies. As mentioned previously, governments use the Fair Information Practice Principles (FIPPS) as a basis for privacy legislation, which in turn is used as guidance for organizational privacy policies (Bernstein, 2007; Cavoukian, 2011; Cavoukian & Hamilton, 2002a; Cocheo, 2000; Culnan & Armstrong, 1999; Delepine, 2011; Dillon et al., 2008;

Eisenhauer 2009; Federal Trade Commission, 2008; Freeman, 2011; Lockton & Rosenberg, 2006; Lugaresi, 2010; PIPEDA, 2010).

Another major set of principles for privacy is in the *Privacy by Design* (*PbD*) framework that Ann Cavoukian, former Information and Privacy Commissioner of Ontario and currently Executive Director - The Privacy and Big Data Institute at Ryerson University, successfully introduced to the world. This framework is translated in over 30 languages and adopted by dozens of countries, particularly those in the European Union. *PbD* consists of seven high-level and interrelated principles that extend traditional Fair Information Practice Principles to prescribe the strongest possible level of privacy assurance. Indeed, *Privacy by Design* (*PbD*) is a framework that influences technology design, business practices, and physical infrastructure. In 2010, *PbD* was voted on and unanimously recognized as a new global privacy standard at a meeting of the International Data Privacy and Protection Commissioners.

The *PbD* principles (see Table 2.1) seek to build a culture of privacy in organizations. Stakeholders embrace the importance of privacy and recognize their roles in implementing its *safeguards*. A mapping of *PbD* principles to the FIPPs is excerpted from Cavoukian (2011) below. According to the Office of the Information and Privacy Commissioner of Ontario, “the Fair Information Practice Principles and its relatives in this table may be applied universally to information technologies and organizational systems.”

Table 2.1

Privacy by Design Principles Mapped to Fair Information Practice Principles

PbD **Principles**	**Meta-FIPPs**	**Traditional FIPPs**
1. Proactive Not Reactive; Preventative Not Remedial	Leadership & Goal-Setting	---
2. Privacy as the Default Setting	Data Minimization	Purpose Specification Collection Limitation Use, Retention & Disclosure Limitation
3. Privacy Embedded into Design	Systematic Methods	---
4. Full Functionality – Positive-Sum, not Zero-Sum	Demonstrable Results	---
5. End-to-End Security Full Life-Cycle Protection	Safeguards	Security
6. Visibility and Transparency - Keep it Open	Accountability (beyond data subject)	Accountability Openness Compliance
7. Respect for User Privacy – Keep it User-Centric	Individual Participation	Consent Accuracy Access Redress

Note. Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices at https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf

To satisfy legislative privacy guidelines, changes to administrative, technical, and physical processes and equipment are needed (Firouzan & McKinnon, 2004**)**. Large organizations, in particular, hire privacy officers to be accountable and responsible for overseeing (1) communications with employees to ensure they understand privacy practices and other privacy-related matters, (2) training employees for privacy-related procedures and systems, (3) maintaining privacy policies, and (4) conducting privacy risk management, which involves understanding reputational and other harms. The privacy officers describe privacy principles in their privacy policies. Indeed, they often organize their privacy policies using FIPPs or legislation with FIPPS wording as section headings. A good example is Canadian Tire's Privacy Policy (Canadian Tire Centre, 2017).

Brand and Privacy

Organizations treat a good brand as an asset. The American Marketing Association defines a **brand** as a "Name, term, design, symbol, or any other feature that identifies one seller's good or service as distinct from those of other sellers" (American Marketing Association Dictionary, 2016). "A strong brand is hugely valuable - it embodies the brand owner's entire investment in its product, from the development time and resources, to the marketing and publicity and the good-will generated by the success of the product" (Hodson & Playle, 2003, p. 93).

"Today, given the changes in society, the steady march of technology, enforcement mechanisms that now exist, and how invasion of privacy can impact an enterprise's brand

and reputation, it's now time for Privacy 3.0, contends Andrew Serwin, a partner with Foley & Lardner in San Diego and a *Security* magazine 'Most Influential' executive" (Zalud, 2010). Privacy 3.0 is the idea of balancing data sensitivity against the benefit of collecting or processing it. Serwin believes "that there is a need to focus regulation on the most sensitive data with appropriate protection while reducing regulation where there is a societal benefit" (Zalud, 2010). Freeman (2011) agrees, "With all the media and legislative attention on Facebook's privacy practices, it makes sense to consider the impact that may have on your brand if you participate on the network" (p. 8).

Both in the U.S. and internationally privacy issues have taken on new prominence. This attention has been driven by the Internet, sophisticated marketing practices, legislation and regulation (Heffes, 2005).

"The leadership of Mayo Clinic knows that the brand is its most valuable asset. Without shareholders or a presence in the equity markets, there has been no reason to put a financial value on the Mayo Clinic brand. It is enough to know that the brand is invaluable and that, if lost, the reputation that is the brand would be gone forever. Any recovery would be partial, at best" (Berry & Seltman, 2007, p. 206).

As early as 1997, a link between privacy and brand appeared in the practitioner literature. The top 400 organizations in Australia were invited to participate in the *Price Waterhouse Privacy Survey* in that year. While the survey results showed the need to comply with international privacy standards was the most important privacy issue facing

organizations, the second highest priority was *the potential impact a privacy breach would have on the company's public image.* Other privacy issues were the move to legislate privacy in the private sector specifically with respect to telecommunications technology developments (Price Waterhouse Coopers, 1997).

Craig Spiezle, executive director and founder of the Online Trust Alliance, "emphasizes brands' new role in protecting customers' personal information: 'Privacy and security are important brand differentiators and companies need to move from a mindset of meeting compliance requirements to becoming a steward of consumer data'" (Maddox, 2015).

"Why you should notify individuals in certain circumstances: (a) Your customers and employees expect businesses to protect their personal information. They want to be informed about privacy risks associated with your personal information handling practices; (b) Through notification, you are demonstrating good privacy practices and building trust into your brand; and (c) good privacy means good business" (Office of the Privacy Commissioner of Canada, 2008a).

According to the Canadian Marketing Association, (2006, p. 12) "Privacy, they (Management) acknowledge, is intimately connected with the organization's reputation – which is among its most valuable assets." "The need for institutional privacy assurances is predicated on the assumption that companies have an incentive to address privacy

because if they fail to do so they will suffer reputational losses" (Xu, Smith, Dinev & Hart, 2008, p. 7).

Brand Protection and Privacy

Multiple definitions of brand protection exist, often in accordance to domain experts' perspectives, or well-established contexts. For example, brand protection is "the act of preventing someone from illegally making and selling a product using a brand name owned by another company" according to the Cambridge Business English Dictionary (2011).

Brand protection is "legislation forbidding other firms from using a company's registered brand names or brand marks without permission" (Bradmore, 2004). According to Berry and Seltman (2007, p. 208) brand protection is "much more a human art than a quantitative science, encompassing each type of influence in the services branding model: the presented brand, external brand communications, and customer experience with the organization."

In this thesis, I integrate the various definitions of brand protection to produce a more comprehensive definition: ***"Brand protection refers to the management, marketing, and legal practices that organizations put in place to protect their brand from counterfeiting and devaluation."***

In interviews conducted by Oehlert (2014) with Insurance ISU agents they were asked 1) "Where does the protection of the organization's reputation and brand fall on the

agency's list of concerns?" Mark Duncan, CPCU, from the Olson Duncan Agency in Torrance, CA, replied "At the top! Branding and reputation are two primary reasons we became an ISU agent. We have embraced the ISU image and enhance it by the ethical manner in which we conduct business."

Smit, Bronner and Tolboom (2007) reported that Harris and Ogbonna (2002) found that "85% of all customer contact employees had performed acts of sabotage in the week prior to their research" (p. 84). "Service employees are brand champions when their frontline performance supports the brand message. Conversely, employees are brand saboteurs when their performance detracts from the brand" (Wallace & De Chernatony, 2009, p. 82). Eighty-five percent is a very high percentage. If the act of sabotage were related to the protection of personal information, as will be included in this study, then it is believed that this would have a negative impact of the brand of the organization.

Sophisticated skills and knowledge are required for brand protection programs. Filtering programs, deleting cookies, or downloading antivirus software are examples of tools for protecting one's privacy (Youn, 2009, p. 395). However, who have the responsibility for deploying, managing, and using the tools are different people with different roles. "Options for privacy protection require sophisticated technical skills and knowledge, which can be highly challenging to young adolescents, and the responsibility in the application of such technologies primarily lies with adults in authority (e.g., parents or teachers) rather than with the child (Maddux et al., 1986; Rifon, LaRose & Lewis,

2007). In Yan's study (2006), young adolescents in grades 7 and 8 were shown to not yet have fully developed knowledge of online protection strategies such as firewalls and password protection" (Youn, 2009, p. 395).

Privacy Training in a Brand Protection Program

Formal training and skills audit are examples of employee development practices that are critical for equipping employees with new knowledge, skills, and competencies according to Iverson and Zatzick (2007). Formal training can "develop employee skills and behavior scripts and motivate employees to apply their skills and behavior scripts… to gain access to a workforce that produces superior employee output" (Way, 2002, p. 769).

Education and training are keys with respect to workplace privacy (Cavoukian & Hamilton, 2002b). A study conducted by Ponemon Institute found that "Negligent insider breaches have decreased in number and cost most likely resulting from training and awareness programs having a positive affect on employees' sensitivity and awareness about the protection of personal information" (Ponemon Institute, 2012). In a survey conducted by Smith, Koohang & Behling (2010) with complete responses from 60 Information Technology (IT) managers, 85% found data privacy to be the most important technology management challenge of the ten challenges universal to both business and government operations. Data management (78.3%), meeting legal requirements (76.7%) and protecting systems from hackers (76.7%) were also identified as very important

privacy management issues. Only 48.3% of the managers thought employee penetration was very important, this involves insiders penetrating and manipulating the system as opposed to outsiders, which is classified as hackers. Smith et al. (2010, p. 96) state that, "Training plays an important role in creating a viable workforce capable of exercising judgement." The authors were surprised by the "perception that staff training is not as important as several others issues, as training is the basis for ensuring that all employees understand their responsibility to protect customer and consumer privacy and data" (Smith et al., 2010, p. 96). Security awareness training was reported as being conducted by 60% of the respondents but of the 60% only 44.7% said that the training was "mandatory" (Smith et al., 2010, p. 96).

An example of the importance of training to privacy is provided of a case where training was strongly recommended for management and staff to learn how to protect personal information from third party disclosure. An investigation by The Office of the Privacy Commissioner found that the complaints alleged against Laurier Optical were well founded. The provisions of the Act that the organization failed to respect were (i) disclosure of personal information without the complainant's consent, and (ii) failure to provide him with access to his personal information. The Office of the Privacy Commissioner "strongly recommend that Laurier Optical take steps to *train* its management and staff about the requirement under the Act to protect a client or former

client's personal information from disclosure to third parties, including when responding to complaints from clients and former clients" (PIPEDA Report, 2011).

In step 4: Prevention of Future Breaches contained within the Privacy Breach Checklist provided on the Office of The Privacy Commissioner of Canada's web site it asks "What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?" (Office of The Privacy Commissioner of Canada, 2007, p. 2). As part of the solution to correct the situation of future breaches of privacy it suggests staff training. Along with developing and reviewing policies and audits, staff training should be conducted to prevent initial and future breaches.

Training for employees, conducting security reviews, having a security program that is documented and designating someone accountable for the program is required by law in Massachusetts. It was "among the first of many states to pass laws that require companies to protect any data about its residents" (Smith, Koohang & Behling, 2010, p. 93). Privacy training is a must for frontline workers, says Dr. Ann Cavoukian, Ontario's former Information and Privacy Commissioner. Privacy and data security policies and practices matter little if they are stuck at the executive level. She recommends that they be moved right down to employees who actually deal with citizens.

Ms. Albornoz Mulligan of Forrester Research states that "People have been mostly concerned about security, so privacy was given short shrift. But a lot of solutions to security problems are technology-based, while privacy is more about process and

education than technology." Ms. Albornoz Mulligan also reported that "If you don't have good security, you can't have privacy" (Pachner, 2008).

Nuala O'Connor, previous global privacy leader at General Electric, and current president and CEO of the Center for Democracy and Technology acknowledges that "privacy and security have to be a cross-functional priority for companies, enhancing the marketing strategy with input from privacy and security experts: 'Privacy professionals need to be engaged with teams across the organization, not just IT, legal, and compliance departments. They should participate in early stage product design processes, meet with the engineers and customer services representatives and take part in marketing and sales efforts'" (Maddox, 2015).

Privacy training and development programs in Canada educate employees about ten fair information practice principles. These principles are contained in the *Personal Information Protection and Electronic Documents Act (*PIPEDA).

Price Waterhouse Privacy Survey conducted in Australia in 1997 found: "Training is also vital to ensure employee compliance with any privacy policy. Consistent with our 1996 survey, 80 per cent of organisations surveyed stated that they did not undertake any form of privacy training. This will clearly hinder the operation of any privacy policy as employee awareness and understanding are two key drivers to the successful implementation of good privacy practice" (Price Waterhouse Coopers, 1997).

Privacy training should be thought of as an "opportunity to ensure that employees really know how to protect information" (Cline, 2010, p. 24). Cline (2010) suggests that organizations should consider if employees are receiving conflicting messages from their chief privacy officer, chief information security officer and legal department. If this is occurring, it will need to be addressed. It should become part of the culture of the organization. For an effective training program, smaller groups will need to be educated about what they will be required to do to implement the objectives of the privacy policy.

"Employee training is probably the most important component of an information risk management process … Every regulation that mandates that reasonable measures be taken to protect information implicitly requires companies to set up training programs to help employees understand what those measures are" (Cline, 2010).

Brand Value (BV)

Brand Value with reference to the Brand Finance literature is the "net present value of the estimated future cash flows attributable to the Brand" (Brand Finance, 2014). The variation between a company's book value and market value can be rationalised by an intangible asset such as brand. Brand Finance's research showed that intangibles account for 62% of the world's business or a global market value of $19.5 trillion of $31.6 trillion. Customer loyalty, staff retention/recruitment are used to measure brand value in the case of consumer product brands (Brand Finance, 2014). "In today's environment there are so many sources of risks especially from a technology standpoint. Security breaches whether

it's operational failures due to technology, those issues become public and really do impact an organization's brand in the public eye and to their stockholders" PwC US. (2012). It is common knowledge in the practitioner's literature that a breach can affect an organization's brand to the public and to their stockholders. This research gathers data to scientifically measure and quantify the relationships between Privacy concerns, privacy practices, brand protection, experienced harms, and brand value.

Two of the largest retail privacy breaches occurred at TJ Maxx and Target, and are used as examples of the effect a privacy breach had on their stock prices. The privacy breach that was announced on March 28, 2007 at the parent company of T.J. Maxx affected 90 million records. The breach affected customers in the Canada, Puerto Rico and the U.S., and potentially in Ireland and in the U.K. "Customers of its T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores" were affected by the data breach in the U.S. and Puerto Rico. "Customers of its Winners and HomeSense stores in Canada and TK Maxx stores in the U.K" were also affected. Thousands of payment cards had to blocked and reissued as a result of the breach. "In addition, personal data provided in connection with the return of merchandise without receipts by about 451,000 individuals in 2003 was also stolen" from TJ Maxx (Vijayan, 2007).

A data breach at Target "compromised 40 million credit and debit card accounts between Nov. 27 and Dec. 15. Then on Jan. 10, the company said hackers also stole personal information – including names, phone numbers as well as email and mailing

addresses – from as many as 70 million customers" (Associate Press, 2014). "Target reported in February that its fourth-quarter profit fell 46% on a revenue decline of 5.3% as the breach scared off customers." "The company's sales, profit and stock price have all suffered since the breach was disclosed." "Shares fell nearly 2% in pre-market trading Monday." "When the final tally is in, Target's breach may eclipse the biggest known data breach at a retailer, one disclosed in 2007 at the parent company of TJ Maxx that affected 90 million records" (Associate Press, 2014). The below discusses the academic literature for brand value.

The Brand Value Chain

The brand resonance model connects brand with customers on a deep emotional level. The brand value chain starts with investing in a marketing program (products, prices, places and promotions) that leads to a customer mind set. This effort results in what the customer thinks about your brand in terms of awareness, excitement, fun, security and warmth, and loyalty, which leads to customers purchasing a product and becoming repeat buyers. This ends in shareholder value, which ideally we want to be increased and optimized. Other definitions of brand value are coincident. "Brand value (BV) is a measure of the intrinsic utility or value of a brand to consumers, after adjusting for situational factors" (Kamakura & Russell, 1993, p. 20). "Brand Value measures

perceived quality, the value assigned by consumers to the brand, after discounting for current price and recent advertising exposures."

Interbrand, one of the world's leading brand companies helps companies create and manage brand value. Interbrand accesses brand value in both customer and financial terms in three ways (1) brand's financial performance (2) influence on customer choice and (3) the brand strength relative to competition. The brand value they calculate is a single measure of the brand's contribution to business results (Interbrand's Brand Valuation Methodology, 2013).

Brand Value Scale

Barnes & Mattsson (2008) brand value scale (see Table 2.2) will be adopted in this dissertation's survey instrument. Their study is based on "Hartman's axiology and uses nine items for measuring the various aspects of brand value. In addition, an overall item for assessing convergent validity is also included (question 10)" (Barnes & Mattsson, 2008, p. 199). "Dr. Hartman identified three dimensions of reality, which he called the Dimensions of Value. We value everything in one of these three ways or in a combination of these dimensions. The Dimensions of Value are Systemic, Extrinsic, and Intrinsic" (Hartman, 2001).

Table 2.2

Barnes & Mattsson's Brand Value Scale

Item No.	Question
1	I feel great pride identifying with Mazda.
2	What Mazda delivers feels right for me.
3	I feel I am able to trust Mazda completely.
4	Mazda does me good.
5	Mazda is a satisfying buy.
6	What I get from Mazda is worth the cost.
7	The uniqueness of Mazda stands out.
8	Mazda is a symbol of quality.
9	Information about Mazda is always correct.
10	Mazda is a good brand.

Note. "Brand value in Virtual Worlds: An axiological approach" by S. Barnes, and J. Mattsson, 2008, *Journal of Electronic Commerce Research, 9*(3), p. 206.

Hypotheses for Privacy Practices, Brand Protection for Privacy, and Brand Value

Summarizing the foregoing literature, major *drivers for data protection programs are legal compliance and risk management including risk around brand.* In one 2011 survey, 50 percent of respondents agree or strongly agree that senior management in their organizations believes that the need to comply with regulations, laws and other mandates is the main reason senior management will fund and support a data protection program. "Twenty-six percent say it is a desire to protect the company's reputation and maintain customer trust and loyalty" (Ponemon Institute, 2011, p. 2).

Negative publicity is possible for an organization when the Privacy Commissioner Offices across Canada post the results of their investigations into privacy violations. The US' Federal Trade Commissioner also posts the results of their investigations and can

also enforce large corporate penalties. For example, the FTC has two large Internet organizations under years of privacy audit – one for as much as 20 years. Non-compliance to privacy legislation, in terms of organizations' privacy practices, leads to the very real risk of reputational harm and (un)associated financial penalties. Risks to an organization's brand and financial position are managed as a priority in many organizations.

If brand protection is explored from my definition within the context of privacy, and if the external communications are positive about the organization, then these should promote a good brand. However, if the external brand communications are negative about the organization, i.e. a privacy breach occurred and was not well-handled, then these will have a negative influence on the brand. I intend to formally investigate these loosely-connected relationships among privacy practices, brand protection, and brand value found in the literature from the employees' perspective, and put forward the following hypotheses:

Hypothesis 1. An organization's privacy practices (PP) will be significantly and positively associated with its brand protection (BP). **H1: PP → BP**

Hypothesis 2. An organization's privacy practices (PP) will be significantly and positively associated with its brand value (BV). **H2: PP → BV**

Hypothesis 3. An organization's brand protection (BP) will be significantly and positively associated with its brand value (BV). **H3: BP → BV**

Experienced Harms due to Privacy Breaches

Anecdotally, an organization's brand and reputation can be impacted by a privacy breach. According to the Ponemon Institute a breach is defined as "an event in which an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk - either in electronic or paper format" (Ponemon Institute, 2014a, p. 3). "A lapse in the handling of customer or employee information could cost companies dearly, not only in dollars (in lawsuits), but also in reputations and subsequent customer loss. Yet while most U.S. companies follow the law, only about 5 percent of the largest U.S. corporations seem to demonstrate a 'strategic' view of privacy, by creating a management position for the implementer of policies, the 'chief privacy officer (CPO)'" (Westin as cited in Heffes, 2005, p. 30). Further, Dr. Alan Westin states that the three things that are driving privacy as a business concern are (1) identity theft (2) spyware and monitoring and (3) huge new regulatory changes in the financial services industry with GLBA (The Gramm-Leach-Bliley Act, or The Finance Modernization Act of 1999). "There's a feeling that the Internet is not a safe place to be" (Westin as cited in Heffes, 2005, p. 30) since "footprints" are left behind leading to harvesting and misuse of identities and information.

People are now given certain choices when they receive notices telling them what information is being collected. Both regulations and the threat of civil litigation issues are reasons why financial-services businesses must pay serious attention to privacy:

> All of the major industries that deal with consumer relations have been impacted by privacy regulation--telecommunications, financial-services, health and medical--and if you're online in any industry, privacy is relevant. Take health, for example. Driven by privacy rules under HIPAA (The Health Insurance and Portability Accountability Act), every doctor or dentist, pharmacy or hospital handling health data-processing is now knee-deep in regulations [and responsible for] privacy notices. These [notices] have intensified the concern about privacy, and moved it from a kind of 'yes, maybe we should say something nice and tell consumers we're concerned about their privacy,' into a 'major marketing, compliance, brand and public image issue.'

Anthem Health Insurance had a data security breach that compromised the personal information of 80 million plan participants. "With the recent data security breaches at several powerhouses, brands need to find new brand management strategies to maintain their value" (Maddox, 2015). Some of the well-known brands that have been compromised by cybercrime include: Target, Home Depot, Zappos, Sony, Anthem and JP Morgan Chase.

Zappos' CEO Tony Hsieh said "We've spent over 12 years building our reputation, brand, and trust with our customers. It's painful to see us take so many steps back due to a single incident." The data security breach that Hsieh is referring to compromised 24 million customers' names, addresses and passwords in 2012.

> Aside from the costs of damage control after a breach has been discovered, the stigma attached to the loss of customers' personal information can have a negative impact on their willingness to choose a brand in the future. This calls for a new type of brand management. As more brands depend on customers maintaining online accounts — full of personally identifying information — to generate revenue and remain competitive, brands need to ensure their value propositions around online safety are more than window dressing (Maddox, 2015).

"The importance of protecting the people who keep brands in business — especially in the ultra-competitive retail industry." In the fall of 2013 forty million credit card numbers were compromised in the Target hack. In two months Target spent $61 million to cover damages from the breach. "The biggest impact was the ripple effect on corporate profits for the holiday season, as Target suffered a 46 percent loss in profit from same-quarter sales year-over-year. The most mind-boggling aspect of the whole incident was that Target had spent more than $1 million to implement preventative cyber security and measures six months before it even happened" (Maddox, 2015). This is evidence of the financial loss an organization faces when the privacy of their customers' personal information is compromised.

"The resulting potential for lost revenue and customer loyalty is even more worrisome to brands that allow customers' sensitive personal information to be exposed. With so much at stake, it's important for brands to ensure that claims of safety and

privacy aren't just marketing fluff and that it is actually part of an overarching brand management strategy, but backed by solid systems and policies designed to protect customer data" (Maddox, 2015).

> Brands can achieve a competitive advantage from their security and privacy practices: Another cautionary tale is Sony Corp. The highly publicized breach at Sony Pictures earlier this year revealed once again that the billion-dollar, multi-national entertainment brand was lax in protecting its digital assets - similar to the incident that occurred with its PlayStation division in 2011. The issues with protecting customer data and their own employees' information raise serious concerns about entrusting sensitive personal information to any network that Sony operates. As Sony plans to launch its Vue premium cable-over-the-Internet service in 2015, the company's poor track record of protecting customers' personal information could impact its ability to attract new subscribers. With so many banking, retail, and entertainment options for consumers to choose from, and practically zero switching cost, security and privacy become more than just table stakes. They can provide a competitive advantage for brands (Maddox, 2015).

"The annual U.S. Cost of Data Breach Study tracks a wide range of cost factors, including expensive outlays for detection, escalation, notification and response along with legal, investigative and administrative expenses, customer defections, opportunity loss,

reputation management, and costs associated with customer support such as information hotlines and credit monitoring subscriptions" (Ponemon Institute, 2012). In the 2014 and 2015 Cost of Data Breach Study three main causes of a data breach have been identified. These are 1) a malicious or criminal attack (44% in 2014 and increased to 47% in 2015); 2) employee negligence or human error (31% in 2014 and decreased to 25% in 2015); or 3) system glitches (25% in 2014 and increased to 29% in 2015) (Ponemon Institute, 2014b; 2015). The cause and the safeguards in place at the time of the data breach can vary the costs of a data breach (see Table 2.3).

Table 2.3

Causes of a Data Breach

Causes of a Data Breach	**Global %**				**Per Capita Data Breach Cost per Compromised Record (U.S.$)**			
	2014	**2015**	**2016**	**2017**	**2014**	**2015**	**2016**	**2017**
Malicious or criminal attack	42	47	48	47	$159	$170	$170	$156
Employee negligence or human error	30	25	25	25	$117	$137	$133	$126
System glitch	29	29	27	28	$126	$142	$138	$128

Note. Ponemon Institute, 2014a; 2015; 2016; 2017.

Ponemon Institute (2014b, p. 1) determined that in the United States in 2014 "the average cost for each lost or stolen record containing sensitive and confidential information increased from $188 to $201. The total average cost paid by organizations in

the United States increased from $5.4 million to $5.9 million." On a global basis the average total cost in US$ of a data breach increased from 3.52 million in 2014 for 314 companies to 3.79 million dollars for the 350 companies participating in the research study in 2015. It then increased to 4.00 million for 383 companies in 2016 and decreased to 3.62 million dollars for the 419 companies participating in the research study in 2017. There was an increase from $145 in 2014 to $154 in 2015 to $158 in 2016 and decreased to $141 in 2017 for the average cost paid for each lost or stolen record containing confidential information. Although the average cost went down in 2017 the average size of the data breaches increased by 1.8 percent (Ponemon Institute, 2014a; 2015; 2016; 2017).

"Our research shows that the healthcare industry is struggling to protect sensitive medical information, putting patients at risk of medical identity fraud and costing hospitals and other healthcare services companies millions in annual breach related costs," says Dr. Larry Ponemon. The cost of a data breach varies by the industry for example in healthcare the average cost is as high as $363 and $300 in education, $121 in transportation whereas the lowest cost per lost or stolen record is $68 in the public sector. The average cost across 320 industries increased from $105 in 2014 to $165 in 2015.

Results from Ponemon Institute's 2015 Cost of Data Breach Study: Global Analysis May 2015 state that,

> JPMorgan Chase & Co. and Sony Pictures Entertainment were two highly publicized mega breaches that occurred in 2014. Seven million small businesses and 76 million households were affected by the JPMorgan Chase & Company data breach. Sony's correspondence and employees' personal data were leaked during a major online attack (Ponemon Institute, 2011).

The 2015 Ponemon Institute study found that a data breach involving at least 10,000 records would most likely occur in Brazil and France with laxer privacy enforcement and penalties to organizations and least likely to happen in Canada and Germany. Data breaches are likely to cost the most per capital cost in the United States ($217) and Germany ($211) and the lowest in Brazil ($78) and India ($56). The highest average total organizational cost is 6.5 million dollars in the United States and 4.9 million in Germany; the lowest organizational costs are 1.8 million in Brazil and 1.5 million in India. There has been a 23% increase in the total cost of a data breach since 2013. The average cost for a lost or stolen record is 154 U.S. dollars.

In Ponemon Institute's 2017 study Canada was determined to have the lowest probability of having a future data breach (14.5%) but data breaches on average per capita cost were found to be the most expensive in the United States ($225) and Canada ($190) and cost the least amount in Brazil ($79) and India ($64). In the United States the average total organizational cost for a data breach was $7.35 million and the lowest average total organizational cost was in Brazil ($1.52 million). Although the average global cost is

$141 for a data breach per lost or stolen record the average cost in health care organizations is $380 and in financial services the average cost is $245 (Ponemon Institute, 2017).

Key findings of the research are:

> The impact of a data breach over a two-year period is approximately $2 million per organization and the lifetime e value of a lost patient is $107,580. The average organization had 2.4 data breach incidents over the past two years. Major factors causing data breaches are unintentional employee action, lost or stolen computing devices and third-party error. Healthcare organizations are not protecting patient data. Organizations have little or no confidence in their ability to appropriately secure patient records (58 percent). Protecting patient data is not a priority. Seventy percent of hospitals stated that protecting patient data is not a top priority (Zalud, 2010).

The Digital Privacy Act was passed by the Canadian government in June 2015. This will require that notification of data breaches and regulations regarding reporting become part of Canadian privacy law. This is expected to go into effect in late 2017. When it does it is predicted that privacy breaches will sky rocket because “organizations will have to log all breaches, and users will have to be notified of any breach that poses a ‘real risk or significant harm’” (Braga, 2017). This refers to “any information that could be used to commit fraud or pull off a social engineering attack - for example, names and addresses,

credit card data, security questions and passwords, or past orders on an online shopping site. But it could also include information with the potential to humiliate or damage a person's reputation" (Braga, 2017). A fine of up to $100,000 could be issued if organizations fail to log a breach or notify users if their data is lost or stolen (Braga, 2017).

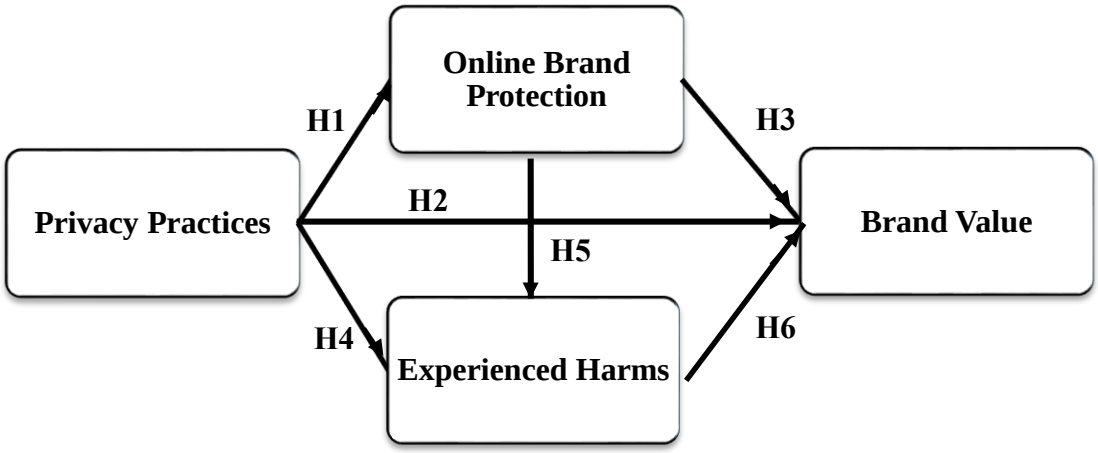
Once a privacy breach occurs "most customers just disappear as suddenly and silently as their data did" (Maddox, 2015). Acquisti, Friedman and Telang (2006) report that data breaches can impact negatively (albeit temporarily) on the stock market valuation of an organization. Results from Smit, Bronner and Tolboom's study (2007) suggest that it is worth the effort to invest in brand relationships because "better relationships reduce the fear of inadequate privacy protection" (p. 627). In this research I believe that it is worth investigating the employee-brand relationships. If employees follow practices to protect data then this can result in positive brand protection. "Service employees are brand champions when their frontline performance supports the brand message" (Wallace & De Chernatony, 2009, p. 82). However, "employees are brand saboteurs when their performance detracts from the brand" (Wallace & De Chernatony, 2009, p. 82). I hypothesize this is also the case with organizations' failure to protect privacy through practices, and formal brand protection programs for privacy.

Hypothesis 4. Experienced harms will be significantly and negatively associated with organizations' privacy practices. **H4: PP → -EH**

Hypothesis 5. Experienced harms will be significantly and negatively associated with organizations' efforts at brand protection. **H5: BP → -EH**

Hypothesis 6. An organization's brand value will be significantly and negatively associated with experienced harms. **H6: EH → -BV**

Initial Privacy-Brand Model



Privacy Practices guided by:

1. **Privacy Laws and Regulations**

2. **Privacy Policies informed by Privacy Principles (FIPPs/*PbD*):**
   1. Consent
   2. Accountability
   3. Purposes
   4. Collection limitation
   5. Use, Retention, and Disclosure limitation
   6. Accuracy (reduce errors)
   7. Security
   8. Openness
   9. Access (control of personal data)
   10. Compliance

Brand Protection Programs comprise:

1. Privacy Training of Privacy Policies and Practices
2. Stakeholder/User/Data Subject Awareness (Communications)
3. Management (e.g. Alignment, Accountability and Role Responsibility Assignment, Best Practices Use, Use of Privacy Management Models, and/or methodologies)
4. Privacy Impact Assessments (PIAs)
5. Auditing
6. Technical defenses

Experienced Harms from Privacy Breaches such as:

1. Credit card fraud
2. Digital brand abuse
3. Social media
4. Website integrity/ defacement
5. Organizational Identity theft
6. Intellectual property abuse
7. Domain name and web traffic diversions
8. Online trademark infringements
9. The use of your brand in phishing attacks

Brand Value

1. Financial
2. Reputational

Figure 2.1. Initial Privacy-Brand Model with Privacy Practices, Brand Protection, Experienced Harm and Brand Value Summary.

The above model (see Figure 2.1) is not found in the current literature and thus, if validated, it would represent a new contribution.

Hypotheses

Hypothesis 1. An organization's privacy practices (PP) will be significantly and positively associated with its brand protection (BP). **H1: PP → BP**

Hypothesis 2. An organization's privacy practices (PP) will be significantly and positively associated with its brand value (BV). **H2: PP → BV**

Hypothesis 3. An organization's brand protection (BP) will be significantly and positively associated with its brand value (BV). **H3: BP → BV**

Hypothesis 4. An organizations' privacy practices (PP) will be significantly and negatively associated with experienced harms (EH). **H4: PP → -EH**

Hypothesis 5. An organizations' efforts at brand protection (BP) will be significantly and negatively associated with experienced harms (EH). **H5: BP → -EH**

Hypothesis 6. An organization's experienced harms (EH) will be significantly and negatively associated with brand value (BV). **H6: EH → -BV**

CHAPTER 3 - SURVEY INSTRUMENT AND RESULTS

This chapter describes the construction of the survey instruments I created to obtain data to validate my proposed model. A very short preliminary survey instrument was first created to capture and understand what are the privacy concerns in the second decade of the 21st century, and in the present-day technological context. A second much longer survey was created to capture information on the constructs of interest in this thesis. Where possible, scales were re-used and where constructs were extended or enhanced with present-day contexts, new scales were created.

Due to the length of the second survey, the percentage responses for the *Privacy Management Survey* results are provided in Appendix E. A few highlights of the percentage responses to each construct's scale is also provided in this chapter.

Method

Preliminary Privacy Concerns Survey

The first short survey instrument referred to as the *Preliminary Privacy Concerns Survey* (see Appendix B) included instructions (see Appendix A) and one open-ended question around people's privacy concerns when online. Participants were asked what concerns do you have about network traffic privacy? The demographics questions inquired about the participants' age range, gender, education, country of origin, country of residence and their Profession/Occupation (see Table 4.2). Chapter 4 describes the data

collected from the survey in detail, presents its analysis, and contribution to question creation for the second survey.

Privacy Management Survey

Once I built The *Privacy Management Survey*, (see Appendix C) I had it reviewed by my supervisor, and by many other privacy experts in the field including: Catherine Tully, Information and Privacy Commissioner for Nova Scotia; Carla Heggie, Past Information Access & Privacy Manager, Government of Nova Scotia; Bob Doherty, Owner, Robert P. Doherty Access and Privacy Services; and Doug Stephen, Information & Privacy Coordinator at Alberta Health Services to name a few, to provide content validity.

I conducted many hard copy trial runs at security and privacy conferences. The attendees' valuable comments and advice were incorporated into the survey instrument. The survey began with an introduction to the researchers with our contact information. Participants were invited to participate in the research if they were at least 18 years old and employed. Instructions were provided to complete the survey. Most questions were answered by selecting the best answer on the seven-point scale that is anchored with "strongly disagree" and "strongly agree." Potential benefits were included. A disclosure stated that the research was approved by Saint Mary's University Research Ethics Board, REB file # 14-340. A thank you was included to all those who participated in the survey.

There were 210 survey questions grouped according to privacy practices, privacy concerns, privacy breaches, brand protection and brand value. Definitions were provided

for personal information, organization and privacy breaches. Two open-ended questions were asked regarding concerns about the privacy of personal information and about network traffic. Demographic information was collected about the participant and their organization (see Participants (N = 315) section at the end of this chapter).

Definitions Included On Survey

The definition for *personal information* means "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Personal information that the organization "collects, uses or discloses in the course of commercial activities" or "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business" (Office of the Privacy Commissioner of Canada, 2013).

The definition for *organization* refers to "private sector entities, public bodies (government departments, agencies, boards and commissions, municipal bodies) and health custodians" (C. Tully, personal communication, January 29, 2015). The description for a *privacy breach* occurs when "information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification" (Personal Health Information Act, 2010).

"Most of the questionnaires embraced in the cited literature ask about *privacy* rather than *information privacy*, as do the general surveys of polling agencies" (Smith et al.,

2011, p. 991). My surveys are asking about *information privacy* of *personal information* and *network traffic.*

Data Collection and Analysis

A literature review provided the background to build the *Privacy-Brand Model* and the constructs studied in this research (see Chapter 2). Validated scales in the literature were incorporated in the questionnaire to test the hypotheses in the model and where there were no scales available scales were generated or modified in each instance.

The privacy practices statements were created according to the ten *The Personal Information Protection and Electronic Documents Act* (PIPEDA) *Fair Information Principles* (FIPs) and are explained below. Privacy concern statements are included from privacy scales, in anticipation of this thesis' second study, which would expand on an initially proposed privacy-brand model with the added privacy concerns construct. In addition privacy concern statements were developed from the qualitative data gathered in the *Preliminary Privacy Concerns Survey*. The categories of privacy concerns identified are explained in Chapter 4. The privacy concerns gathered from the preliminary survey's qualitative data were also gathered on the *Privacy Management Survey* to confirm the privacy concerns gathered in the preliminary survey and to identify new privacy concerns, which may have evolved. These privacy concerns are discussed in Chapter 6 in the *Expanded Privacy-Brand Model*. Privacy breaches statements were developed from the literature review and through examples of actual privacy breaches. Brand Value

statements were included from the Brand Value Scale used in Barnes & Mattsson (2008) paper, entitled Brand Value In Virtual Worlds: An Axiological Approach.

Specific Aims

The specific aims of this research are to investigate the links between privacy related variables (e.g. privacy concerns) and the outcomes of these variables on brand. To the best of my knowledge there is little work on privacy and its effect on the organization's brand protection and brand value, and no scientifically validated models connecting them. The studies in this work will form a new contribution to the literature.

A *Preliminary Privacy Concerns* study was conducted in 2009 and 2010. Privacy concerns were qualitatively gathered from this study. These privacy concerns were gathered and incorporated into the *Privacy Management Survey* conducted in January 2016.

Incorporating subscales from Smith, Milberg and Burke's (1996) validated instrument, I investigated if the primary dimensions of individuals' concerns about organizational informational privacy practices are still valid and explore new concerns for information privacy to build upon. The preliminary study was helpful in informing the final *Privacy-Brand Model*.

The Privacy Management Survey is large. Among other things, it investigates if brand protection measures are in place e.g. privacy training, and whether privacy programs and practices provide awareness, alignment and management of privacy

policies with practices and captures whether privacy impact assessments (PIAs) and auditing are being conducted.

The survey determines if privacy breaches or threats are occurring within the organization. It looks in depth at the nature of these breaches and if an organization's brand value is affected by privacy breaches.

The variable associated with the survey statement is included to help identify the statement when the variable is used in models in Chapters 4 and 6. For example, PP_RESPO is part of privacy practices and is related to the statement, My organization is responsible for personal information under its control.

Survey Questions and Percentage Results

The following statements on the survey related to privacy practices have been modified from the privacy principles (Office of the Privacy Commissioner of Canada, 2009). The fair information privacy principles (FIPPs) are the building blocks for the *Personal Information Protection and Electronic Documents Act* (PIPEDA). There are two federal privacy laws in Canada: *The Privacy Act* and *The Personal Information Protection and Electronic Documents Act* (PIPEDA). *The Privacy Act* covers "the personal information-handling practices of federal government departments and agencies" and *PIPEDA* covers "the federal private-sector privacy law" (Privacy Legislation in Canada, 2014).

With the risks that the government and organizations face with threats to their networks and security practices it is important to include privacy practices on the survey so we know what organizations are doing to protect personal information. It is also crucial for an organization to build privacy and security into their design. This is known as privacy by design. Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada from 1997 to 2014 argued for "*Privacy by Design*" (*PbD*). It is a philosophy that developers build privacy and protection for data into the original design. During development privacy is embedded into the technology.

The survey questions make us aware if organizations are being accountable, if they are identifying the purpose for collecting personal information, what they are doing around consent, and if they are limiting the amount of information they collect, use, disclose and retain. The practices will allow us to know if the information is being kept accurate and stored safely. The questions will identify if the organizations' policies and procedures are available, if individuals can access their information upon request and if they can challenge compliance with an individual responsible for the organization's compliance. The first fifteen questions on *The Privacy Management Survey* are about an organization's privacy practices built around PIPEDA's fair information principles as provided in Chapter 2.

I have provided the statements in the next section from Smith, Milberg & Burke's (1996) *Concern for Information Privacy (CFIP) Instrument*. They asked participants,

from the standpoint as an individual, the extent to which they agreed or disagreed with their statements related to four subscales: (1) collection; (2) unauthorized secondary use; (3) accuracy; and (4) improper access. I included statements on the survey related to their four subscales.

PIPEDA Principles Adapted to Privacy Practices Survey Statements

Two statements were included on the survey to determine how accountable organizations are for privacy, making good business sense. "An accountable organization can demonstrate to customers, employees, shareholders, regulators, and competitors that it values privacy, not only for compliance reasons, but also because privacy makes good business sense" (Office of the Information and Privacy Commissioner of Alberta, n.d.).

Principle 1 - Accountability

1). PP_RESPO: My organization is responsible for personal information under its control. Eighty-nine percent agreed (55% strongly agreed, 23% agreed, 11% moderately agreed) that their organization is responsible for personal information under its control. Six percent neither agreed nor disagreed / neutral and only 5% disagreed.

2). PP_DESIG: My organization has designated an individual or individuals who are accountable for the organization's compliance with the Privacy principles (Fair information principles).

Eighty percent agreed (42% strongly agreed, 28% agreed, 10% moderately agreed) that their organization has designated an individual or individuals who are accountable for the organization's compliance with the Privacy principles (Fair information principles). Thirteen percent neither agreed nor disagreed / neutral and only 6% disagreed. The majority of the organizations surveyed were found to be accountable for privacy.

When personal information is collected the organization should identify the purposes for collecting the information. The following statement was included to examine if purposes are identified for collection of personal information.

Principle 2 - Identifying Purposes

3). PP_PURPO: My organization identifies the purposes for which personal information is collected at or before the time the information is collected.

Eighty-eight percent agreed (49% strongly agreed, 28% agreed, 11% moderately agreed) that their organization identifies the purposes for which personal information is collected at or before the time the information is collected. Eight percent neither agreed nor disagreed / neutral and only 4% disagreed. The majority of the organizations surveyed were found to identify the purposes for which personal information is collected at or before the time the information is collected.

Consent may be given by not opting out of a transaction or by agreeing to the collection, use, or disclosure of personal information.

Principle 3 - Consent

4). PP_CONSE: My organization requires the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate. Eighty-five percent agreed (51% strongly agreed, 24% agreed, 10% moderately agreed) that their organization requires the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate. Nine percent neither agreed nor disagreed / neutral and only 5% disagreed. The majority of the organizations surveyed were found to require the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate.

Smith et al.'s (1996) statements that comprise the "Collection" subscale were "A. It usually bothers me when companies ask me for personal information. E. When companies ask me for personal information, I sometimes think twice before providing it. J. It bothers me to give personal information to so many companies. and O. I'm concerned that companies are collecting too much personal information about me." The following two statements were included on the survey related to Limiting Collection:

Principle 4 - Limiting Collection

5). PP_MINIM: My organization limits the collection of personal information to that which is necessary for the purposes identified by the organization.

Eighty-four percent agreed (45% strongly agreed, 28% agreed, 11% moderately agreed) that their organization limits the collection of personal information to that which is

necessary for the purposes identified by the organization. Nine percent neither agreed nor disagreed / neutral and only 7% disagreed.

6). PP_FAIR: My organization collects information by fair and lawful means. Ninety-two percent agreed (62% strongly agreed, 25% agreed, 5% moderately agreed) that their organization collects information by fair and lawful means. Five percent neither agreed nor disagreed / neutral and only 4% disagreed. The majority of the organizations surveyed were found to limit the collection of personal information and collect information by fair and lawful means.

Smith et al.'s (1996) statements regarding "Unauthorized Secondary Use" subscale included "C. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information. G. When people give personal information to a company for some reason, the company should never use the information for any other reason. K. Companies should never sell the personal information in their computer databases to other companies. and M. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information." The statements I included on my survey related to unauthorized secondary use are as follows:

Principle 5 - Limiting Use, Disclosure, and Retention

7). PP_DISCL: My organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the

individual or as required by law.

Ninety percent agreed (64% strongly agreed, 21% agreed, 5% moderately agreed) that their organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Six percent neither agreed nor disagreed / neutral and only 4% disagreed.

8). PP_RETEN: My organization retains personal information only as long as necessary for the fulfillment of the purposes, which it was collected, except with the consent of the individual or as required by law.

Eighty-seven percent agreed (54% strongly agreed, 25% agreed, 8% moderately agreed) that their organization collects information by fair and lawful means. Seven percent neither agreed nor disagreed / neutral and only 6% disagreed. The majority of the organizations surveyed were found to not use or disclose personal information for purposes other than those for which it was collected, and retain personal information only as long as necessary for the fulfillment of the purposes which it was collected, except with the consent of the individual or as required by law.

Smith et al.'s (1996) statements regarding “Accuracy” subscale were “B. All the personal information in computer databases should be double-checked for accuracy - no matter how much this costs. F. Companies should take more steps to make sure that the personal

information in their files is accurate. L. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases."

Malhotra, Kim, and Agarwal's (2004) adapted Smith et al.'s (1996) privacy scale to an online environment called the *Internet Users' Information Privacy Concerns (IUIPC)* scale. Their statements related to accuracy which they categorized under errors are "(2) Online companies should take more steps to make sure that the personal information in their files is accurate. (3) Online companies should have better procedures to correct errors in personal information. (4) Online companies should devote more time and effort to verifying the accuracy of the personal information in their databases."

The statements I included on my instrument related to accuracy are as follows:

Principle 6 - Accuracy

9). PP_ACCUR: My organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Ninety-one percent agreed (51% strongly agreed, 29% agreed, 11% moderately agreed) that their organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Four percent neither agreed nor disagreed / neutral and only 5% disagreed.

14). PP_CORR: An individual is able to challenge the accuracy and completeness of the information and have it amended as appropriate in my organization.

Eighty-four percent agreed (41% strongly agreed, 30% agreed, 13% moderately agreed) that their organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Eleven percent neither agreed nor disagreed / neutral and only 6% disagreed.

116). PC_ACCME: I worry about the accuracy of computerized information about me.

Sixty-six percent agreed (17% strongly agreed, 20% agreed, 29% moderately agreed) that they worry about the accuracy of computerized information about them. Twenty percent neither agreed nor disagreed / neutral and 14% disagreed.

123). BH_PROC: I look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved.

Fifty-four percent agreed (17% strongly agreed, 18% agreed, 19% moderately agreed) that they look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved. Nearly a third, 32%, neither agreed nor disagreed / neutral and 14% disagreed. While the majority of the organizations surveyed were found to ensure the accuracy and completeness of personal information and have it amended the majority of participants still worry about the accuracy of computerized information about them but most do not see what practical procedures for accuracy, challenge and correction of errors

the business organization or government agency follows when consumer or citizen evaluations are involved.

In the privacy classification made in the Westin privacy segmentation Privacy Fundamentalists are “worried about the accuracy of computerized information and additional uses made of it” I separated “worried about the accuracy of computerized information and additional uses made of it” into two survey questions described in the privacy classification section.

Smith et al.'s (1996) statements regarding “Improper Access” subscale were “D. Companies should devote more time and effort to preventing unauthorized access to personal information. I. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs. and N. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers” (p. 170).

My survey statement was related to safeguarding personal information to help prevent improper access.

Principle 7 - Safeguards

10). PP_SECUR: My organization protects personal information by security safeguards appropriate to the sensitivity of the information.

Eighty-nine percent agreed (53% strongly agreed, 27% agreed, 9% moderately agreed) that their organization protects personal information by security safeguards appropriate to

the sensitivity of the information. Six percent neither agreed nor disagreed / neutral and 5% disagreed. The majority of the organizations surveyed were found to protect personal information by security safeguards appropriate to the sensitivity of the information.

Principle 8 - Openness

11). PP_POLIC: My organization makes specific information about its policies and practices relating to the management of personal information readily available to individuals.

Eighty-five percent agreed (46% strongly agreed, 27% agreed, 12% moderately agreed) that their organization makes specific information about its policies and practices relating to the management of personal information readily available to individuals. Ten percent neither agreed nor disagreed / neutral and 5% disagreed. The majority of the organizations surveyed were found to make specific information about its policies and practices relating to the management of personal information readily available to individuals.

Principle 9 - Individual Access

12). PP_AWARE: My organization informs an individual of the existence, use, and disclosure of his or her personal information.

Eighty-five percent agreed (42% strongly agreed, 31% agreed, 12% moderately agreed) that their organization informs an individual of the existence, use, and disclosure of his or

her personal information. Ten percent neither agreed nor disagreed / neutral and 5% disagreed.

13). PP_ACCES: My organization gives an individual access to his or her personal information upon request.

Eighty-three percent agreed (48% strongly agreed, 26% agreed, 9% moderately agreed) that their organization gives an individual access to his or her personal information upon request. Ten percent neither agreed nor disagreed / neutral and 7% disagreed.

14). PP_CORR: An individual is able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Eighty-four percent agreed (41% strongly agreed, 30% agreed, 13% moderately agreed) that their organization is able to challenge the accuracy and completeness of the information and have it amended as appropriate. Eleven percent neither agreed nor disagreed / neutral and 5% disagreed. The majority of the organizations surveyed were found to inform individuals of the existence, use, disclosure and provide access to their personal information upon request; challenge the accuracy and completeness of the information; and have it amended as appropriate.

Principle 10 - Challenging Compliance

15). PP_CHALL: My organization allows an individual to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization’s compliance.

Eighty-four percent agreed (39% strongly agreed, 29% agreed, 13% moderately agreed) that their organization allows an individual to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization's compliance. Fourteen percent neither agreed nor disagreed / neutral and 6% disagreed. The majority of the organizations surveyed were found to allow an individual to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization's compliance.

Due to the length of the survey rather than going through each section with the percentage of results in a summary table, *Privacy Management Survey* Results, is provided in Appendix E. A few highlights will be explained in the next sections.

Privacy Practices

Most organizations were found to have privacy practices in place for collection, use, disclosure and retention of personal information. Eighty-nine percent agreed that their organization is responsible for personal information under its control. Eighty percent have designated an individual or individuals who are accountable for the organization's compliance with the privacy principles (fair information principles - FIPs). The majority of the organizations surveyed were found to be accountable for privacy.

Eighty-eight percent of organizations identify the purposes for which personal information is collected at or before the time the information is collected. Eighty-five

percent require the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate. Eighty-four percent limits the collection of personal information to that which is necessary for the purposes identified by the organization. Ninety-two percent collects information by fair and lawful means. The majority of the organizations surveyed collected personal information with consent but it was found that 67% were concerned that their personal information is used without permission.

Ninety percent agreed that their organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Eighty-seven percent agreed that their organization retains personal information only as long as necessary for the fulfillment of the purposes which it was collected, except with the consent of the individual or as required by law. Although the majority of the organizations surveyed were found to properly use, disclose and retain personal information, it was found that 68% are concerned that their personal information is accessed without permission and 72% worry about additional uses made of their computerized information.

Accuracy of personal information rated high by organizations but is a concern for participants. Ninety-one percent ensures that their organization's personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Eighty-four percent agreed that an individual is able to challenge the accuracy and

completeness of the information and have it amended as appropriate in my organization. Although the majority of the organizations surveyed were found to ensure the accuracy of their personal information, it was found that 66% of participants worry about the accuracy of computerized information about them but only 54% look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved.

Security is necessary to keep personal information protected. Eighty-nine percent agreed that their organization protects personal information by security safeguards appropriate to the sensitivity of the information. Eighty-five percent agreed that their organization makes specific information about its policies and practices relating to the management of personal information readily available to individuals.

The majority of the organizations inform individuals, provide access to their personal information upon request, allow them to challenge the accuracy and completeness of their information and have it amended as appropriate. Eighty-five percent inform an individual of the existence, use, and disclosure of his or her personal information. Eighty-three percent agreed that their organization gives an individual access to his or her personal information upon request. Eighty-one percent of organizations allowed an individual to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization's compliance.

Brand Protection (BP)

The brand protection scale is a new contribution that I make to the literature. During the early stages of my research, brand protection that included protecting personal data was a new concept. There were no existing brand protection scales available in the academic literature. Through a practitioner literature review, a company was found that did brand protection services focusing on digital brand abuse. My scale was developed based on the harm that may result from malicious behaviour to personal information, digital brand abuse, brand abuse on social media sites, defacement of the organization's website and identity theft. My brand protection scale also includes intellectual property abuse, abuse of its domain name, web traffic diversions and online trademark infringements. Survey statements are included to determine what an organization has in place to help protect its brand. Investigation into privacy training, privacy policies, programs, management models, methodologies, privacy impact assessments (PIAs) and audits, personal information storage and privacy safeguards, all as brand protection mechanisms, are included in the various sections of the survey.

Privacy Training (TR) for Brand Protection

It is necessary for an organization to have privacy policies and practices in place but for these policies and practices to be put into action it is important to train the employees, partners and stakeholders. The next eight questions on the survey are related to privacy training, education, contracts and communication. The questions ask who gets training

and how often. If the training covers Acts, policies and practices and if it is extended to partners and stakeholders. The privacy training statements have been arranged according to the ones that participants strongly agreed (SA) with the most to the least (see Table 3.1). Seventy-nine percent agreed (48.9% strongly agreed, 19.4% agreed, 10.8% moderately agreed) that their privacy training covers the policies and practices established by the organization. Thirteen point three percent neither agreed nor disagreed / neutral and 7.6% disagreed.

16). BP_TR_RE: My organization requires all employees who access personal information to take privacy training.

17). BP_TR_FR: My organization provides mandatory training on personal privacy protection at least every two years.

18). BP_TR_PA: My organization trains employees about the federal *Privacy Act (PA).*

19). BP_TR_HI: My organization trains employees about the *Health Insurance Portability and Accountability Act (HIPAA).*

20). BP_TR_PP: My organization's privacy training covers the policies and practices established by the organization.

21). BP_TR_CL: My organization educates clients to help manage the risk of client loss resulting from corporate identity theft.

22). BP_TR_PR: My organization extends training on personal privacy protection to partners.

23). BP_TR_AS: My organization extends privacy training to all stakeholders (i.e. employees, clients).

24). BP_LC3: Contracts with 3rd party service providers include protection of personal information.

25). BP_CO_ST: My organization provides communication to stakeholders and users regarding data privacy awareness.

Regarding training as a brand protection program, the deployment of the survey found that 73% of the organizations require all employees who access personal information to take privacy training. Only 63% provide mandatory training on personal privacy protection at least every two years. Sixty-seven percent train their employees about the Privacy Act (PA) and 65% train their employees about the Health Insurance Portability and Accountability Act (HIPAA). Seventy-nine percent of the privacy training covers the policies and practices established by the organization. The survey found that 60% educate clients to help manage the risk of client loss resulting from corporate identity theft. Only 54% extend training on personal privacy protection to partners and 52% extend privacy training to all stakeholders (i.e. employees, clients). It was discovered that 62% that have contracts with 3rd party service providers include protection of personal information. Sixty-one percent provide communication to stakeholders and users regarding data privacy awareness.

Table 3.1

Privacy Training Statements Participants Strongly Agreed with the Most to the Least

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
20	My organization's privacy training covers the policies and practices established by the organization.	3.5%	1.9%	2.2%	13.3%	10.8%	19.4%	48.9%	79%
16	My organization requires all employees who access personal information to take privacy training.	6.3%	3.5%	5.1%	11.7%	8.6%	18.1%	46.7%	73%
18	My organization trains employees about the Privacy Act (PA).	7.0%	5.1%	5.4%	15.6%	9.2%	16.2%	41.6%	67%
17	My organization provides mandatory training on personal privacy protection at least every two years.	7.3%	6.3%	6.7%	16.2%	8.3%	13.7%	41.6%	63%
19	My organization trains employees about the Health Insurance Portability and Accountability Act (HIPAA).	8.9%	5.4%	4.8%	15.9%	9.8%	16.2%	39.0%	65%
24	Contracts with 3rd party service providers include protection of personal information.	7.0%	3.2%	5.7%	21.9%	10.8%	19.0%	32.4%	62%
25	My organization provides communication to stakeholders and users regarding data privacy awareness.	5.4%	6.0%	4.8%	22.9%	14.0%	19.4%	27.6%	61%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
21	My organization educates clients to help manage the risk of client loss resulting from corporate identity theft.	6.3%	7.3%	4.4%	21.9%	14.0%	19.4%	26.7%	60%
23	My organization extends privacy training to all stakeholders (i.e. employees, clients).	8.6%	7.0%	7.0%	25.4%	9.5%	17.1%	25.4%	52%

Privacy Policies, Programs, Management Models, Methodologies, Privacy Impact Assessments and Audits for Brand Protection

The next section of questions on the survey determines what organizations have in place to help protect their brand. It quantifies the percentage of organizations surveyed that have a privacy policy, a policy to deal with a data breach and alignment of privacy policies with privacy practices. It reveals if the organization has best practices use for privacy, a privacy program to deal with credit card fraud and digital brand abuse. The survey questions whether the organization uses privacy management models and methodologies. It informs us if the organization is conducting privacy impact assessments (PIAs) and privacy audits.

26). BP_H_PP: My organization has a privacy policy.

27). BP_H_DBP: My organization has a policy in place so employees know what to do if there is a data breach.

28). BP_H_ALN: Management provides alignment of privacy policies with privacy practices.

29). BP_H_BP: My organization has best practices use for privacy.

30). BP_H_PPR: My organization has a privacy program.

31). BP_H_MOD: My organization uses privacy management models.

32). BP_FRAUD: My organization has a privacy program to prevent credit card fraud.

33). BP_ABUSE: My organization has a privacy program to prevent digital brand abuse.

34). BP_H_PM: My organization uses privacy methodologies.

35). BP_PIAS: My organization conducts privacy impact assessments (PIAs).

36). BP_AUDIT: My organization conducts privacy audits.

Personal Information Storage and Privacy Safeguards

With the rapid change in technology and mobility of data it is important that personal information is being stored securely whether it is being used at a public hotspot, for

conducting e-business or being saved in the cloud. The following group of survey questions deals with storage of personal information and proper protection i.e. using encryption or software intrusion programs.

37). BP_MCRYP: My organization stores personal information on mobile devices such as laptops, tablets and jump drives *with* encryption.

38). BP_NCRYP: My organization stores personal information on mobile devices such as laptops, tablets and jump drives *without* encryption.

39). BP_ENCRY: My organization uses encryption when storing data.

40). ORG_E_BUS: My organization conducts e-business.

41). BP_SSL: My organization uses Secure Socket Layer (SSL) to encrypt sensitive information that is transmitted over the Internet during e-commerce transactions.

42). BP_DETEC: My organization uses software to detect intruders.

43). ORG_CLOU: My organization stores personal information in the cloud.

44). ORG_INTL: My organization stores personal information in other countries.

45). BP_SECUR: My organization has the security necessary to ensure the ongoing protection of personal information.

46). BP_PPOL: My organization has policies in place to protect personal information.

47). BP_COMPL: My organization ensures that policies to protect personal information are put into practice each and every day.

48). BP_AUD_P: My organization periodically examines portable storage devices to ensure they are being used solely for legitimate reasons.

49). BP_RECOR: My organization reviews holdings, disposes of transitory records and classifies remaining records at the appropriate security level.

Organizations were asked about their privacy programs, policies for privacy and data breaches and alignment with their practices. Eighty-nine percent of the organizations have a privacy policy and 71% have a policy in place so employees know what to do if there is a data breach. Participants thought that 76% of their organizations provide alignment of privacy policies with privacy practices and that 78% of the organizations have best practices use for privacy. Seventy-six percent have a privacy program while 57% use privacy management models. It was found that 60% have a privacy program to prevent credit card fraud and 56% have a privacy program to prevent digital brand abuse. Sixty-three percent of the organizations use privacy methodologies. Privacy impact assessments (PIAs) are conducted 49% and 56% conduct privacy audits.

Encryption is one method to prevent personal information from being accessed if it is stolen. It was discovered that 62% store personal information on mobile devices such as laptops, tablets and jump drives with encryption and 36% store it without encryption. Seventy-two percent use encryption when storing data and 55% use Secure Socket Layer (SSL) to encrypt sensitive information that is transmitted over the Internet during e-commerce transactions. Intruder detection software is used by 70% of organizations. Only 75% said that they have the security necessary to ensure the ongoing protection of personal information while 84% have policies in place to protect personal information and 79% ensure that policies to protect personal information are put into practice each and every day.

Portable storage devices are periodically examined by 55% to ensure they are being used solely for legitimate reasons while 42% restrict the use of portable storage devices. System software which blocks unauthorized use of portable storage devices on desktop computers is used by 49%. It was found that 64% review holdings, dispose of transitory records and classify remaining records at the appropriate security level.

Privacy Breaches (PB)

Even with safeguards in place a privacy breach may occur. The three main reasons for this are malicious or criminal attacks, employee negligence, or a system glitch.

The survey questions explore privacy breaches in depth. They determine if the organization has experienced a data privacy breach and if so the reason for the breach. It investigates whether there is an incident response plan in place and someone appointed to lead this. It looks at data breach reporting and customer relationships. The effect of a data breach on the organization's brand to lose value is considered. The survey determined whether clients' credit or debit cards were compromised and if this involved the inconvenience of cancelling cards. Safeguards such as passwords and the changing of clients' passwords as a result of a data breach are uncovered. Unauthorized attempts to access personal information are revealed. With more mobile devices being used than ever before there is a greater risk of personal information being lost or stolen with the device. This is explored along with the use of encryption and the restriction of portable storage devices. The privacy breach questions on the survey are provided below.

50). PB_YES: My organization has experienced a data privacy breach.

51). PB_ATTAC: My organization had a data breach because of malicious or criminal attacks.

52). PB_EMPLO: My organization had a data breach because of employee negligence.

53). PB_GLITC: My organization had a data breach because of system glitches.

54). PB_INCID: My organization has a formal incident response plan in place to address data breaches.

55). PB_LEAD: My organization has appointed an individual to lead the data breach incident response team.

56). PB_NOREP: My organization does not report instances of a data privacy breach to authorities.

57). PB_REPY: My organization has reported instances of a data privacy breach to authorities.

58). PB_CTERM: My organization had customers terminate their relationship with the company because of a data breach.

59). PB_LOSBV: A data privacy breach has caused my organization's brand to lose value.

60). PB_CC: My organization has had clients' credit card information compromised.

61). PB_DEBIT: My organization has had clients' debit card information compromised.

62). PB_CANCL: Clients of my organization have faced the inconvenience of cancelling cards.

63). BP_PWORD: My organization requires staff and/or clients to regularly change their passwords.

64). H_PWORD: Clients of my organization have expressed inconvenience related to changing passwords as a result of a data privacy breach.

65). PB_ATTCK: My organization has had unauthorized attempts to access personal information.

66). PB_MOBIL: My organization has had a mobile device (i.e. laptop) lost or stolen that contained unencrypted personal information.

67). PB_MSTOL: My organization has had a mobile device (i.e. laptop) lost or stolen that contained encrypted personal information.

68). BP_PORTA: My organization restricts the use of portable storage devices.

69). BP_BLKPO: My organization uses system software which blocks unauthorized use of portable storage devices on desktop computers.

Nineteen percent of organizations have experienced a privacy breach although this percentage could be higher because 17% neither agreed nor disagreed. It was interesting that almost an equal amount, 13%-14%, of privacy breaches were caused by malicious or criminal attacks, employee negligence or because of system glitches. Almost half of the

organizations have a formal incident response plan in place to address data breaches (although it is surprising that 22% did not know). Forty-five percent of organizations have appointed an individual to lead the data breach incident response team. Nine percent admitted that their organization does not report instances of a data privacy breach to authorities while 22% have reported instances of a data privacy breach to authorities. Twelve percent of organizations have had customers terminate their relationship with the company because of a data breach. Out of the 19% who experienced a data privacy breach it has caused 9% of the organization's brand to lose value. This percent may be higher because 18% did not agree or disagree with the statement. See Table 3.2 for a detailed breakdown of the percentages of an excerpt of privacy breaches from the survey. For complete survey results please refer to Appendix E.

Table 3.2

Sample of Privacy Breach Results from Privacy Management Survey

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
50	My organization has experienced a data privacy breach.	33%	23%	7%	17%	6%	5%	8%	19%
51	My organization had a data breach because of malicious or criminal attacks.	38%	24%	9%	15%	3%	3%	7%	13%
52	My organization had a data breach because of employee negligence.	38%	24%	7%	17%	5%	4%	5%	14%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
53	My organization had a data breach because of system glitches.	37%	23%	6%	20%	5%	3%	5%	13%
54	My organization has a formal incident response plan in place to address data breaches.	14%	10%	5%	22%	14%	13 %	22 %	48%
55	My organization has appointed an individual to lead the data breach incident response team.	13%	9%	6%	27%	13%	14 %	18 %	45%
56	My organization does not report instances of a data privacy breach to authorities.	38%	17%	10%	27%	1%	4%	4%	9%
57	My organization has reported instances of a data privacy breach to authorities.	21%	13%	6%	37%	3%	7%	11 %	22%
58	My organization had customers terminate their relationship with the company because of a data breach.	44%	15%	6%	22%	4%	3%	5%	12%
59	A data privacy breach has caused my organization's brand to lose value.	45%	19%	8%	18%	3%	3%	3%	9%

Experienced Harms (H)

The harm that could be caused by a privacy data breach was examined to see if the organization experienced a loss of time, productivity, litigation costs, direct financial costs, damaged brand value or loss of customer trust. If the organization is service-oriented that depends on information a data breach could even affect public safety. A data breach can cause an organization to lose revenue or intellectual property. Fraudulent emails to clients from spammers can harm an organization's brand. A breach of client privacy may impact an organization's financial position or decrease its market valuation or brand value. By preventing a data breach from occurring by protecting privacy and security it may avoid harm to the organization and lead to a competitive advantage for an organization. The statements included on the survey for harm from brand abuse are as follows:

70). H_DBATK: My organization's database of personal information has been changed maliciously.

71). H_STROY: Personal information held by my organization has been maliciously destroyed.

72). H_ABUSE: My organization has experienced digital brand abuse.

73). H_SMABU: My organization has had its brand abused on social media sites.

74). H_WEBDF: My organization has experienced defacement of its site's website.

75). H_IDTHF: My organization has experienced identity theft.

76). H_IPABU: My organization has experienced intellectual property abuse.

77). H_DNABU: My organization has experienced abuse of its domain name.

78). H_TRAFF: My organization has experienced web traffic diversions.

79). H_TM: My organization has experienced online trademark infringements.

80). H_PH: My organization has experienced the use of its brand in phishing attacks.

81). ORG_SOA: My organization is a service-oriented business that depends on information (e.g. airline schedules or stock quotes).

82). H_HACK: My organization has experienced instances of hacking.

83). H_TIME: A data breach has caused my organization to experience a loss of time.

84). H_PRODUC: A data breach has caused my organization to experience a loss of productivity.

85). H_COSTS: My organization has experienced litigation costs because of a data breach.

86). H_FINANL: My organization has experienced direct financial costs because of a data breach.

87). H_BRVAL: My organization has experienced damaged brand value because of a data breach.

88). H_CUSTRS: My organization has experienced loss of customer trust because of a data breach.

89). H_PS: A data breach has caused my organization to affect public safety.

90). H_REVNUE: My organization has experienced lost revenue because of a data breach.

91). H_LOSEIP: A data breach has caused my organization to experience a loss of intellectual property.

92). H_SPAM: Spammers have abused my organization's brand by distributing fraudulent emails to clients.

Risk Resulting from a Privacy Breach (R)

The next statements gather participants' opinions as to the result which may occur from a breach of client privacy. Some of the risks could impact the organization's financial position, market value, brand value, and litigation costs. On the other hand, if privacy and security are protected it may lead to a competitive advantage for an organization.

93). R_FINPOS: A breach of client privacy may have a severe impact on an organization's financial position.

94). R_MKTVAL: A breach of client privacy may result in a decreased market valuation.

95). R_BRNVAL: A breach of client privacy may result in lost brand value.

96). R_LEGCOS: A breach of client privacy may result in costs for litigation.

97). R_COMADV: Protecting privacy and security may lead to a competitive advantage for my organization.

Segments of Internet Users (IU)

The three segments of internet users according to Hann, Hui, Lee & Png (2007) are: Privacy Guardians, Information Sellers and Convenience Seekers. Privacy Guardians make up the majority of subjects who are relatively sensitive to online information privacy concerns. Information Sellers are a smaller proportion who are relatively willing to provide personal information in exchange for money. Convenience Seekers are an even smaller proportion who are relatively willing to provide personal information in exchange for convenience. To determine the segment of Internet users (IU) completing the survey the statements adapted on the survey are:

98). IU_SENSI: I am sensitive to online information privacy concerns.

99). IU_XMONY: I am willing to provide personal information in exchange for money.

100). IU_XCONV: I am willing to provide personal information in exchange for convenience.

In survey 2 it was found that the majority 78% (10% were neutral) of the participants would be considered Privacy Guardians. This agrees with Hann et. al. (2007) but only 14% were information sellers and more, 17% were convenience seekers (see Table 3.3).

Table 3.3

Privacy Guardians, Information Sellers, and Convenience Seekers

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
98	I am sensitive to online information.	7%	3%	2%	10%	19%	25%	34%	78%
99	I am willing to provide my personal information in exchange for money.	46%	14%	7%	19%	6%	3%	4%	14%
100	I am willing to provide my personal information in exchange for convenience.	37%	14%	8%	24%	8%	5%	4%	17%

Belief (BF)

Six statements were included to gather participants' feelings and beliefs about privacy training, practices, policies, brand, breaches, consumer confidence and brand value. Although participants may not have experienced some or all of these they may still have an opinion.

101). BF_GAPS: I feel there are gaps between privacy practices and privacy training in my organization.

102). BF_GAPPP: I feel that privacy policies and privacy practices in my organization are not aligned.

103). BF_PRITR: I believe that privacy training helps to protect my organization’s brand.

104). BF_DMGBR: I believe that a privacy breach would damage my organization's brand.

105). BF_LOSCC: I believe that privacy breaches may result in substantial loss of consumer confidence.

106). BF_LBVAL: I believe that privacy breaches may result in loss of value of my organization's brand.

Privacy Behavior

To determine the privacy behavior of participants completing the survey two statements were adapted from the general caution privacy behavior scale (Buchanan, Paine, Joinson, & Reips, 2007): Do you read a website's privacy policy before you register your information? Do you read license agreements fully before you agree to them?

107). BH_READ: I read license agreements fully before I agree to them.

108). BH_READW: I read a website's privacy policy before I register my information.

Privacy Aware (PA)

Statements were included to see how engaged participants are in social networking and how aware they are of privacy issues such as privacy settings and privacy breaches and notifications.

109). PA_SN: I am engaged in social networking over the Internet.

110). PA_PRSET: I use the privacy settings in social networking over the Internet.

111). PA_GOV: I am aware that Employment and Social Development Canada has a hard drive missing that contained the Social Insurance number, name, date of birth, home address, telephone number, loan amounts and balances for more than half a million student loan recipients from 2000 to 2006.

112). PA_TJMAX: I am aware of the privacy breach in 2007 at the parent company of TJ Maxx that affected 90 million records.

113). PA_THEFT: I am aware that my organization experienced hackers' theft of information on many customers.

114). BF_NOTIF: I believe that we need a system that requires people to be notified when their personal data has been breached.

Privacy Classification

The Westin privacy segmentation has classified people into three categories: the *Fundamentalists*, the *Pragmatists* and the *Unconcerned* (Harris et al., 1998). The Privacy Fundamentalists are generally distrustful of organizations that ask for their personal information; worried about the accuracy of computerized information and additional uses made of it; in favour of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies and generally choose privacy controls over consumer-service benefits when these compete with each other. The questions are codes as PC-privacy concerns, BF-beliefs, and BH-behaviours.

115). PC_DISTR: I am generally distrustful of organizations that ask for my personal information.

116). PC_ACCME: I worry about the accuracy of computerized information about me.

117). PC_ADUSE: I worry about additional uses made of computerized information about me.

118). BF_LAWS: I am in favour of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies.

The Unconcerned are generally trustful of organizations collecting their personal information; comfortable with existing organizational procedures and uses; are ready to forego privacy claims to secure consumer-service benefits or public-order values and are not in favour of the enactment of new privacy laws or regulations.

119). BF_TRUST: I am generally trustful of organizations collecting their personal information.

120). BF_COMPP: I am comfortable with my organization's existing privacy practices.

121). BF_NOLAWS: I am not in favour of the enactment of new privacy laws or regulations.

I omitted "are ready to forego privacy claims to secure consumer-service benefits or public-order values" in my survey.

The statements "worried about the accuracy of computerized information and additional uses made of it" were separated into two survey questions and I omitted

"generally choose privacy controls over consumer-service benefits when these compete with each other" in my survey.

The Pragmatists weigh the benefits to them of various consumer opportunities and services before providing my personal information; protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved; look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved; believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it; where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists.

122). BH_BENF: I weigh the benefits to them of various consumer opportunities and services before providing my personal information.

123). BH_PROC: I look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved.

124). BF_EARNT: I believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it.

125). BH_OUT: Where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists.

I omitted "protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved" in my survey.

Privacy Concerns

Two open-ended qualitative questions were asked as a longitudinal study to Survey 1. The two questions asked about privacy concerns of their personal information and network traffic. The results of the qualitative data collected are discussed in Chapter 4.

126). PC_PRPI: What concerns do you have about the privacy of your personal information?

127). PC_NETTR: What concerns do you have about network traffic privacy?

Milne, Rohm and Bahl (2004, p.226) found that the "level of privacy concerns was a strong predictor of online privacy and identity protection behaviors such as falsifying information, refusing information disclosure or transactions, or removing personal information from lists." These were made into three privacy concern statements on the survey.

128). PC_FALSE: If I have concerns for online privacy I use protection behaviors such as falsifying information.

129). PC_REFUS: If I have concerns for online privacy I use protection behaviors such as refusing information disclosure or transactions.

130). PC_REMPI: If I have concerns for online privacy I use protection behaviors such as removing personal information from lists.

If participants refrain from disclosing their personal information when they have concerns for their privacy online a statement was included to determine if they use their personal information when they are not concerned.

131). PC_USEPI: If I do not have concerns for online privacy I use my personal information.

To determine if privacy-enhancing technologies are used when participants are concerned about their online privacy the following statement was included.

132). PC_PETS: If I have concerns for online privacy I adopt privacy-enhancing technologies.

Statements were adapted from Seounmi (2009) regarding refraining from using a website.

- I go to other Web sites that do not ask my personal information
- Usually, I do nothing and leave the Web site

133). PC_REFRA: If I have concerns for online privacy I refrain from interacting with a Web site.

With apps becoming popular on mobile devices two statements were included to determine if participants engage in mobile commerce and if they are concerned about this activity.

134). BH_MCOM: I engage in m-commerce (mobile commerce).

135). PC_MOBPR: I have concerns for mobile privacy.

Jensen, Potts, Jensen (2005) privacy attitude (concerns) scale includes the following statements. Concerns about identity theft and credit card fraud were also identified in the *Preliminary Privacy Concerns Survey* (McLeod & McLeod, 2011) and included as 7-point Likert scale statements on the survey.

- I am concerned about online identity theft.
- I am concerned about online credit card fraud.
- I am concerned about my privacy online.
- I am concerned about my privacy in everyday life.
- I am likely to read the privacy policy of a site I visit for the first time.

Statements 136 - 170 (see Table 3.4) were added to the survey based on the qualitative data collected in the study of privacy concerns in the *Preliminary Privacy Concerns Survey* (McLeod & McLeod, 2011).

Table 3.4

Privacy Concerns Added to Privacy Management Survey

Concern gathered from Preliminary Privacy Survey 1	**Concern added to Privacy Management Survey 2**
Increase number of mobile devices	136). PC_NOMOB: I am concerned about the increase number of mobile devices.
	137). PC_INVPI: I have personally been the victim of what I felt was an improper invasion of privacy of my personal information.
	138). ORG_IVPI: My organization has been the victim of an improper invasion of privacy of personal information.
Personal information accessed / Used without permission	139). PC_PIACC: I am concerned that my personal information is accessed without permission.
	140). PC_PIUSE: I am concerned that my personal information is used without permission.
Online banking / Financial risks, information seen or intercepted by a third party / theft	141). PC_ONBNK: I am concerned about online banking.
Online Credit cards / Online shopping	142). PC_ONCRC: I am concerned about online credit card transactions.
	143). PC_ONSHP: I am concerned about online shopping.
Seen or intercepted by a third party	144). PC_INFTH: I am concerned about information seen or intercepted by a third party.
Someone hijacking my system and performing illegal activities where my system is the only traceable element.	145). PC_HIJCK: I am concerned that someone may hijack my system and perform illegal activities where my system is the only traceable element.
Identity theft	146). PC_IDTHF: I am concerned about identity theft.
Privacy online is an Illusion; doesn't exist.	147). PC_PRILL: I am concerned that privacy online is an illusion; it does not exist.

Concern gathered from Preliminary Privacy Survey 1	Concern added to Privacy Management Survey 2
Lack of control	148). PC_LKCTR: I am concerned about the lack of privacy control online.
Emails	149). PC_EMAIL: I am concerned about the privacy of my email messages.
Photos	150). PC_PHOTO: I am concerned about the privacy of my photographs online.
Viruses / spyware / malware / EXE files / Multimedia files	151). PC_VIRUS: I am concerned about viruses / spyware / malware / EXE files / Multimedia files.
Deleted Facebook account	152). PC_FACBK: I am concerned about Facebook so I deleted my account.
Want protected would not put online	153). PC_NOTON: If I want my personal information protected I would not put it online.
People who have data don't care about its security.	154). PC_SECUR: I am concerned about people who have personal data do not care about its security.
No way to tell if secure.	155). PC_PISEC: I am concerned that there is no way to tell if personal data being stored is secure.
Data obtained and shared with others.	156). PC_SHARE: I am concerned that personal data obtained is shared with others.
Tracking purchase habits.	157). PC_PURCH: I am concerned about tracking purchase habits.
Privacy of passwords.	158). PC_PASWD: I am concerned about privacy of passwords.
Wireless access at home.	159). PC_WIRHM: I am concerned about the privacy of wireless access at home.
Wireless access at work.	160). PC_WIRWK: I am concerned about the privacy of wireless access at work.
Wireless access at public hot spots.	161). PC_WIRPB: I am concerned about the privacy of wireless access at public hot spots.
Protecting client's data.	162). PC_PROTC: I am concerned about protecting client's data.

Concern gathered from Preliminary Privacy Survey 1	Concern added to Privacy Management Survey 2
Export of data to jurisdictions with lax privacy laws.	163). PC_EXPOR: I am concerned about export of data to jurisdictions with lax privacy laws.
Information readily available / risks not communicated to public.	164). PC_PIAVL: I am concerned that personal information is readily available and that risks are not communicated to the public.
Lack of privacy / rights	165). PC_RIGHT: I am concerned about the lack of privacy rights.
Location tracking	166). PC_LOCAT: I am concerned about location tracking.
Bad guys / government	167). PC_GOVPI: I am concerned about the government having my personal information.
Network traffic leaking private data.	168). PC_NETTR: I am concerned that network traffic is leaking private data.
Online registration easily compromised.	169). PC_REGIS: I am concerned that online registration is easily compromised.
Hijack my account and ruin my reputation.	170). PC_REPUT: I am concerned that someone may hijack my account and ruin my reputation.

Brand Value Scale

Barnes and Mattsson's (2008) brand value scale (see Table 3.5) was used for the survey instrument. Their study is based on "Hartman's axiology and uses nine items for measuring the various aspects of brand value. In addition an overall item for assessing convergent validity is also included (question 10)" (Barnes & Mattsson, 2008: 199). "Dr. Hartman identified three dimensions of reality, which he called the Dimensions of Value. We value everything in one of these three ways or in a combination of these dimensions. The Dimensions of Value are Systemic, Extrinsic, and Intrinsic" (Axiology, 2001).

Table 3.5

Barnes & Mattsson's Brand Value Scale

Item No.	Question
1	I feel great pride identifying with Mazda.
2	What Mazda delivers feels right for me.
3	I feel I am able to trust Mazda completely.
4	Mazda does me good.
5	Mazda is a satisfying buy.
6	What I get from Mazda is worth the cost.
7	The uniqueness of Mazda stands out.
8	Mazda is a symbol of quality.
9	Information about Mazda is always correct.
10	Mazda is a good brand.

Note. "Brand value in Virtual Worlds: An axiological approach" by S. Barnes, and J. Mattsson, 2008, *Journal of Electronic Commerce Research, 9*(3), p. 206.

Barnes & Mattsson (2008) brand value scale was modified from Mazda for the participant's organization, Government, TJX Companies Inc. (Winners and Home Sense), and Bank of America on the *Privacy Management Survey*.

171). BV_ORG_P: I feel great pride identifying with my organization.

172). BV_ORG_R: What my organization delivers feels right for me.

173). BV_ORG_T: I feel I am able to trust my organization completely.

174). BV_ORG_G: My organization does me good.

175). BV_ORG_S: My organization is a satisfying buy.

176). BV_ORG_W: What I get from my organization is worth the cost.

177). BV_ORG_U: The uniqueness of my organization stands out.

178). BV_ORG_Q: My organization is a symbol of quality.

179). BV_ORG_C: Information about my organization is always correct.

180). BV_ORG_B: My organization is a good brand.

181). BV_GOV_P: I feel great pride identifying with my government.

182). BV_GOV_R: What my government delivers feels right for me.

183). BV_GOV_T: I feel I am able to trust my government completely.

184). BV_GOV_G: My government does me good.

185). BV_GOV_S: My government is a satisfying experience.

186). BV_GOV_W: What I get from my government is worth the cost.

187). BV_GOV_U: The uniqueness of my government stands out.

188). BV_GOV_Q: My government is a symbol of quality.

189). BV_GOV_C: Information about my government is always correct.

190). BV_GOV_B: My government is a good brand.

191). Repeated BV_GOV_P: I feel great pride identifying with my government.
It should have been BV_ TJX_P: I feel great pride identifying with TJX Companies Inc. (Winners and Home Sense).

192). BV_ TJX_R: What TJX Companies Inc. (Winners and Home Sense) delivers feels right for me.

193). BV_TJX_T: I feel I am able to trust TJX Companies Inc. (Winners and Home Sense) completely.

194). BV_TJX_G: TJX Companies Inc. (Winners and Home Sense) does me good.

195). BV_TJX_S: TJX Companies Inc. (Winners and Home Sense) is a satisfying buy.

196). BV_TJX_W: What I get from TJX Companies Inc. (Winners and Home Sense) is worth the cost.

197). BV_TJX_U: The uniqueness of TJX Companies Inc. (Winners and Home Sense) stands out.

198). BV_TJX_Q: TJX Companies Inc. (Winners and Home Sense) is a symbol of quality.

199). BV_TJX_C: Information about TJX Companies Inc. (Winners and Home Sense) is always correct.

200). BV_TJX_B: TJX Companies Inc. (Winners and Home Sense) is a good brand.

201). BV_BoA_P: I feel great pride identifying with Bank of America.

202). BV_BoA_R: What Bank of America delivers feels right for me.

203). BV_BoA_T: I feel I am able to trust Bank of America completely.

204). BV_BoA_G: Bank of America does me good.

205). BV_BoA_S: Bank of America is a satisfying buy.

206). BV_BoA_W: What I get from Bank of America is worth the cost.

207). BV_BoA_U: The uniqueness of Bank of America stands out.

208). BV_BoA_Q: Bank of America is a symbol of quality.

209). BV_BoA_C: Information about Bank of America is always correct.

210). BV_BoA_B: Bank of America is a good brand.

Participants (*N* = 315)

The percentage response details for the *demographic* information in the data set for survey 2, used in the thesis studies, are presented in this section in order to present a complete background to the studies and their results.

In my long survey (survey 2), all participants were from the United States. The gender of the survey participants included 73 males, which equals 23%, and 77% or 242 of the 315 participants were females (see Figure 3.1).

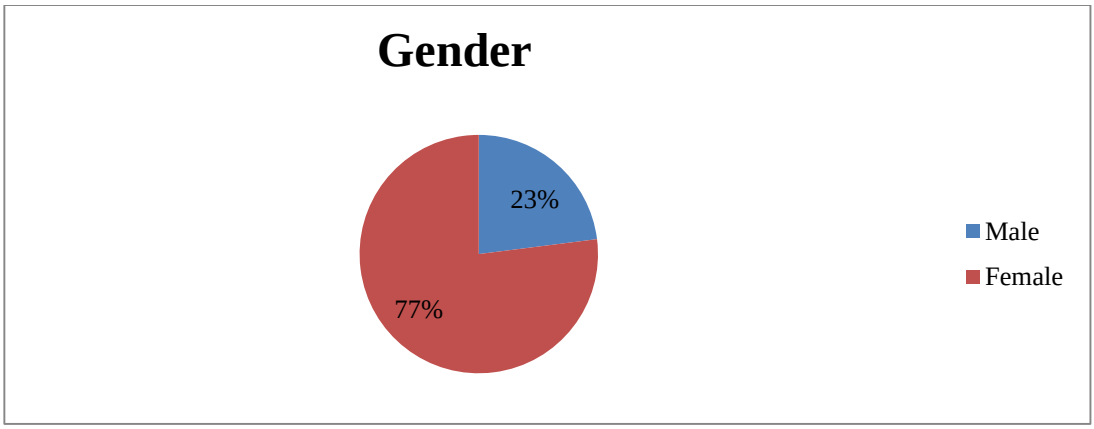


Figure 3.1. Gender of the Participants.

Forty-four percent of participants were between 25 to 34 years old. This was followed by 21% between the ages of 35 to 44 and 16% who were 45 to 54 years old (see Figure 3.2).

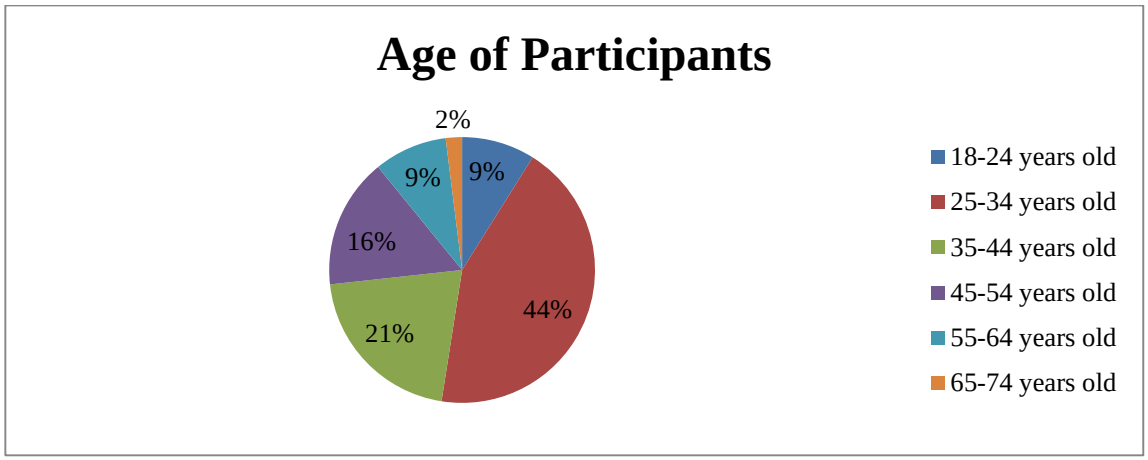


Figure 3.2. Age of the Participants.

The participants were well educated with 42% having a Bachelor's degree. This was followed by 17% having some college or university but no degree; 13% having an Associated degree; and 10% having a Master's degree and 10% having completed high school (see Figure 3.3).

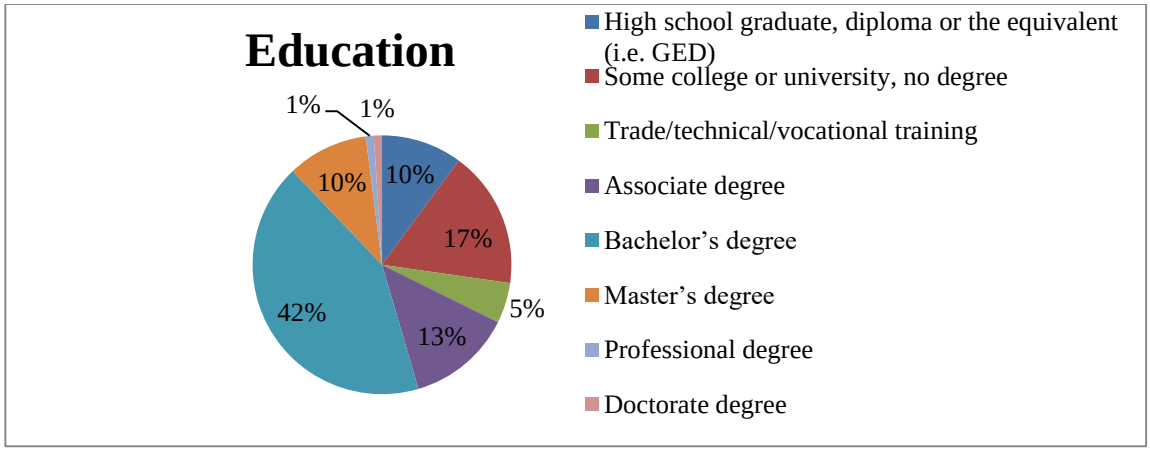


Figure 3.3. Education of the Participants.

In Figure 3.4 37% of the respondents were Clerical/Labour/Other Support. Middle Management accounted for 28%; Technical 16%; 11% Senior Management and 8% were Others. Other levels provided were: Artist, Assistant, Associate, Automotive, Business owner, Caregiver, Development operations, General staff, Graduate students, I don't have a level - I am the organization, Nurses, Owners, P.M., Sales associate, Sales coordinator, Supervisor, and Technician.

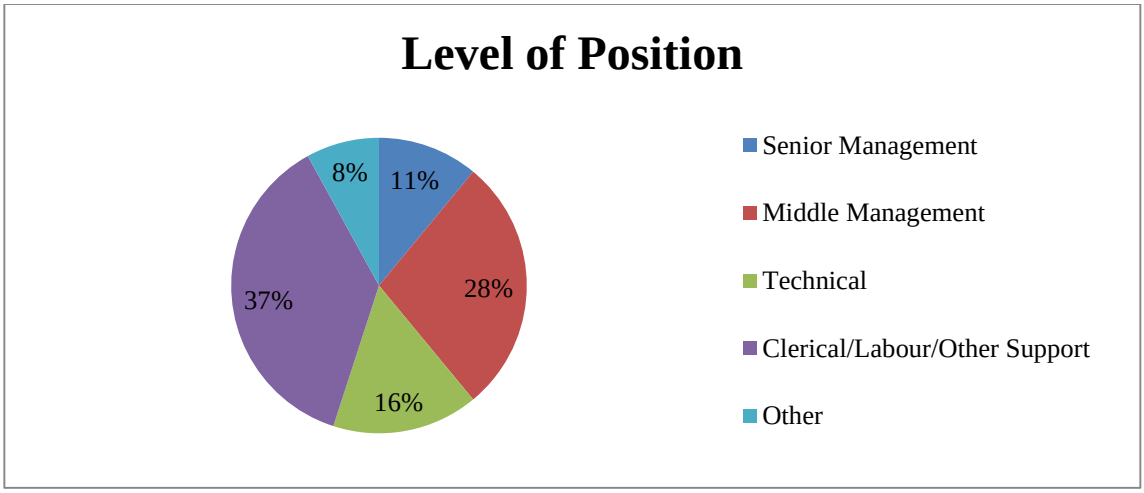


Figure 3.4. Level of Position.

Figure 3.5 displays the profession or occupation of the participants. A heterogeneous group of occupations resulted by not restricting the sample selection to a certain occupation. In Table 3.6 the 23% Other Professions or Occupations are provided. Twenty-one percent were Administrative support; 12% were Medical and 12% in Sales and marketing; 10% were in Information Technology; 4% were each in Financial, Human Resources and Professor / Teacher; 3% were in Arts and Entertainment; 2% Legal; and 1% were each in Engineering, Law Enforcement, Science, and Transport.

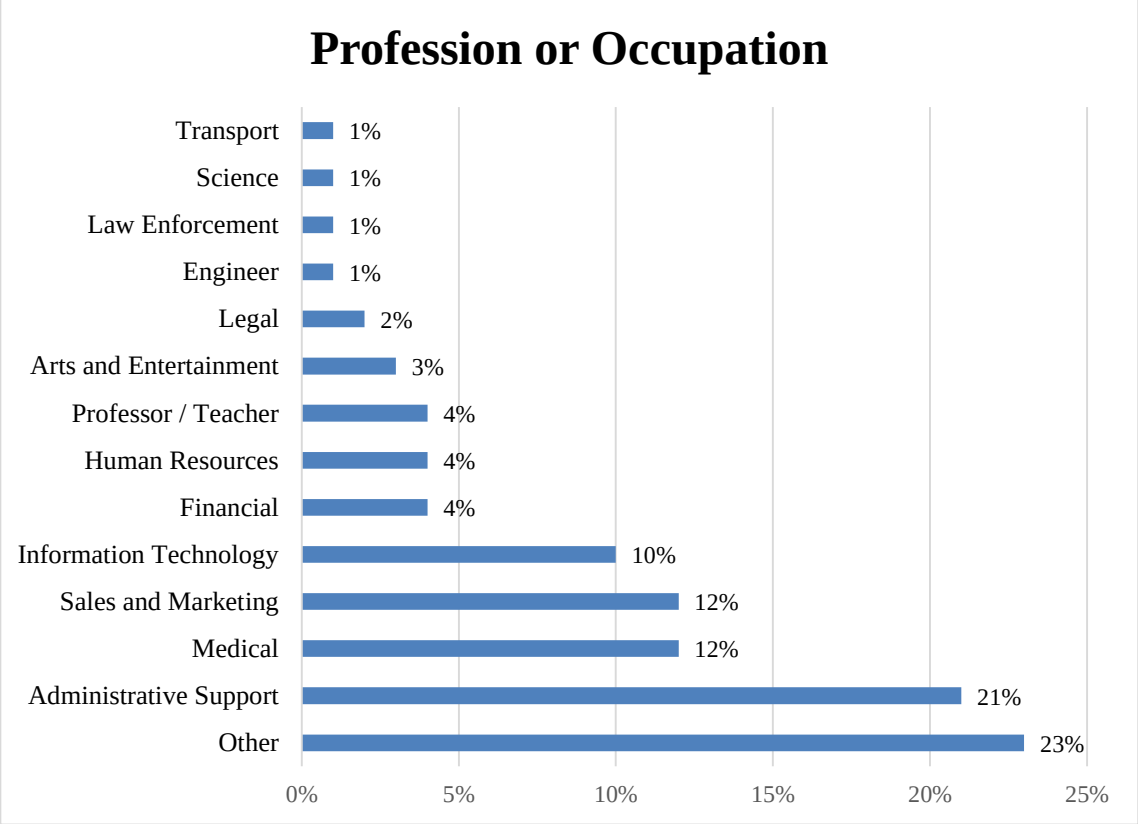


Figure 3.5. Profession or Occupation of the Participants.

There were a variety of professions represented by the sample. Some of these occupations included Retail; Insurance agents; Customer Service and Sales; Education; Automotive; Health Care Home Sector; Manufacturing; and Social Worker (see Table 3.6).

Table 3.6

Other Professions or Occupations of Participants

Accountant	Control valve	Inspector	Property Management
Agricultural	Cook	Insurance Agent (4)	Religious
Assistant	CPA	Landscaper	Repair Technician
Associate	Crafts	Logistics	Retail (5)
Automotive (2)	Customer Service & Sales (3)	Management	Secretary
Bail agent	Data Clerk	Manufacturing (2)	Service (2)
Billing	Daycare	Mechanical repairs	Small business owner
Business Development Specialist	Editor	Musician	Social Worker (2)
Business owner	Education (3)	Non-profit for special needs	Sports
Case manager	Food industry	Online retail	Technical Telecommunications
Child Care	Freelancer	Private after school program	Technician
Civil servant	General manager	Procurement	Utilities - Energy
Construction	Government, non-profit	Production	
Consumer Electronics Sales	Health care home sector (2)	Project Manager	

Ninety percent of the organizations represented had an online presence while only 56% had a mobile presence. Eighty-two percent provided products or services to the

general public of which 58% provided products or services online. Online purchases were made by 78% of the organizations. Sixty-nine percent provided products or services to public and other businesses / organizations while 29% provided products or services only to other businesses / organizations (see Figure 3.6).

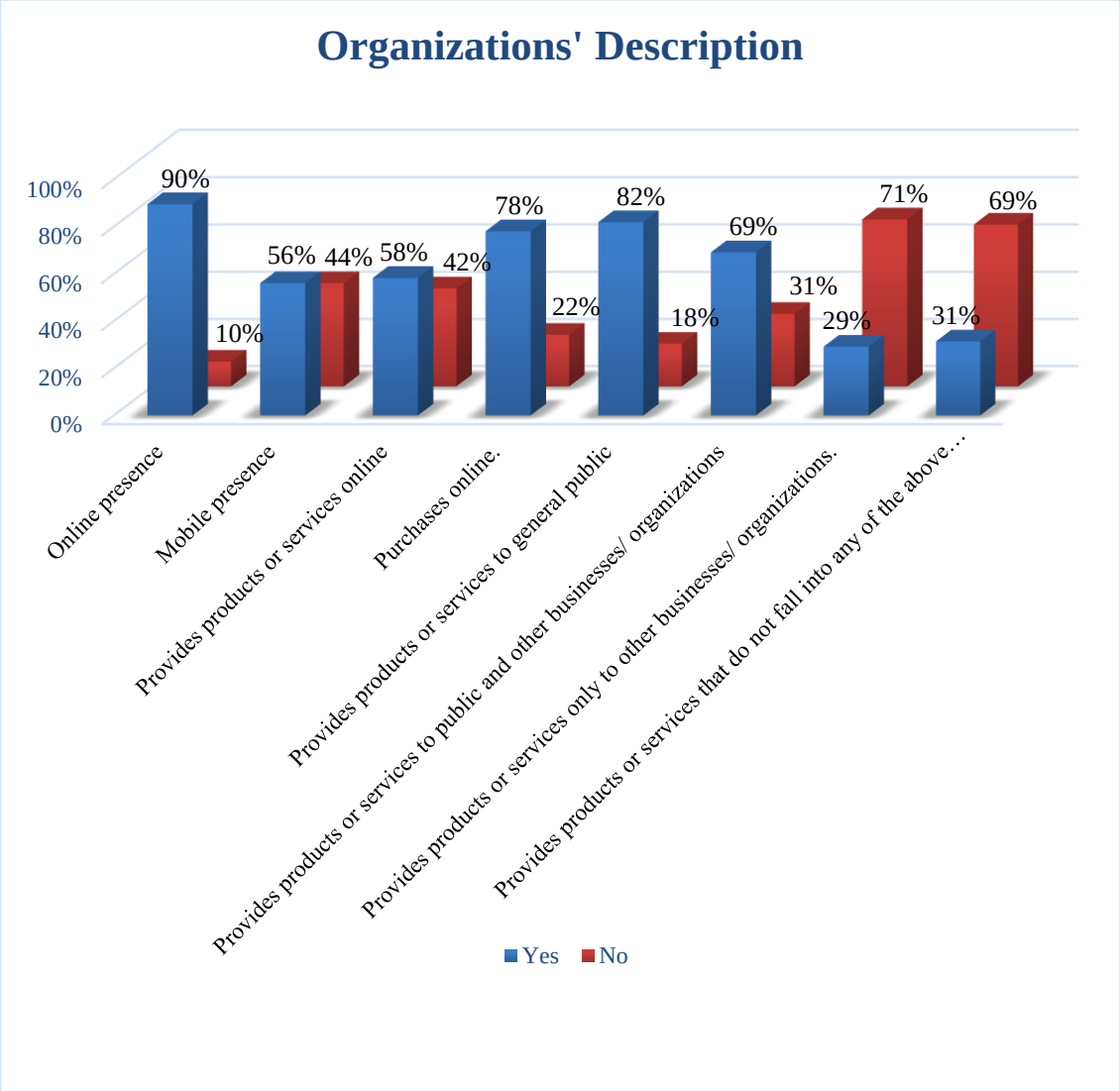


Figure 3.6. Description of the Organizations.

Ninety-one percent of the organizations used personal information while 75% used credit card information and 70% used financial information. Medical information was used by 46 % and 45% used proprietary information (see Figure 3.7).

Five percent used other information of which examples were given as confidential information, criminal history, family, names, birthdates, addresses, phone numbers, non-disclosure agreements, public information, religious background, police records, spousal birth date, social security number and student data.

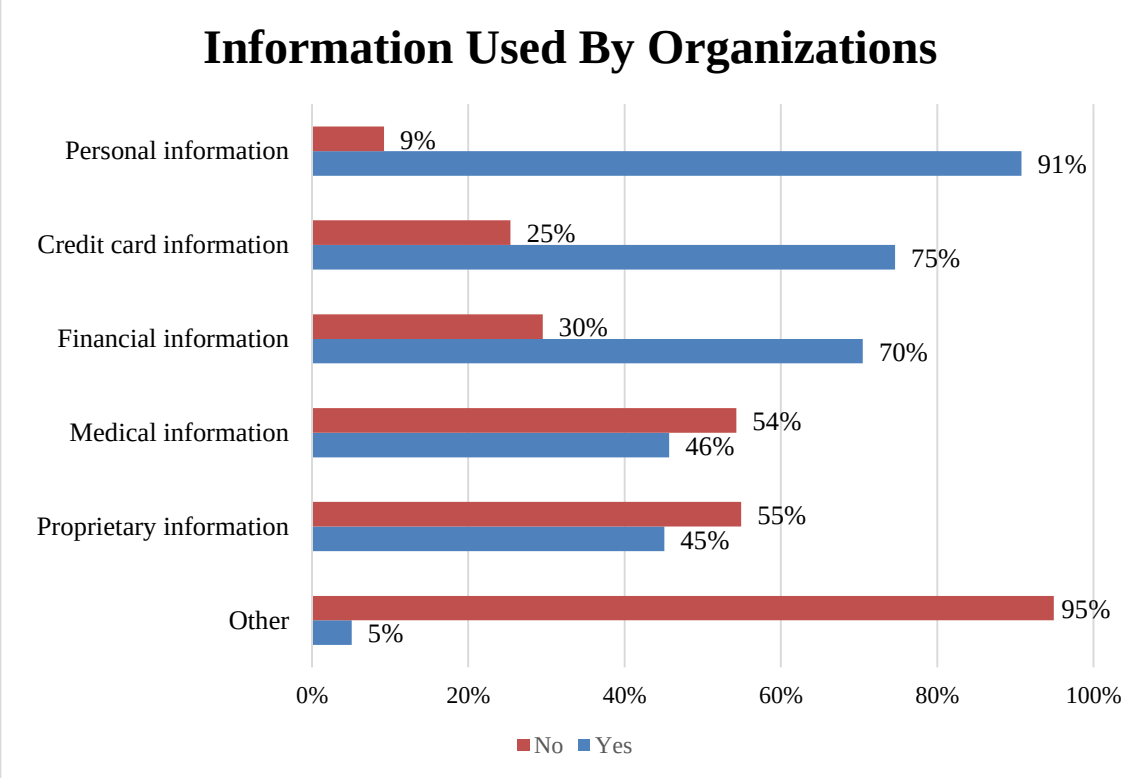


Figure 3.7. Information Used by Organizations.

Forty-four percent of the organizations were large with over 500 employees. Twenty-six percent were very small with between 1 to 50 employees while 20% were medium-sized with 101 to 500 employees. Nine percent were small with 51 to 100 employees and 1% did not know the size of their organization (see Figure 3.8).

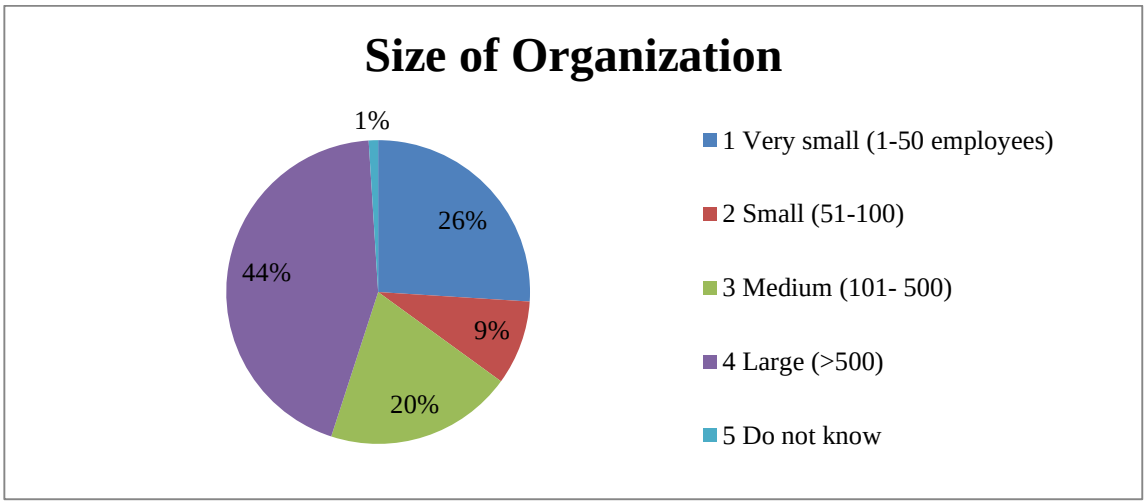


Figure 3.8. Size of the Organizations.

Public organizations accounted for 47% while 38% were private organizations, 13% were not-for-profit and 2% were other (see Figure 3.9).

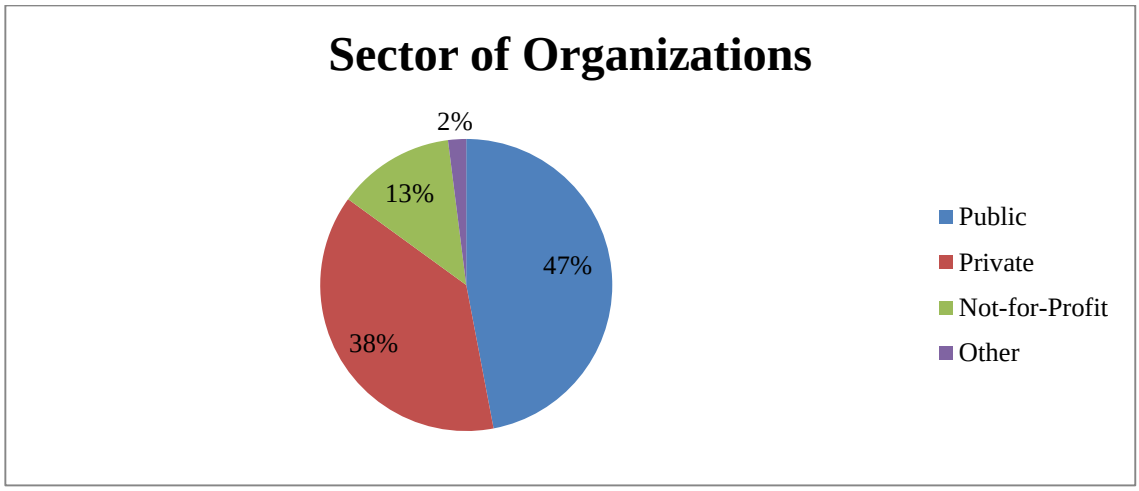


Figure 3.9. Sector of the Organizations.

To provide external validity a variety of industry sectors were included in the sample. It was found that 18% of participants belong in the healthcare and social assistance sector; 13% work in educational services; 10% in retail trade; 8% in the finance and insurance business; 7% professional, scientific and technical services; 7% in other; 5% work for the government; 4% were in manufacturing; 4% were in arts, entertainment and recreation; 4% worked in accommodation and food services; 3% work in other services except public administration; 3% were with legal; 3% in the construction trade; 2% in wholesale trade; 2% telecommunications industry; 2% work with food and beverage; while 1% for utilities; 1% for transportation and warehousing; 1% were in real estate, rental and leasing; 1% worked with information and cultural industries; and 1% with agricultural forestry, fishing and hunting (see Figure 3.10).

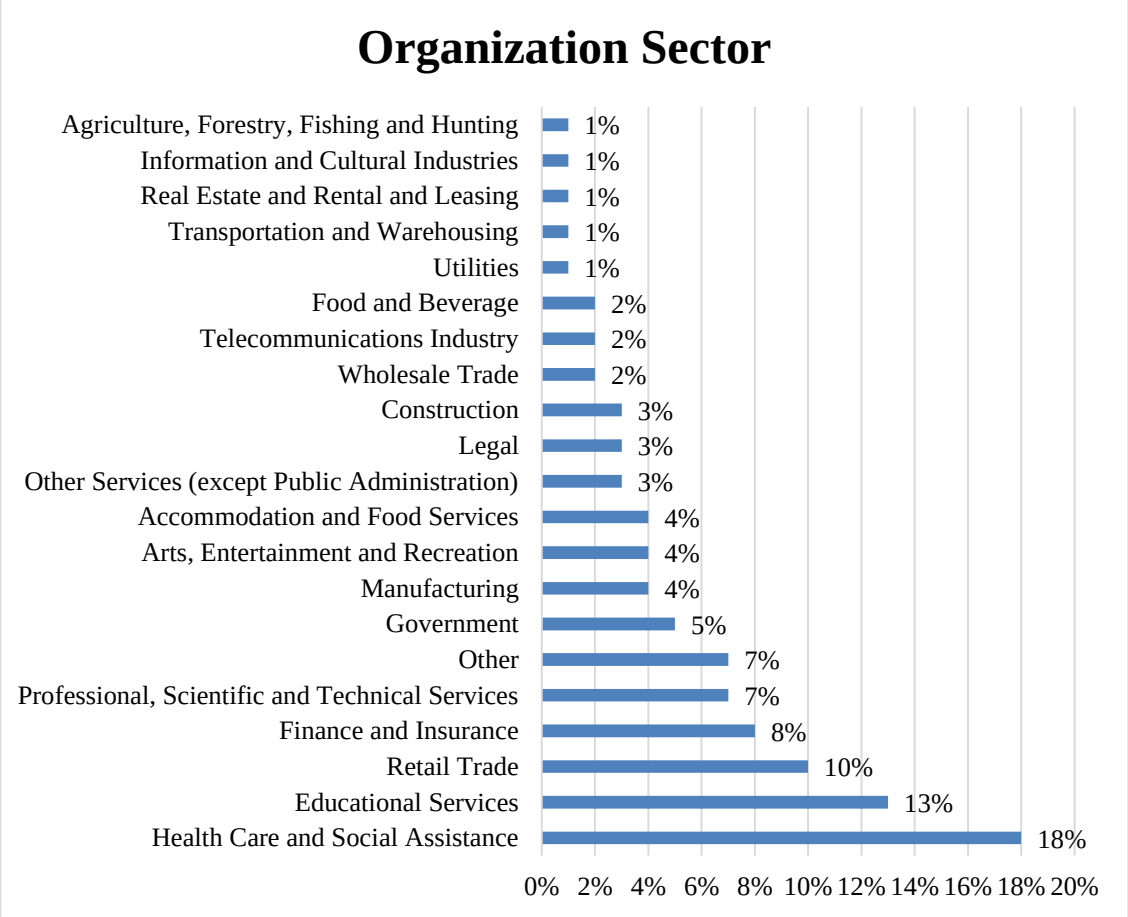


Figure 3.10. Sector of the Organizations.

Discussion

The percentages for Strongly Disagree (SD), Disagree (D), Moderately Disagree (MD), Neither Agree nor Disagree / Neutral (N), Moderately Agree (MA), Agree (A), Strongly Agree (SA) are provided for the 208 questions on the *Privacy Management Survey* (see Appendix E). A Combined Agree percentage was calculated by summing MD: Moderately Agree + A: Agree + SD: Strongly Agree.

New scales were proposed for the privacy management practices construct, based on the fair information practice principles (FIPPs) and Smith et al. (1996)'s seminal scale on information privacy. Brand protection was extended to include privacy management models, training, policies, programs, audits and assessments. New scales to measure privacy breaches and experienced harms were also proposed. A new privacy concerns scale was developed based on a blend of modern-day technological contexts captured in Survey 1 and existing scales around privacy concerns in the academic literature. The brand value scale was adapted from Barnes & Mattsson (2008).

Variables' names and statements have been provided so they can be referred to from other chapters when used in tables and figures. The demographic information for the data set for the long survey are presented in this chapter in order to present a background to the studies' results presented in subsequent chapters.

CHAPTER 4 – STUDY 1: A QUALITATIVE STUDY ON PRIVACY CONCERNS

In this chapter, privacy concerns are studied from qualitative data gathered on two surveys. First I would like to say that I am not apologizing for including qualitative data but rather emphasizing the richness of information the participants have provided to this thesis. In this study, data was collected from 260 mostly expert responses to an open-ended question around privacy concerns in 2010. In addition, data on privacy concerns were gathered from 315 respondents in January 2016 providing free-form details in the survey created in Chapter 3. Further, qualitative data for privacy concerns were gathered from 205 respondents to the same survey in a holdout sample in February 2016. I triangulate the results from analyses of responses from three distinct data sources.

With respect to chronological ordering, the privacy concerns collected from the 260 first-survey respondents were used to formulate a subsequent survey's questions to gather both quantitative and qualitative data during following-on studies. Collecting qualitative information across 3 studies has allowed for a qualitative inquiry of privacy concerns over time as well in the 6-year period of 2010 to 2016. I compare my results with the findings of a seminal 1996 study also on privacy concerns.

According to Mills (2015) his "inclination is to search for socio-political moments over time to understand: first, how selected events influenced the production of a phenomenon; and second, how that influence was embedded in certain actions and translations" (p. 326). With rapid technological changes, proliferation of user devices, and

employees accessing workplace data from work, home, and public areas over networks, it is important to understand how privacy concerns may influence practices, brand protection, and transitively brand value. But first, I needed to capture current-day privacy concerns. As mentioned previously, rich qualitative data on privacy concerns were gathered from three sources (see Table 4.1). In my first exploratory survey, the data describe what people's privacy concerns are from many experts in the privacy and security field. These privacy concerns inform the instrument creation work for the privacy management survey that was described in Chapter 3, including this survey's questions informing the expanded privacy management model (see Chapter 6). The methods employed to collect the qualitative and quantitative data, results of privacy concerns, and discussions are described in this chapter.

Table 4.1

Summary Chart of the Qualitative and Quantitative Studies

	Survey 1	Survey 2	
Title:	*Privacy Concerns Preliminary Survey*	*Privacy Management Survey*	
Date survey conducted:	November 2009 - 2010	January 2016	February 2016
Sample size:	*N* = 260	Sample 1 *N* = 315	Sample 2 *N* = 205 Hold-out sample
Qualitative Data:	one open-ended question around people's privacy concerns when online	two open-ended questions around people's privacy concerns when online of their private information and network traffic	

	Survey 1	Survey 2
Purpose of Qualitative Study:	1) To understand and create themes of privacy concerns 2) To create Privacy concerns statements for survey instrument used in study 2	To understand and create themes of privacy concerns
Qualitative Data Analysis Tools:	NVivo used on the above Qualitative data	NVivo used on the above Qualitative data
Quantitative Data:		208 7-point Likert Scale questions. *Note:* the 2 open-ended questions used in Study 1 (this chapter's study) are not included in the Quantitative data used in Studies 2 and 3. Used existing and new scales for Privacy practices, Brand protection, Experienced harms and Brand value, and privacy concern statements collected from Survey 1.
Purpose of Quantitative Study:		1) To empirically understand current state of privacy concerns, privacy practices, brand protection, experienced harms and brand value 2) To build scales 3) Create a *Privacy-Brand Model* 4) Create an Expanded *Privacy-Brand Model* 5) To test Hypotheses (relationships between constructs)
Data Analysis Tools:	Excel	Excel, SPSS, AMOS
Demographic Information:	• Gender • Age • Education • Country • Profession/Occupation	• Gender • Age • Education • Level of Position • Profession or Occupation • Sector of Organization • Size of Organization • Information used by Organization • Organization Information • Country

Privacy Concerns (PC)

Researchers have established that people are concerned about their privacy. According to Menn (2011), “Online privacy is an increasing subject of concern for the general public and lawmakers, who are contemplating a number of measures including a proposed privacy 'bill of rights' in the US”. Hann, Hui, Lee and Png’s (2007) work categorizes people according to their privacy concerns, and further links privacy concerns and measures that may be taken to alleviate them: “organizations may possess means to actively manage the privacy concerns of Internet users. Our results distinctly show that privacy policies are valued by users. Hence, organizations can capitalize on this by stating their privacy policy more prominently” (p. 33).

According to a seminal paper in privacy, individuals' concerns about organizational information privacy practices include collection, error protection, secondary use and improper access of personal information (Smith et al., 1996). My Privacy Management Survey qualitatively confirms that two of these concerns are still of importance twenty years later, and add a few more categories. The methodology and analyses details are provided below.

Privacy concerns have economic impact: “Privacy problems have been identified to be a major impediment to e-commerce. According to the U.S. Public Interest Research Group, ‘the single, overwhelming barrier to rapid growth of e-commerce is a lack of consumer trust that consumer protection and privacy laws will apply in cyberspace. Consumers . . . worry, deservedly, that supposedly legitimate companies will take

advantage of them by invading their privacy to capture information about them for marketing and other secondary purposes without their informed consent'" (Hann et al., 2007, p. 14). My Privacy Management Survey qualitatively confirms that these concerns are still of importance close to a decade later.

This study tapped employees to answer questions around privacy concerns, with the understanding that an employee may also play a role as a consumer and/or as a manager. Prior research had found that consumers and managers both have concerns about the privacy of information but may have different perspectives. Campbell (1997) found that while managers and consumers were both concerned about the "intended uses for consumer information, they tend to focus on different aspects of information privacy" (p. 54). Consumers are more concerned with "potential abuses of information" while managers are focused on "potential benefits to consumers of better-targeted direct marketing campaigns" (p. 54). I tapped the employee perspective in the Privacy Management Survey, and the consumer and employee perspectives in my preliminary Privacy Concerns Survey. As all employees are consumers, this respondent's roles blurring is acceptable.

Method

Participants

The majority of the sample for the *Preliminary Privacy Concerns Survey* (Survey 1) was chosen from conference attendees from defined disciplines (i.e. information

technology and administrative professionals). The security and privacy conferences were in Canada, United States and Spain. Many of these individuals were responsible for privacy and security in their organizations. Conferences were selected for the sample so there was control over who was providing the data. Professionals were targeted where they congregate and were accessible. The attendees at the conferences represented a random sample because it was not decided in advance who would attend these conferences. Attendees at *Verney Access & Privacy Conference* in Halifax, Nova Scotia, Canada were invited to participate, where I volunteered and attended the conference for many years. Attendees at the *31st International Conference of Data Protection and Privacy* held in Madrid, Spain were invited to participate because this conference is "the largest forum dedicated to privacy in the world, which every year brings together the highest authorities and institutions guaranteeing data protection and privacy, as well as experts in the field from every continent" (Lombarte, 2009).

Other participants included Nova Scotia Provincial Government Administrators and Information Technology employees who attended an annual conference and participants who attended security training and awareness workshops. The sample also consisted of Faculty of Management graduate students at Dalhousie University and MBA students at Saint Mary's University; both located in Halifax, Nova Scotia, Canada. Data was gathered from people originating in 27 countries.

There were 267 participants who responded to survey 1. Seven responses were eliminated because the respondents selected more than one answer for their privacy expectation for a location. *N* = 260 surveys were included in the analysis. Demographic information was collected regarding the participant's gender, age group, level of education, country of origin and residence and their profession or occupation (see Appendix D).

Preliminary Privacy Concerns Survey (Survey 1) demographic information is provided in Table 4.2. The sample was comprised of 38 percent females and 58 percent males and 4% did not identify their gender. There were 2% of participants born before 1950; 19% before 1960; 28% before 1970; 28% before 1980; 21% before 1990; 1% before 2000 and 2% were unspecified.

There were 4% who had No College or University; 19% with Some College or University; 31% with an Undergraduate Degree(s); 42% with Graduate Degree(s); and 4% did not indicate their education.

There were 71% of the participants from Canada; 13% from the U.S.; 2% from China and 14% were from the following countries: Australia, Bangladesh, Czech Rep., Denmark, England, France, Germany, Haiti, Holland, Hong Kong, India, Iran, Italy, Kenya, Netherlands, Nigeria, Pakistan, Romania, Russia, Slovenia, South Africa, Spain, Trinidad & Tobago and Vietnam.

Table 4.2

Descriptive Statistics of Survey 1 Respondents (*N = 260*)

Gender	Male	151 (58%)
	Female	99 (38%)
	Not identified	10 (4%)
Age	Born before 1950 (67 years +)	13 (2%)
	Born before 1960 (57 - 66 years)	49 (19%)
	Born before 1970 (47 - 56 years)	73 (28%)
	Born before 1980 (37 - 46 years)	73 (28%)
	Born before 1990 (27 - 36 years)	55 (21%)
	Born before 2000 (18 - 26 years)	3 (1%)
	Unspecified	5 (2%)
Education	No college or university	10 (4%)
	Some college or university, but no degree	49 (19%)
	Undergraduate degree(s)	81 (31%)
	Graduate degree(s)	109 (42%)
	Did not indicate their education	10 (4%)
Country	Canada	185 (71%)
	United States	34 (13%)
	China	5 (2%)
	Other	36 (14%)

The collected demographic information from the second survey, the *Privacy Management Survey*, includes: gender, level of education, age bracket by decade, country of residence, province/state where employed, profession or occupation, size of organization (number of employees). Information was gathered related to the organization's online and mobile presence and if products or services are provided online.

The type of information the organization uses, discloses or retains: credit card information, financial, medical, personal information and proprietary information.

The type of sector is disclosed: public, private or not-for-profit. The study population includes individuals who live in the United States, are employed full time and are 18 years or older. The organization uses personal information to conduct their business (see Appendix D for demographic questions and Table 4.3 for descriptive statistics for survey 2).

Table 4.3

Descriptive Statistics of Survey 2 Respondents from Sample 1 (N = 315)

Gender	Male	73 (23.2%)
	Female	242 (76.8%)
Age	18 - 24 years	29 (9.2%)
	25 - 34 years	138 (43.8%)
	35 - 44 years	65 (20.6%)
	45 - 54 years	51 (16.2%)
	55 - 64 years	27 (8.6%)
	65 - 74 years	5 (1.6%)
Education	High school graduate, diploma or the equivalent (i.e. GED)	31 (9.8%)
	Some college or university, but no degree	53 (16.8%)
	Trade/technical/vocational training	17 (5.4%)
	Associate degree	42 (13.3%)
	Bachelor's degree	132 (41.9%)
	Master's degree	31 (9.8%)
	Professional degree	4 (1.3%)
	Doctorate degree	4 (1.3%)
	Other	1 (0.3%)

Level of Position	Senior Management	36 (11.4%)
	Middle Management	89 (28.3%)
	Technical	50 (15.9%)
	Clerical/Labour/Other Support	115 (36.5%)
	Other	25 (7.9%)
Profession or Occupation	Administrative Support	67 (21.3%)
	Arts and Entertainment	8 (2.5%)
	Engineer	4 (1.3%)
	Financial	13 (4.1%)
	Human Resources	14 (4.4%)
	Information Technology	33 (10.5%)
	Law Enforcement	3 (1.0%)
	Legal	6 (1.9%)
	Medical	39 (12.4%)
	Privacy Officer	0 (0.0%)
	Professor / Teacher	12 (3.8%)
	Sales and Marketing	38 (12.1%)
	Science	4 (1.3%)
	Security	0 (0.0%)
	Student	1 (0.3%)
	Transport	2 (0.6%)
	Other	71 (22.5%)
Sector of Organization	Public	148 (47.0%)
	Private	121 (38.4%)
	Not-for-Profit	40 (12.7%)
	Other	6 (1.9%)
	Accommodation and Food Services	14 (4.4%)
	Administrative and Support, Waste Management and Remediation Services	1 (0.3%)
	Agriculture, Forestry, Fishing and Hunting	4 (1.3%)
	Airline	1 (0.3%)
	Arts, Entertainment and Recreation	12 (3.8%)
	Construction	9 (2.9%)

	Educational Services	40 (12.7%)
	Finance and Insurance	26 (8.3%)
	Food and Beverage	5 (1.6%)
	Government	15 (4.8%)
	Health Care and Social Assistance	57 (18.1%)
	Information and Cultural Industries	3 (1.0%)
	Legal	8 (2.5%)
	Management of Companies and Enterprises	1 (0.3%)
	Manufacturing	14 (4.4%)
	Mining, Quarrying, and Oil and Gas Extraction	0 (0%)
	Other Services (except Public Administration)	9 (2.9%)
	Professional, Scientific and Technical Services	21 (6.7%)
	Public Administration	1 (0.3%)
	Real Estate and Rental and Leasing	2 (0.6%)
	Retail Trade	32 (10.2%)
	Telecommunications Industry	7 (2.2%)
	Transportation and Warehousing	3 (1.0%)
	Utilities	2 (0.6%)
	Wholesale Trade	6 (1.9%)
	Other	22 (7.0%)
Size of Organization	Very small (1-50 employees)	83 (26.3%)
	Small (51-100 employees)	27 (8.6%)
	Medium (101 - 500 employees	63 (20.0%)
	Large (>500 employees)	139 (44.1%)
	Do not know	3 (1.0%)
Information used by Organization	Personal information	286 (90.8%)
	Credit card information	235 (74.6%)
	Financial information	222 (70.5%)
	Medical information	144 (45.7%)
	Proprietary information	142 (45.1%)
	Other information	16 (5.1%)
Organization Information	Has an online presence	282 (89.5%)
	Has a mobile presence	177 (56.2%)

	Provides products or services online	184 (58.4%)
	Purchases online	246 (78.1%)
	Provides products or services directly to the general public	258 (81.9%)
	Provides products or services both to the public and to other businesses/ organizations	218 (69.2%)
	Provides products or services only to other businesses/ organizations	92 (29.2%)
	Provides products or services that do not fall into any of the above categories	99 (31.4%)
Country	United States	315 (100%)

Survey questions were asked on the *Privacy Management Survey* (Survey 2) to determine if participants fall into the category of privacy guardians, information sellers or convenience seekers. “Subjects can be categorized into three distinct segments - privacy guardians, information sellers, and convenience seekers. The majority of subjects were relatively sensitive to online information privacy concerns (‘privacy guardians’). By contrast, a smaller proportion was relatively willing to provide personal information in exchange for money (‘information sellers’), and an even smaller proportion was relatively willing to provide personal information in exchange for convenience (‘convenience seekers’)” (Hann et al., 2007, p. 33). In study 2 the majority 78% (10% were neutral) of the participants would be considered Privacy Guardians. This agrees with Hann et al. (2007) but only 14% were information sellers and more, rather than less, 17% were convenience seekers.

Data Collection and Analysis

This research was reviewed and approved by the Saint Mary's University Research Ethics Board. If participants had any questions or concerns about ethical matters, they were instructed to contact the Chair of the Saint Mary's University Research Ethics Board at ethics@smu.ca or (902) 420-5728 and refer to REB File # 09-218 for study 1 and REB File # 14-340 for studies 2 and 3. The Privacy Management Survey, in long form - "*The lmpact of Privacy Management on Brand Protection and Value*", received a Certificate of Ethical Acceptability for Research lnvolving Humans and was approved from November 25, 2014 to November 25, 2015 and renewed from December 22, 2015 to December 22, 2016. The research was conducted according to the Guidelines of the Research Ethics Board at Saint Mary's University in Halifax, Nova Scotia. If participants had any questions related to the surveys they were asked to contact the researcher or Faculty Advisor. Contact information including e-mails and telephone numbers were provided for each on the surveys. There were no harmful exposures induced during this research project. The data collected is anonymous and voluntary. Implied consent was given by participants by submission of their survey.

Data was gathered from conducting two surveys: the *Preliminary Privacy Concerns Survey* (N = 260) and the *Privacy Management Survey*. The second survey was deployed twice (N = 315 and N = 205). The first short survey instrument (see Appendix B) included one open-ended question around people's privacy concerns when online and close-ended

questions around their expectation of privacy when different privacy programs were in effect (at work, home, and ad-hoc public hotspot). The open-ended question enabled the collection of free-form utterances, which were then subjected to an application of McCracken (1988) data analysis procedure with its progression of analyzing individual observations to identifying the grouping of general themes. Logical relations of identity, similarity, opposition, and contradiction were noted. A refinement process to identify patterns and general properties was conducted next. Then judgment was used to identify themes and their interrelationships forming an analytic view of the study's context. Each generalized theme consists of a delineated privacy concern.

NVivo 11 was used to analyze the qualitative data collected from the two surveys to provide rigor, validity and reliability. "Using NVivo in the data analysis process also adds rigour to the process by allowing the researcher to carry out quick and accurate searches of a particular type, adding to the and reliability of the results by ensuring that all instances of a particular usage are found" (Boisson, 2017, 5.2.2). The data from the two surveys were organized into themes in NVivo and presented in this chapter. The associated statements to the themes are provided in tables. Figures are used to visualize the results.

NVivo allowed for in-depth analyses of a vast amount of qualitative data. "In summary, QSR-NVivo is a powerful tool that, if used appropriately, can facilitate many aspects of the grounded theory process from the design and early sampling procedures,

through to the analysis of data, theoretical development and presentation of findings" (Hutchison, Johnston, and Breckon, 2010).

Johnston (2006) states that "QDA [qualitative data analysis] software has undoubtedly legitimized qualitative research in disciplines that have traditionally adopted quantitative approaches" (p. 384). More common in the behavioural and social sciences there is a "growing interest in mixed-methods approaches" (Johnston, 2006, p. 384). Johnston (2006) believes that "one of the reasons for this may be the increased ability to link qualitative and quantitative data in a way that was extremely difficult to do without software" (p. 384). Johnston (2006) suggests "stepping back from the data and thinking logically about how to build and develop the results of searches into an iterative series of steps is at the heart of expert use of NVivo" (p. 388).

The data from survey 1 were entered into Excel spreadsheets. The data from survey 2 (both original and holdout samples) were collected in SPSS files. Microsoft Excel, IBM SPSS Statistics 23, AMOS Graphics in IBM AMOS 23 and NVivo 11 were the computer programs used to analyse the survey data. Excel was used to create graphs for the demographic data and calculate percentages of the survey responses. SPSS and AMOS were used to analyze the quantitative data. SPSS was used to do principal components analysis (PCA). AMOS Graphics was used to do confirmatory factor analyses to make diagrams using structural equation modelling. NVivo was used to organize, analyze and prepare visual reports of the qualitative data. NVivo organized the data into themes. The

statements that were associated with each theme for each survey were converted into tables. Charts were created to help visualize the results.

After a literature review was conducted (see Chapter 2) survey questions were developed to measure the constructs in this research (see Chapter 3). The constructs are privacy practices, privacy concerns, online brand protection, experienced harm, and brand value. Privacy concerns were collected to determine how privacy concerns have changed over time.

A hard copy survey was tested at conferences as well as by interviews with experts in the field of privacy. Their comments and suggestions were incorporated into the survey.

The questions were then programmed into LimeSurvey by the researcher. Once the online survey was ready, email addresses were gathered at conferences of those who were interested in completing the survey. The link to the survey was emailed to those people. As well, the Privacy Commissioner of Nova Scotia sent the link to the survey to Privacy Colleagues across Canada for survey distribution. Other colleagues distributed the survey to their contacts. Due to the low response rate, a professional survey company, Qualtrics, subsequently was hired to gather the data for survey 2. My invitation to participate in the study and online survey instrument deployed by Qualtrics are provided in Appendix C. My survey included two open-ended questions around people's privacy concerns about their personal information and network traffic. It also included 208 items that were rated

on a 7-point Likert scale from 1 = strongly disagree to 7 = strongly agree. This methodology was chosen to gather data to empirically test the hypotheses in this research (see Chapter 5). The value of the survey method allowed for a greater number of participants and questions than could have been accomplished through in-depth interviews.

A pilot study or soft launch of my *Privacy Management Survey* was conducted by Qualtrics on January 8th, 2016 with 30 participants. The survey data was verified to be accurate before the actual data collection began for survey 2.

Two random samples of participants (N = 315 and N =205) were selected by Qualtrics for studies 2 and 3. The participants had to pass four qualifying questions in order to participate in the survey. The questions included being 18 years or older, employed full time, work with personal information and live in the United States. There was also one statement included to eliminate anyone selecting answers without reading the statement. The statement was "To show your commitment to providing thoughtful answers please select disagree." Only participants who selected disagree were included in the sample. There was a duration check set at 6 minutes and 54 seconds to ensure that participants were taking an appropriate amount of time to respond. There were 1770 people who started the survey and out of 1639 who completed the survey 315 met the four qualifications and answered all of the questions. The survey data file was received

on January 18, 2016. Another 205 surveys were collected by Qualtrics on February 12, 2016 (see Chapter 7).

Information was collected in the preliminary phase of study 1 during 2009 and 2010 until more than 200 surveys were completed. Data entry and statistical analysis were completed in 2011. Survey 2 was conducted in January 2016 and a subsequent Survey 2 redeployment was conducted in February 2016 to obtain a holdout sample. Data entry and statistical analyses for survey 2 were completed in studies 2 and 3 in 2016 - 2017.

Results

Privacy Concern Themes Using NVivo 11

NVivo is a user-friendly, highly recommended program to organize qualitative data. NVivo was used to analyze the privacy concerns of network traffic from survey 1; the privacy concerns of personal information and network traffic from two sets of independent data collection done at different times with different respondents based on my second survey entitled the Privacy Management Survey. The statements that were associated with each theme for each survey were made into tables. Mind maps, project maps, tree maps, word frequency and word clouds were created to help visualize the results.

Privacy Concerns from Survey 1 (*N* = 260)

Over half, 138 of the 260 participants, included privacy concerns in response to the open-ended questions on their survey. This question was optional on survey 1. To avoid missing data participation in the privacy concern statements along with all other statements were made mandatory on the second survey.

I autocoded the privacy concerns in NVivo. The raw themes that emerged were: 1) access/ unauthorized access 2) exposing accounts 3) exposing online activities 4) exposing address 5) exposing banking/ banking information / online banking 6) exposing data/ financial data 7) exposing online history 8) exposing home information 9) exposing the individual 10) exposing info/ information/ much info/ personal info 11) concern about the internet 12) exposing location 13) concern about the network 14) tampering with packet headers 15) concern over privacy 16) concern regarding protection 17) concern over providers 18) concern about revealing to the public 19) security concern 20) social networking concern 21) identity theft 22) traffic and 23) data use. These raw themes and overlapping privacy concerns are provided in Figures 4.1 and 4.2. Then the automatically generated themes were analyzed and the themes that were determined to be similar were combined, such as access and unauthorized access as per below and in Table 4.4.

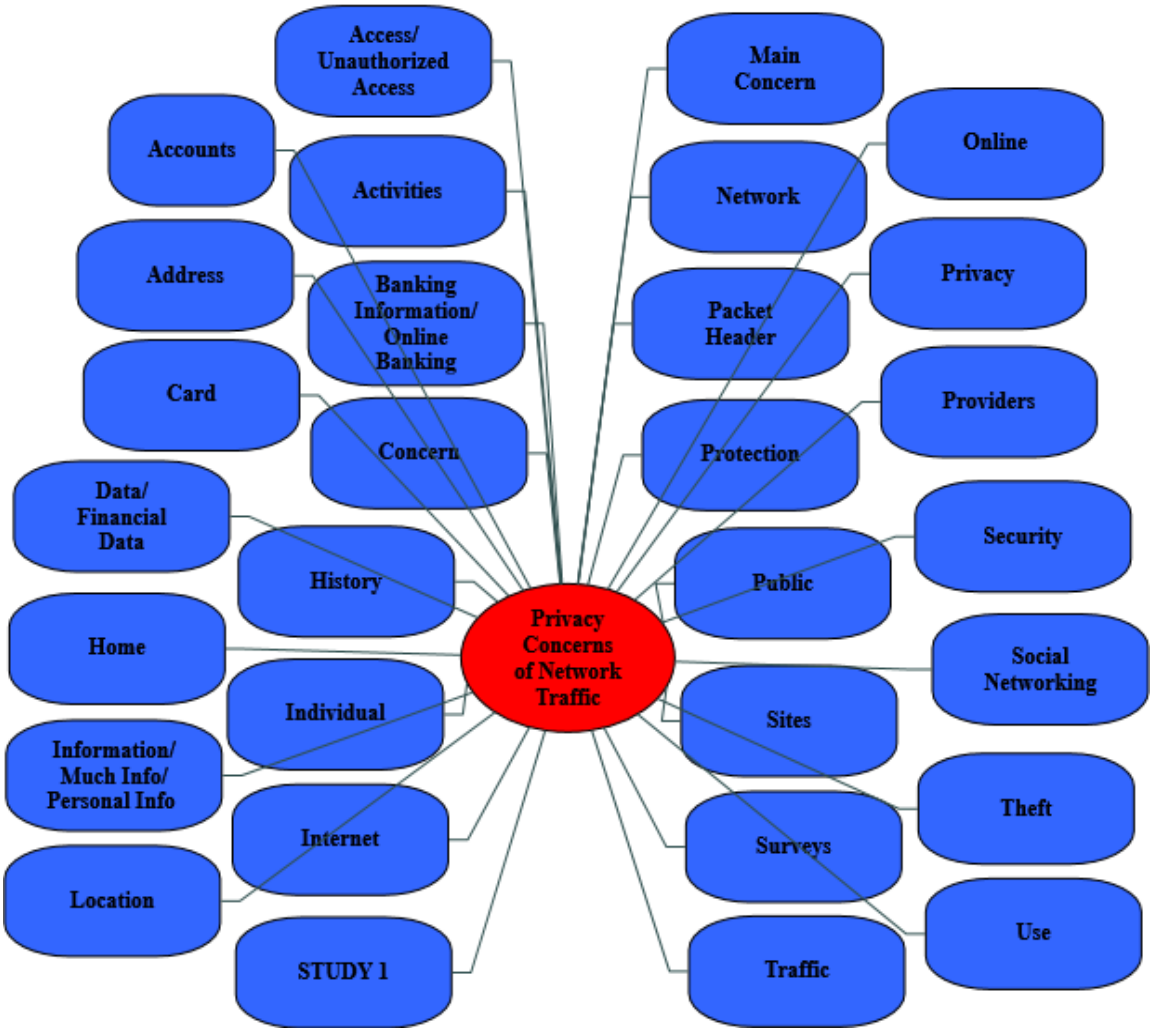


Figure 4.1. Privacy Concerns of Network Traffic from Study 1 Autocoded in NVivo.

Figure 4.2 represents a word cloud of the most frequent words used when asked, what concerns do you have about the privacy of your network traffic? Words with more occurrences are displayed with a larger font size.

Figure 4.2. Word Cloud of Privacy Concerns of Network Traffic.

Some of the more common words found during the word frequency query in NVivo, with the count provided in parentheses, are: information (32), privacy (28), data (25) and private (20). For further details refer to the word frequency table (see Table 4.4).

Table 4.4

Word Frequency of Privacy Concerns from Survey 1.

Word	**Count**	**Word**	**Count**	**Word**	**Count**
information	32	know	10	info	8
Privacy	28	network	10	people	8
Data	25	security	10	use	8
Private	20	concern	9	access	7
online	17	Identity	9	banking	7
traffic	14	Theft	9	expect	7
personal	13	Concerns	8	financial	7
concerned	12	Credit	8	internet	7

Examples are provided of privacy concerns from each theme. The statements were selected that were thought to best explain the theme. Sometimes statements are coded under more than one category if multiple examples of privacy concerns were provided on a survey. To avoid repetition, if a statement was already explained it was not selected as an example for a different theme.

Unauthorized Access

A consistent theme of a privacy concern that emerged is unauthorized access. "Access of information by a third party that is not authorized" is a concern of several participants. Remaining private online was one person's method of protecting their financial accounts, "My primary concern involves online banking, loan, applications, and student accounts. Therefore, I try to be as 'private' as I can online (i.e. deleted my Facebook account)."

Unencrypted traffic on the network that can be intercepted and financial data gathered is a concern for these respondents who are "concerned about network traffic leaking private data, especially credit / bank cards" and "my top concern is that my traffic is unencrypted and can be easily intercepted at various points." Virus attacks when surfing the Internet are a concern as this person said, "I am constantly concerned about getting viruses / spyware / malware when I surf." This participant is concerned about the security of corporate servers with databases of credit card information, "I'm more

concerned with the security of stored data (like credit card databases on a corporate server) than with viewing of transactions." This respondent recommends using software to protect sensitive data, "You should expect that there will be a breach and modify communications accordingly and use other data protection software to additionally secure information that is being communicated - if it is sensitive."

Misuse/ Unauthorized Use/ Privacy Breaches

A person who is concerned about anonymized individual records stated, "Any organization releasing data, containing information on persons as individual records, which has been believed anonymized." One felt helpless about their online information, "I worry about my information online but do not feel like there's all that much I can do about it."

Another participant also agrees that their Internet use should be private as explained, "Personal data and other data that can be used to create profile of my Internet use should be private, i.e. should not be shared with anyone." Scam networks in public locations were a concern raised, "number of scam networks in public locations, for example airports." This is especially troubling for those who expect privacy in public hotspots.

It is so much easier to find information since "so much info is now online, archived & searchable." It is better to be able to find information online in many situations but it is a concern for this participant who may not want their information to be so accessible. This person uses encryption if they want privacy in network traffic. They responded, "I

don't expect privacy in network traffic unless I choose to encrypt my communications." This person's privacy concern is that network traffic is monitored by the U.S. government, AT&T and other providers as stated, "US gov't routinely monitors network traffic, as does AT&T and perhaps other backbone providers."

This participant's concern is the "risk of online shopping and banking." This respondent takes precautions if they want their information on the network to be private, "If I want it to stay private, I better ensure that myself - whether for payload or packet header." This person is concerned that there may be more large-scale privacy breaches by moving to cloud internet based servers, "moving to more open source and cloud internet based servers might lend to more large-scale privacy breaches." An ATIP (*Access to Information and Privacy)* professional stated that their "Concerns are of personal information being leaked out by error." A Manager of Communications stated that their concern was with "Third party access, security and confidentiality of information. Not everyone has the same understanding therefore open for errors!" An Access Coordinator believed that "Simpler language" was required "so that there is no misunderstanding, more education within the youth especially."

Another respondent's concern is "unsecure public wifi (wireless) networks." This person is concerned that even with proper security measures in place a hacker could get private information if determined as stated, "concerned that if something should be kept

private, and appropriate security actions are taken, it would still be insufficient against a determined attacker."

Posting personal information on social networking sites has this person "concerned about the erosion of personal privacy with Facebook and Twitter and peoples need to post every detail about their lives online." This participant is concerned about the privacy of passwords and tracking of purchase habits without permission as they responded, "Tracking of purchase habits done without my knowledge or consent (vs. a survey inquiry) also privacy of various passwords is a concern."

"Identity theft / credit card theft is a concern" that has been expressed by many survey respondents. A person is concerned about their Internet Service Provider as he/she said, "I would love it if I trusted my ISP not to sell/analyze my traffic patterns & DNS [domain name service] lookups, but profit seems to come first in USA." This person has "concerns about misuse / fraudulent use of information."

Theft of Identity, Financial information, Pictures and Personal information

A police officer's concern is that there may be a "take over of my 'personality' and it's use for negligent purposes. An Information Access and Privacy (IAP) Professional said they had "None at work (except spoofing); however, all kinds of concerns with regards to PI (personal information) as a private individual – identity theft, theft of financial information. Concerned about 'registration' for almost everything online is easily compromised."

With people congregating on online platforms, there are ethical concerns of how information is used from social networking sites. A survey participant is concerned about "government / employers / business using information from social networking sites against individuals." This person is concerned with their search history, browser history and the sites that they visited are being monitored, "I'm not very concerned about privacy but my main concerns are first search history and then browser history / visited sites." This participant has an expectation of complete privacy of their data at home, "At home providers should have ZERO ability to view any data." Another respondent stated: "I worry about the slow accretion of personal info that may not be overly sensitive on its own, but is simply no one's business - such as current location, photos, etc. that I might not want online → it makes a sort of informal (but very complete) dossier on my daily activities." Aggregation of data from various sources to build profiles that could not be built from a single source is a concern of another respondent.

Need for Protections

New Laws and Regulations around Privacy are both needed and reviled. A Ph.D. in Informatics stated that he was concerned that there was no privacy of the packet header. He noted that the "EU [legal] discussion about IP (Internet Protocol address of the computer) equal to personal ID" is ongoing. He believed that the payload should be completely private and that it should be "prohibited by Law to inspect payload." One respondent indicated that in "Principle: 1) Any network traffic or other traffic sent over

the air is expressly interceptable under U.S. law. 2) Traffic, once it enters an ISP or other provider's network, is interceptable by the provider (formally) or its employees (informally). Therefore, I as an individual can have no expectation that traffic is private. If I want it to stay private, I better ensure that myself - whether for payload or packet header." One respondent was concerned about "Increasing power of law enforcement where new laws allow for the mapping of IP address to physical addresses without the need of a warrant."

Prominently displaying privacy policies is an important method for organizations "to actively manage the privacy concerns of Internet users" (Hann et al., 2007, p. 33). Some organizations are not doing this well as one expert's concern is that, "I'm also troubled by how opaque and verbose privacy policies are."

A Manager of Policy and Planning for Education said, "There is really not much control or restriction on this." They thought it was "sort of (an) unknown area." An Administrator/ Consultant stated, "I don't want to be out there! More integrated work is required from all levels of government, business, IT, etc. to somehow bring this in control more." A Manager for the Government of Nova Scotia is concerned with an "invasion of privacy". One person commented that the "U.S. government routinely monitors network traffic, as does AT&T and perhaps other backbone providers." Their concern was that "This access can be abused."

Large scope of privacy loss

One Canadian Policy analyst was concerned that “moving to more open source and cloud Internet based servers might lend to more large-scale privacy breaches.” They suggested that “a solution might be in proactive approaches to best practices.” An Access & Privacy Manager stated that, “Nothing is 100% secure. You should expect that there will be a breach and modify communications accordingly and use other data protection software to additionally secure information that is being communicated – if it is sensitive.” An Application Database Administrator (IT) said, “I don't expect privacy in Network Traffic unless I choose to encrypt my communications.” A Health IT (Information Technology) Consultant disclosed that, “It is easy for people in the know to intercept and view network traffic.” They recommended that there “should be more security by default to protect people who don't know.” A Canadian Lawyer/Privacy Specialist said their concern was “Disclosure or unauthorized access to my Personal Information.” A Professional Services Consultant (Information Management) was concerned with “unauthorized access by hackers.” “Surreptitious access” was the concern of an Information Technology professional. A FOIPOP (Freedom of Information and Protection of Privacy) Administrator had two concerns: “1) Hackers and 2) Third party disclosure.” “Too many people accessing my personal information” was the concern of a Federal Government Access to Information & Privacy Official.

Social networking is a big enable to wide privacy loss. A Communications professional stated, “That too much information – private information – goes out through social networking.” This caused another respondent to cancel her Facebook page. She was worried that there was “Too much information about a person (and their acquaintances) on own Facebook page; unknown what others on your friends list do with your pictures or information – a big concern.”

A Canadian Coordinator, FOI (Freedom of Information) and Privacy said they have “lots” of concerns about network traffic privacy. A Canadian Coordinator, Security and Compliance, used the word “all” to describe their concerns. An IT Professional is concerned about, “Everything in relation to privacy.” They “always hope that network access is private but know in reality it is probably not.” Another participant’s concern was that “Every piece of your information could be revealed to the public.”

The statements associated with each privacy concern theme from survey 1 are provided (see Table 4.5).

Table 4.5

Privacy Concern Themes and Statements from Survey 1

Unauthorized Access
Unauthorized access by hackers.
Disclosure or unauthorized access to my Personal Information.
Always hope that network access is private but know in reality it is probably not.
surreptitious access
My top concern is that my traffic is unencrypted and can be easily intercepted at various points.
Third party access, security and confidentiality of information.
Number of scam networks in public locations, for example airports.
U.S. gov't routinely monitors network traffic, as does AT&T and perhaps other backbone providers.
It is easy for people in the know to intercept and view network traffic through social network especially.
At home providers should have ZERO ability to view any data.

Data / Financial Data / Health Data
Concerned about network traffic leaking private data, especially credit/bank cards
Loss of financial data.
Personal or financial data being seen or intercepted by a third party.
My concerns are primarily social, with a bit of government data (e.g. health information).
Mainly privacy protection of financial data.
Personal data and other data that can be used to create profile of my Internet use should be private, i.e. should not be shared with anyone.
privacy of credit cards
Always wonder about online credit card transactions.
I'm more concerned with the security of stored data (like credit card databases on a corporate server) than with viewing of transactions.
Credit card info, banking info.
Also, identity theft / credit card theft is a concern.
I always worry about completing online banking @ dalhousie internet.
My primary concerns involve online Banking, loan, applications, and student accounts.
Banking information, private conversations.
Banking information leaked, any privacy or Id Breaks from sites on or off (t. ne)
The network, questionable objectives.

Need Better Protection
New laws allowing for the mapping of IP address to physical addresses without the need of a warrant.
Immediately before, after, on other information flows happening at the same time etc. Also who gets to use that data: when, where, for what purpose; how is it governanced; management of failure when something goes wrong with the personal info involved etc.
You should expect that there will be a breach and modify communications accordingly and use other data protection software to additionally secure information that is being communicated - if it is sensitive.
I only work on my home computer since it has software to protect me and my information
At home, providers should have ZERO ability to view any data.
Protecting client's data at home office.
Mainly privacy protection of financial data.
Packet header - no privacy, EU discussion about IP equal to personal ID.
If I want it to stay private, I better ensure that myself - whether for payload or packet header.
I don’t expect privacy in network traffic unless I choose to encrypt my communications.
I'm also troubled by how opaque and verbose privacy policies are.
Concerned that if something should be kept private, and appropriate security actions are taken, it would still be insufficient against a determined attacker.
Mostly my concerns are with regards to my ISP's security practices.
Lost confidence with internet security.
Lack of knowledge concerning the privacy infrastructure.
I am constantly concerned about getting viruses / spyware / malware when I surf.

Unauthorized Disclosure/Privacy Breach
Any organization releasing data, containing information on persons as individual records, which has been believed anonymized.
Exposure of client's data at home office.
all kinds of concern with regard to PI as private individual - identity theft
Exposure of confidential information
unsecure public wifi (wireless) networks

Privacy Loss via Social Networking
Government / employers / business using information from social networking sites against individuals.
through social networking especially.

Concerned about the erosion of personal privacy with Facebook and Twitter and peoples need to post every detail about their lives online.
I try to be as "private" as I can online (i.e. deleted my Facebook account).
Large-Scope Loss of Privacy
My concern is that my privacy doesn't exist.
Concerns what does get out there is no real privacy; one becomes an open book.
I worry about the slow accretion of personal info that may not be overly sensitive on its own, but is simply no one's business - such as current location, photos, etc. that I might not want online -> it makes a sort of informal (but very complete) dossier on my daily activities.
Banking information leaked, any privacy or Id Breaks from sites on or off (t. ne) The network, questionable objectives.
Organizations can amass a database of personal online activity.
Concerned about "registration" for almost everything online is easily compromised
Risk of online shopping and banking.
I would love it if I trusted my ISP not to sell/analyze my traffic patterns & DNS [domain name service] lookups, but profit seems to come first in USA.
So much info is now online, archived & searchable.
Personal data and other data that can be used to create profile of my Internet use should be private, i.e. should not be shared with anyone.
Lost confidence with internet security.
Moving to more open source and cloud internet based servers might lend to more large-scale privacy breaches.
Too much info about a person.
Search history and then browser history / visited sites are readily available.
U.S. gov't routinely monitors network traffic, as does AT&T and perhaps other backbone providers.

Misuse/Unauthorized Use
Government / employers / business using information from social networking sites against individuals.
Also, concerns about misuse / fraudulent use of information.
Identity theft (18 occurrences)
(except spoofing) none at work, however all kind of concern with regard to PI as private individual - identity theft
Also, identity theft / credit card theft is a concern.
Someone hijacking my system and performing illegal activities where my system is the only traceable element.
Personal data and other data that can be used to create profile of my Internet use should be private, i.e. should not be shared with anyone.

The privacy concerns gathered from the above data collection and analysis were incorporated into a subsequent survey instrument and quantitatively examined in study 2. For quick reference the subsequent survey statements are listed in Table 4.6. They are arranged according to the ones that participants strongly agreed (SA) with the most to the least i.e. in descending order (see Table 4.6).

Table 4.6.

Privacy Concerns Participants Strongly Agreed with the Most from Study 2

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
151	I am concerned about viruses / spyware / malware / EXE files / multimedia files.	1%	2%	3%	9%	24%	28%	33%	85%
161	I am concerned about the privacy of wireless access at public hot spots.	4%	3%	5%	12%	18%	27%	32%	76%
133	If I have concerns for online privacy I refrain from interacting with a Web site.	2%	2%	3%	10%	22%	32%	30%	83%
162	I am concerned about protecting client's data.	4%	3%	3%	11%	19%	29%	30%	79%
146	I am concerned about identity theft.	1%	3%	5%	7%	27%	27%	30%	84%
130	If I have concerns for online privacy I use protection behaviors such as removing personal information from lists.	2%	3%	3%	12%	26%	29%	26%	81%
144	I am concerned about information seen or intercepted by a third party.	4%	3%	5%	13%	24%	25%	26%	75%
165	I am concerned about the lack of privacy rights.	3%	3%	5%	18%	21%	24%	26%	70%
166	I am concerned about location tracking.	4%	4%	8%	13%	23%	22%	26%	70%
129	If I have concerns for online privacy I use protection behaviors such as refusing	1%	3%	2%	14%	24%	30%	25%	79%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
	information disclosure or transactions.								
158	I am concerned about privacy of passwords.	4%	4%	6%	11%	22%	29%	25%	75%
135	I have concerns for mobile privacy.	3%	2%	3%	16%	28%	24%	25%	77%
167	I am concerned about the government having my personal information.	6%	6%	8%	14%	19%	23%	25%	66%
148	I am concerned about the lack of privacy control online.	3%	3%	6%	11%	31%	22%	24%	77%
164	I am concerned that personal information is readily available and that risks are not communicated to the public.	3%	3%	3%	13%	27%	28%	23%	77%
150	I am concerned about the privacy of my photographs online.	4%	6%	11%	16%	20%	20%	23%	64%
140	I am concerned that my personal information is used without permission.	6%	7%	6%	14%	25%	19%	23%	67%
155	I am concerned that there is no way to tell if personal data being stored is secure.	2%	3%	3%	15%	25%	31%	22%	78%
156	I am concerned that personal data obtained is shared with others.	3%	2%	3%	10%	27%	34%	21%	82%
145	I am concerned that someone may hijack my system and perform illegal activities where my system is the only traceable element.	6%	7%	8%	18%	20%	20%	21%	61%
147	I am concerned that privacy online is an illusion; it does not exist.	7%	5%	4%	18%	26%	18%	21%	65%
163	I am concerned about export of data to jurisdictions with lax privacy laws.	4%	4%	5%	22%	21%	24%	20%	65%
170	I am concerned that someone may hijack my account and ruin my reputation.	5%	4%	10%	17%	21%	23%	20%	64%
139	I am concerned that my personal information is accessed without permission.	6%	7%	5%	15%	26%	22%	20%	68%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
157	I am concerned about tracking purchase habits.	5%	7%	8%	13%	22%	26%	19%	68%
169	I am concerned that online registration is easily compromised.	5%	3%	5%	17%	26%	25%	19%	71%
154	I am concerned about people who have personal data do not care about its security.	4%	2%	5%	23%	27%	20%	19%	65%
149	I am concerned about the privacy of my email messages.	4%	6%	11%	18%	23%	19%	18%	61%
168	I am concerned that network traffic is leaking private data.	4%	5%	5%	19%	24%	26%	17%	67%
159	I am concerned about the privacy of wireless access at home.	6%	5%	11%	16%	20%	25%	17%	62%
142	I am concerned about online credit card transactions.	8%	9%	10%	16%	23%	17%	17%	57%
160	I am concerned about the privacy of wireless access at work.	9%	11%	13%	17%	16%	19%	16%	50%
131	If I do not have concerns for online privacy I use my personal information.	6%	7%	7%	13%	22%	29%	15%	66%
153	If I want my personal information protected I would not put it online.	4%	6%	10%	23%	23%	19%	15%	57%
134	I engage in m-commerce (mobile commerce).	15%	7%	7%	22%	18%	17%	15%	50%
143	I am concerned about online shopping.	7%	9%	12%	17%	24%	16%	15%	55%
141	I am concerned about online banking.	8%	11%	11%	17%	25%	13%	15%	53%
132	If I have concerns for online privacy I adopt privacy-enhancing technologies.	2%	4%	8%	23%	25%	24%	13%	63%
136	I am concerned about the increase number of mobile devices.	10%	11%	11%	19%	17%	18%	13%	49%
128	If I have concerns for online privacy I use protection behaviors such as falsifying information.	8%	18%	13%	17%	18%	15%	10%	43%
137	I have personally been the victim of what I felt was an	24%	21%	11%	11%	15%	10%	9%	34%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
	improper invasion of privacy of my personal information.								
152	I am concerned about Facebook so I deleted my account.	32%	28%	12%	14%	5%	4%	5%	14%
138	My organization has been the victim of an improper invasion of privacy of personal information.	36%	23%	5%	18%	8%	7%	3%	18%

Eighty-five percent agreed (33% strongly agreed, 28% agreed, 24% moderately agreed) that they are concerned about viruses / spyware / malware / EXE files / multimedia files. Nine percent neither agreed nor disagreed / neutral and 6% disagreed. The percentages provided in parentheses are the combined percentage of moderately agree, agree and strongly agree. The next top privacy concerns in order of strongly agree are about the privacy of wireless access at public hot spots (76%), protecting client's data (79%), identity theft (84%), information seen or intercepted by a third party (75%), the lack of privacy rights (70%), location tracking (70%) and that personal data obtained is shared with others (82%).

If participants are concerned about their privacy they refrain from interacting with a Web site (83%), use protection behaviors such as removing personal information from lists (81%) and refusing information disclosure or transactions (79%). The survey results were found to agree with Milne, Rohm and Bahl (2004) identity protection behaviors.

It is interesting that 34% (9% strongly agreed, 10% agreed, 15% moderately agreed) have personally been the victim of what they felt was an improper invasion of privacy of their personal information. While 18% (3% strongly agreed, 7% agreed, 8% moderately agreed) said that their organization has been the victim of an improper invasion of privacy of personal information.

Privacy Concerns from Survey 2 (*N* = 315)

Respondents also provided open free-form answers in the Privacy Management Survey, which contains the above questions. These free-form answers were analyzed using NVivo, and these results are triangulated with the results from the first survey.

Privacy Concerns of Personal Information from Survey 2

I autocoded the privacy concerns of personal information from 315 respondents to my second survey in NVivo. In this analysis, the themes that emerged of the privacy concerns of personal information overwhelmingly relate to concern over access and misuse of financial-related data and identity. People are concerned about account data, whether it is their bank account, investment account or their credit card account. They are worried that their personal information will be sold or stolen and get into the wrong hands in real life or online. The unpleasant outcome could be identity theft, which could result in monetary loss. One participant speaks from experience, “I have had my bank account information stolen before & my account was ripped off.” Another response was, “I'm concerned that my personal information will be sold to other companies and individuals,

who may use the information to open a credit card, steal money from my checking account, etc." The statements provided for each theme are provided (see Tables 4.7 - 4.11).

Table 4.7

Survey 2 Statements for each Theme of Privacy Concerns of Personal Information

Concern over Access and Misuse of Financial Data
I have had my bank account information stolen before & my account was ripped off.
I worry about my bank account being hacked into.
My personal information would be used to open new credit card accounts and rack up thousands of dollars of debt for me.
I'm concerned that someone could steal my identity and gain access to money; bank accounts, investment accounts, etc.
account numbers
I (we) have numerous online bank/credit accounts.
I'm concerned that my personal information will be sold to other companies and individuals, who may use the information to open a credit card, steal money from my checking account, etc.
Monetary loss from access to bank accounts, brokerage accounts, social security, health records for nefarious purposes or identity theft
don't want my bank account info to be taken
worried about fraud on my bank account and credit cards
I have concerns that my bank account would be used to buy unauthorized things, as well as my ssn being used to open up new accounts, especially student loans.
As long as it isn't my bank information, I don't really care.
I am afraid the wrong person will abuse my credit information resulting in negative scores within my credit report.
I am mostly concerned of my credit card information being breached.
I do a lot of online shopping, mostly through very reputable vendors (Amazon) but there's always the off chance that I've been irresponsible and I'm going to wake up with my bank accounts drained and unexpected debt on my credit report etc. I worry about identity theft.
Concerned about how to figure out who has what - who has my phone number, which sites did I enter my credit card information into, etc. I interact so frequently online that it is easy to lose track of what information I supply to whom

happened to me with someone accessing my credit card information somehow.
I am concerned about credit card fraud, identity theft, and all other threats to my personhood.
Concerns about identity theft or stolen credit card information
Credit card fraud and online hackers connected to identity theft
I don't want anyone getting my credit card numbers or social security number that may be able to ruin by business.
I am concerned about losing credit card info
that it will be gotten by someone who has intentions of taking my money or running up a big credit card bill
Identity theft, credit card theft
That someone will use my credit information and use my credit cards, or steal my identity.
I do worry about my personal information, especially credit card and banking info, being abused.
I don't want my credit card information getting out

Privacy of information has been a long time concern for online shopping. One participant said, “I do a lot of online shopping, mostly through very reputable vendors (Amazon) but there's always the off chance that I've been irresponsible and I'm going to wake up with my bank accounts drained and unexpected debt on my credit report etc. I worry about identity theft.” Many people are worried about abuse of their personal information. This respondent stated that, “I do worry about my personal information, especially credit card and banking info, being abused.”

Many aspects of credit were mentioned as a privacy concern and are displayed as a project map (see Figure 4.3). These include: big credit card bill, credit accounts, credit card accounts, credit card fraud, credit card info, credit card information, credit card numbers, credit card theft, credit hacking, credit information, credit report, credit score, especially credit card and losing credit card info.

Figure 4.3. Project Map of Credit Concerns of Personal Information.

The misuse theme was communicated strongly as personal information getting into the wrong hands and identity theft. The concerns are having their credit destroyed or their identity stolen. “My concerns about the privacy of my personal information are that the information will get into the wrong hands and be put ‘out there’ for anyone to misuse” (see Table 4.8).

Table 4.8

Privacy Concern: Into the Wrong Hands, Unauthorized Access and Misuse

Wrong Hands / Unauthorized Access and Misuse
that it could get into the wrong hands
how it's in other peoples hand
I'm concerned that my personal information can get it the wrong hands
That it may fall into the wrong hands and be used in ways to destroy my credit
That it could get into the wrong hands and my identity could be stolen. Scary.
I worry it could get into the wrong hands
that it could get in the wrong hands
That it ends up in the wrong hands and that it could hurt me in many ways.
Personal information getting into the wrong hands.
My concerns about the privacy of my personal information are that the information will get into the wrong hands and be put "out there" for anyone to misuse.
stealing information
I am mostly concerned of my credit card information being breached.
I feel that any online information can eventually be hacked into; I worry constantly about my information being stolen.
Concerned about how to figure out who has what - who has my phone number, which sites did I enter my credit card information into, etc. I interact so frequently online that it is easy to lose track of what information I supply to whom.
Happened to me with someone accessing my credit card information somehow.
About people hacking into company's data information and taking my personal information, credit cards, and money
That I do not want it to end up in the wrong hands.

Identity theft "is increasingly becoming the biggest crime in the world" and is a "huge concern" participants stated. Identity theft is causing people to worry about having their information hacked. The results may lead to "monetary loss from access to bank accounts, brokerage accounts, social security, health records for nefarious purposes or identity theft." This will "cripple their financial or personal being" because "once identity

theft has occurred it's extremely difficult to fix and follows a person for life." This contributor is concerned about their safety online and in real life as they have "concerns about identity theft, loss of intellectual property, general concern over my safety both online and in real life" (see Table 4.9).

Table 4.9.

Identity Theft of Personal Information Huge Privacy Concern

Identity Theft
Identity theft (18 occurrences)
stealing my identity period!!!
identity theft is increasingly becoming the biggest crime in the world.
I worry about identity theft and theft of my financial information
Worried about hacking and identity theft
Identity theft that would cripple my financial or personal being
I don't want my personal information stolen because of identity theft
I do a lot of online shopping, mostly through very reputable vendors (Amazon) but there's always the off chance that I've been irresponsible and I'm going to wake up with my bank accounts drained and unexpected debt on my credit report etc. I worry about identity theft.
Once identity theft has occurred it's extremely difficult to fix and follows a person for life.
I worry slightly about identity theft and that someone could ruin my credit or even steal my home from me.
being stolen which may result in identity theft
Identity theft is a huge concern.
I am concerned about credit card fraud, identity theft, and all other threats to my personhood.
I would be afraid of identity theft
Monetary loss from access to bank accounts, brokerage accounts, social security, health records for nefarious purposes or identity theft
Credit card fraud and online hackers connected to identity theft
Obviously leaks and identity theft
Concerns about identity theft, loss of intellectual property, general concern over my safety both online and in real life
That it could be subject to those that have ill will and lead to identity theft

Identity theft, credit card theft
I also know that identity theft is an issue.
hacking; identity theft; losing money
I am well aware of identity theft.
What really concerns me is identity theft.
identity theft, hacking, phishing
Concerns about identity theft or stolen credit card information
Companies selling my information and identity theft.

There are many privacy concerns related to bank accounts, credit cards, medical information, children's personal information and online information. There are concerns of "how it is used, shared, and protected." People worry that their personal information will be stolen and inaccurate information will be used. One participant's comment was, "My info is out there in so many ways (hospitals have it, doctors, bill collectors, car loan, etc.) that I know there is no way to keep it all safe, no matter what each source does to protect it. We've seen large companies get hacked with ease" (see Table 4.10).

Table 4.10.

Privacy Concerns Related to Data Governance and Protection

Information Governance and Protection
Too many organizations asking for too much information.
Multitude, due to internet and the ability for anyone to find information about me online without my knowledge.
I'm concerned that they held onto confidential information for so long, for no justified reason
I think online sites ask for too much information.
I sometimes feel that online companies do not have enough security measures in place to protect consumer information.

Examples of information that participants are concerned about include: bank account, confidential information, consumer information, credit card information, credit information, data information, medical information and online information. They are concerned about people finding their information, giving away their information, using inaccurate information, having too much of their information and stealing their information. Information concerns are displayed in a project map (see Figure 4.4).

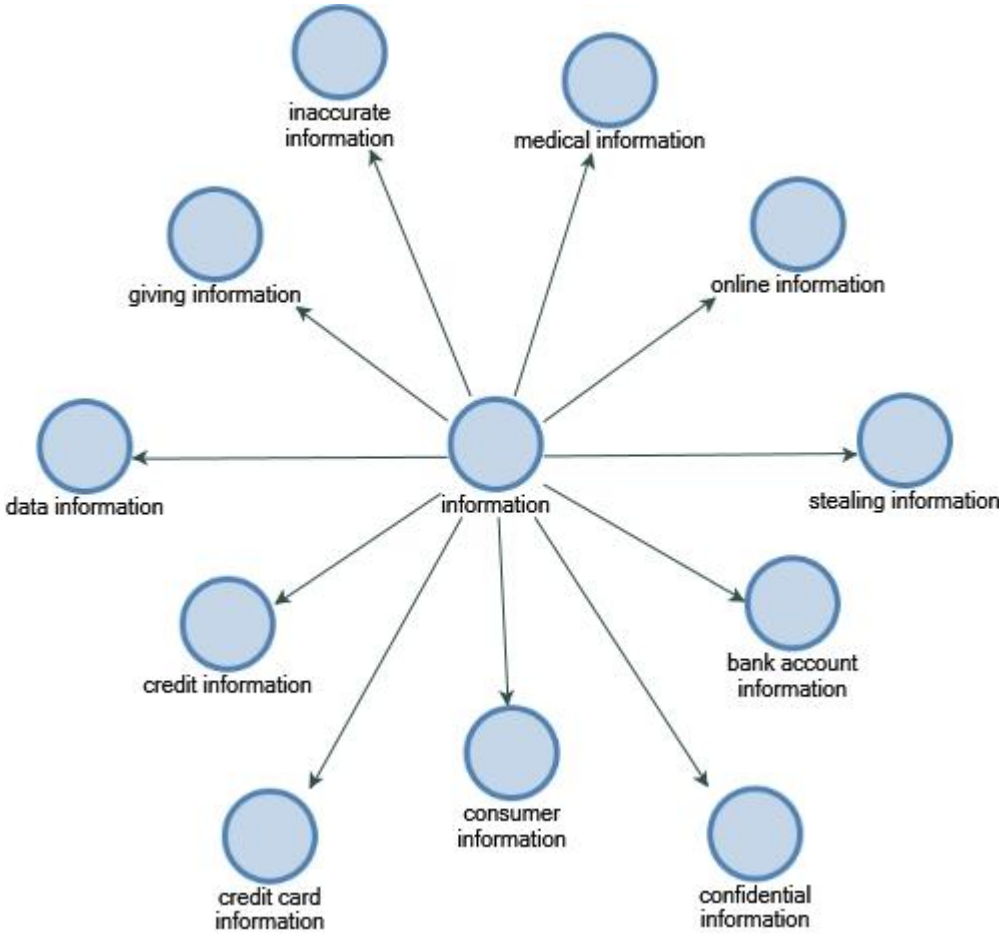


Figure 4.4. Project Map of Information Concerns of Personal Information.

People are worried about their online bank or credit account information being hacked into and stolen, which may lead to identity theft and credit card fraud. People are worried about being stalked by having their personal information accessed online. One person responded, “My address and other personal information being publicly available online makes me worry about being stalked.” The level of security protecting information online is a concern. One participant said, “I sometimes feel that online companies do not have enough security measures in place to protect consumer information.” They feel “that any online information can eventually be hacked into; I worry constantly about my information being stolen” (see Table 4.11).

Table 4.11

Online Privacy Concerns of Personal Information

Online
I do a lot of online shopping, mostly through very reputable vendors (Amazon) but there's always the off chance that I've been irresponsible and I'm going to wake up with my bank accounts drained and unexpected debt on my credit report etc. I worry about identity theft.
My address and other personal information being publicly available online makes me worry about being stalked.
I feel that any online information can eventually be hacked into; I worry constantly about my information being stolen.
I (we) have numerous online bank/credit accounts.
I have worked very hard to build this business, an entirely online business, it would be devastating to have someone learn all my personal info and use it to destroy my business/liquidate its assets.
Credit card fraud and online hackers connected to identity theft
This makes me more hesitant to share information, thereby inhibiting my online interactions.
I think online sites ask for too much information.
If signing up for something online I always try to make sure I'm not automatically

signing up for other people or companies to have any of my information.
I sometimes feel that online companies do not have enough security measures in place to protect consumer information.
I am very young and worry about my future with security online and anywhere else.

The topics discussed related to concerns online were: available online, online bank, online business, online companies, online hackers, online information, online interactions, online shopping, online sites and security online. Online concerns of personal information are displayed in a project map (see Figure 4.5).

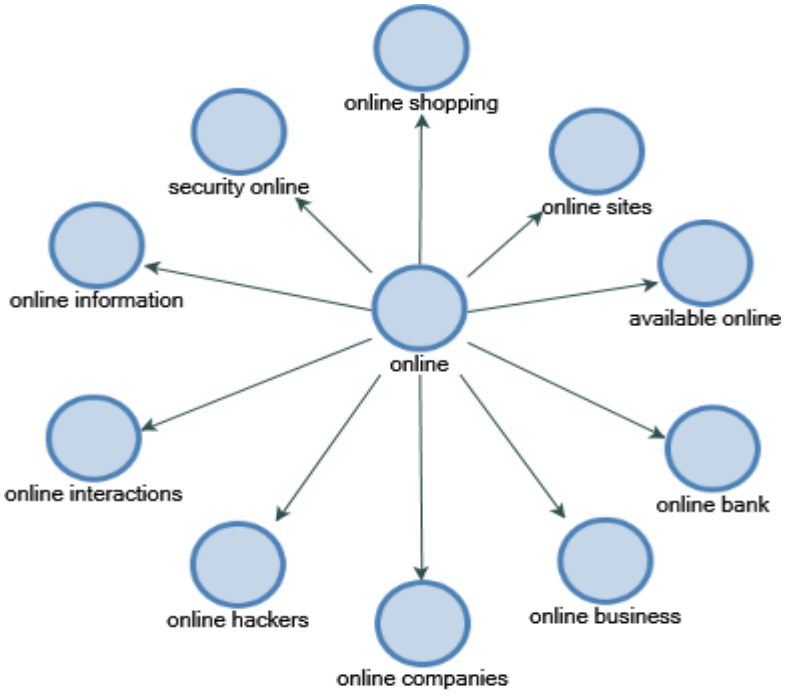


Figure 4.5. Project Map of Online Concerns of Personal Information.

Privacy Concerns from Third Data Collection (*N* = 205)

My third data collection represents a holdout sample obtained from use of the Privacy Management questionnaire (survey 2). This data is used to triangulate the results of the above two analyses i.e. analysis of qualitative data from survey 1, and qualitative data from first sample collected with survey 2.

Privacy Concerns of Personal Information on 205 surveys

I autocoded the privacy concerns of personal information gathered on 205 surveys in study 3 in NVivo. The themes that emerged are: 1) breaches 2) identity theft 3) information and 4) wrong hands. Figure 4.6 is a mind map of the privacy concerns of personal information autocoded in NVivo.

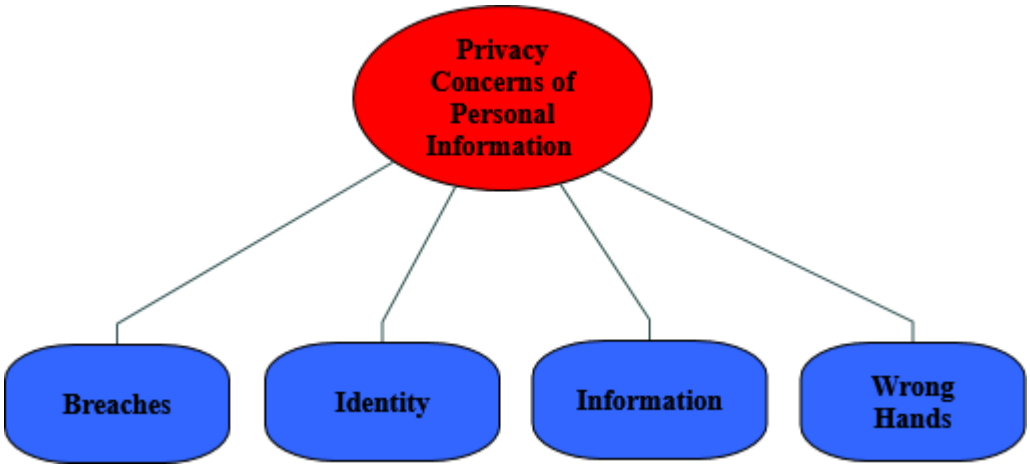


Figure 4.6. Privacy Concerns of Personal Information from Study 3.

Figure 4.7 represents a word cloud of the most frequent words used when asked, What concerns do you have about the privacy of your personal information? Some of the

concerns identified in the word frequency query are: information (55), identity (36), theft (31), personal (26), stolen (19), concerned (15), hackers (13) and credit (12).

Figure 4.7. Word Cloud of Privacy Concerns of Personal Information.

The statements supporting the four themes that emerged are provided (see Tables 4.11 - 4.14).

Breaches / Unauthorized Access

Data breaches are “always” a privacy concern of some participants. Areas of data breaches specifically mentioned were in the state’s healthcare system and on smart phones. A participant is concerned with “data breach updates and new laws.” A concern was found that breaches are not always being communicated to victims, “I'm not sure every agency is communicating breaches as they occur” (see Table 4.12).

Table 4.12

Privacy Concern Statements Regarding Breaches

Breaches / Unauthorized Access
I am always concerned about data breaches.
Especially with possible security breaches in our state`s healthcare system.
Data breach updates and new laws.
Concerned about risks to data breaches on smart phones.
I'm not sure every agency is communicating breaches as they occur.
Exactly who can see sensitive info in a company.
Someone hacking private information.

The breach nodes for privacy concerns of personal information are displayed in Figure 4.8. These are: data breaches, breach updates, communicating breaches and possible security breaches.

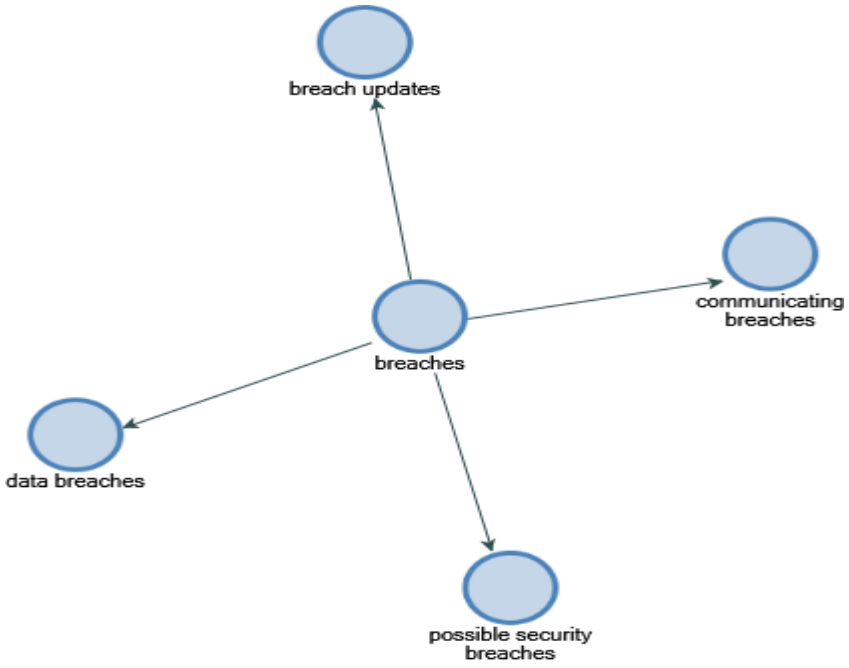


Figure 4.8. Breaches Node for Privacy Concerns of Personal Information.

Identity Theft

Identity is a theme. A "big concern" for many is harming their identity through identity theft or identity fraud. Participants are concerned of the effects from identity fraud and identity theft such as: hurting their credit rating, loss of money and assets and the time to repair the damage. Identity theft is also a worry because of the fact that you do not know who, where or when someone may access your information as one commented, "That anyone anywhere at any time could access all my personal information and commit identity theft." One participant shared their experience of being a victim of identity theft from another employee at their organization (see Table 4.13).

Table 4.13

Privacy Concern Statements Regarding Identity Theft

Identity Theft
It may lead to identity fraud and hurt my credit rating.
Identity theft (12 occurrences)
Concerns about identity theft.
I worry about becoming a victim of identity theft and losing money and assets as well as time to repair the damage.
Identity theft is a big concern.
How that information will be used and the possibility of identity theft or fraud.
I don't want to experience identity theft.
I am a victim of identity theft from another employee at my organization who indicated that she had a criminal record when she was hired.
I am concerned about protecting my name, address, credit info, and other due to the potential of everything from spammers to identity theft.
It may lead to identity fraud and hurt my credit rating.
I am concerned about the possibility of identity theft.
That it will be used for identity theft.
That anyone anywhere at any time could access all my personal information and commit identity theft

That highly sensitive personal information, such as medical information or my social security number, will be stolen and result in someone stealing my identity. Whether my credit information is correct / I had some concerns about my identity with the IRS.

The nodes of identity, identity fraud and identity theft are displayed in Figure 4.9.

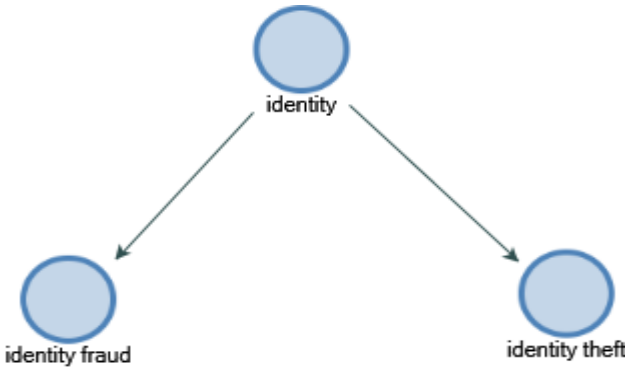


Figure 4.9. Identity Nodes for Privacy Concerns of Personal Information.

Information Misuse

Concerns about information were expressed in the form of private information, debit card information, partial information, credit information, medical information and social security number. Concerns of hacking, selling, not reporting loss of information, accessing and piecing together information are expressed in participants' statements. "Someone hacking private information" is a common concern. This person is concerned with entry-level employees' access to debit card information, "I'm concerned that debit card information is readily available most of the places it is used by entry level employees." With data mining piecing together partial information to obtain personal information is a concern, "That someone will gain partial information and piece it

together to get into my personal information." Participants are concerned that their personal information is being used and sold without their consent, "Unlawful use, sale of my personal info to third party organizations without my knowledge." Stealing highly personal information that will result in identity theft is a big concern, "That highly sensitive personal information, such as medical information or my social security number, will be stolen and result in someone stealing my identity." This person's "credit card info has been stolen before multiple times." Disposing of information properly is a concern of this person, "With information/data existing on Drives and servers permanently until destroyed I worry not only about hackers but also the proper disposal of the information/data when the entity possessing such information upgrade or replaces hardware." This person is concerned that they would not be notified if their information was stolen, "That loss of personal info would not be reported in a timely manner" (see Table 4.14).

Table 4.14

Privacy Concern Statements Regarding Information Governance and Misuse

Information Governance and Protection
I'm concerned that debit card information is readily available most of the places it is used by entry-level employees.
That someone will gain partial information and piece it together to get into my personal information.
I feel most places do a good job of protecting information.
Unlawful use, sale of my personal info to third party organizations without my knowledge.
With information/data existing on Drives and servers permanently until destroyed I worry not only about hackers but also the proper disposal of the

information/data when the entity possessing such information upgrade or replaces hardware.
Until there is a standard, information will always remain vulnerable and at risk.
That loss of personal info would not be reported in a timely manner.
I like private info to remain private.
I am concerned that if I enter my information online that the company could then sell it to anyone either legally or illegally.
Credit card info has been stolen before multiple times.

The nodes of information describe private information, protecting information, standard information, credit information, debit card information, information online, information upgrade, medical information and partial information (see Figure 4.10).

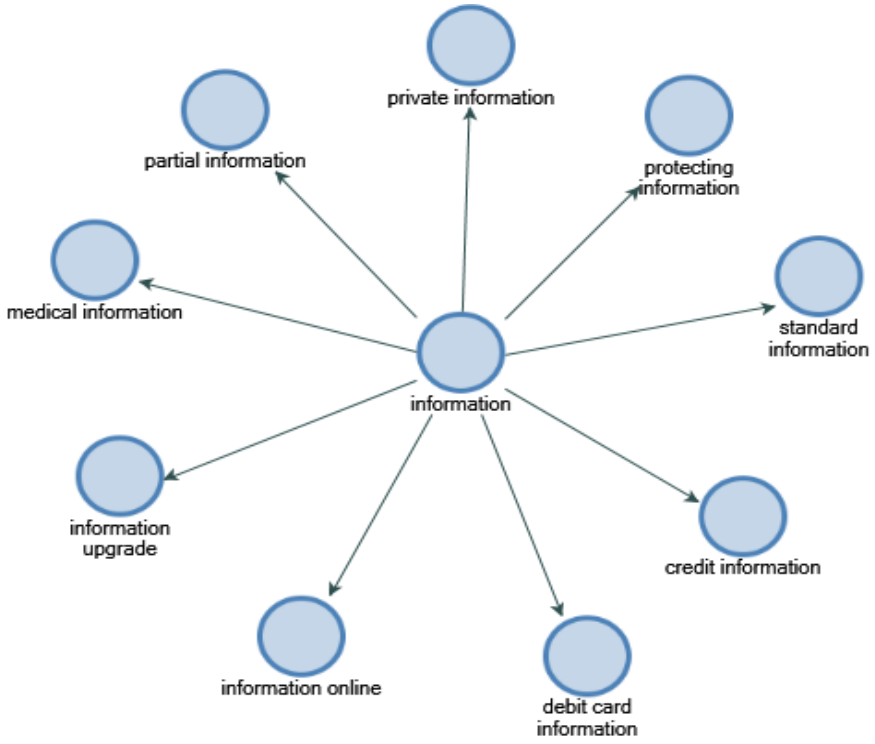


Figure 4.10. Information Nodes for Privacy Concerns of Personal Information.

A theme that developed is personal information getting into the wrong hands. One person is worried "what could happen if it gets into the wrong hands" (see Table 4.15).

Table 4.15

Privacy Concern Statements Regarding Private Information Getting Into the Wrong Hands

Wrong Hands i.e. Unauthorized Access and Use
That it will get in the wrong hands.
Being in the wrong hands or being sold.
What could happen if it gets into the wrong hands.
That it would end up in the wrong hands.
Getting in the wrong hands.
Being hacked and getting in the wrong hands.

These themes align closely with those found in the qualitative analysis of survey 1 and the first (N = 315) sample collected using survey 2.

Discussion

Three sources of qualitative data describing privacy concerns were collected and analyzed individually in this chapter. Major themes for privacy concerns are: (1) unauthorized access to private information (2) misuse of private information, particularly financial information, which is the area that is most harmed in identity theft, (3) unauthorized disclosure of private information (4) huge scope of privacy loss, and (5) need for better privacy protections. Recurring themes across data sets particularly re-emphasize unauthorized access, disclosure, and use. Two of the four subscales in Smith, Milberg & Burke's (1996) seminal *Concern for Information Privacy (CFIP) Instrument*: (1) collection; (2) unauthorized secondary use; (3) accuracy; and (4) improper access are

still found to be privacy concerns today but through a different means - the Internet and its free software platforms, which also amplifies the complexity and heavily widened scope of each concern. Collection of data was not voiced as a concern as people are resigned to the fact that data collection is happening in the background as they have exchanged their data for the convenience of using the Internet. Accuracy of data is also less of a concern today than 20 years ago, likely as we have better and cheaper means for accurate data entry to correct data than before. Similarly, the scope of errors has significantly expanded since 1996. For example, today an error may be the low-cost posting of a very large data set containing personally identifiable information by accident.

In conclusion, this study's resulting themes were helpful in informing the *Privacy-Brand Model*, which I proposed (see Chapters 2, 5, 6, and 7) in the sense that the need for privacy protections became clear as interviewee and survey respondents almost unanimously voiced such concerns around their and other people's privacy. Thus the thesis examines organizational privacy practices, privacy and security protections as a new means of brand protection, and how employees relate privacy management and brand protection to their organizations' brand value.

CHAPTER 5 – STUDY 2: PRIVACY MANAGEMENT, BRAND PROTECTION AND BRAND VALUE

Method

A positivism methodology was engaged in an online survey instrument format. This methodology was chosen to gather data to empirically test the hypotheses in this research. The value of the survey method allowed for a greater number of participants and questions than could have been accomplished through in depth interviews.

After a literature review was conducted (see Chapter 2) survey questions were developed to measure the constructs in this research (see Chapter 3). The constructs are privacy practices, privacy concerns, online brand protection, experienced harm, and brand value. Interviews were conducted with experts in the field of privacy. A hard copy survey was Ad Hoc Delphi tested for ecologic validity at conferences. Comments and suggestions were incorporated into the survey and these modifications were approved by The Saint Mary's University Research Ethics Board (REB).

The questions were then programmed into LimeSurvey by the researcher. Once the online survey was ready, email addresses were gathered at conferences of those who were interested in completing the survey as an initial sampling strategy. The link to the survey was emailed to those people. As well, the Privacy Commissioner of Nova Scotia sent the link to the survey to Privacy Colleagues across Canada for survey distribution. Other colleagues distributed the survey to their contacts. These efforts resulted in an

unacceptably low response rate and as a consequence, a professional survey company, Qualtrics, subsequently was hired to gather the survey data for surveys 2 and 3. Data was gathered from conducting three surveys (N = 260, N = 315 and N =205). SPSS and AMOS were used to analyze the quantitative data. NVivo was used to analyze the qualitative data (see Chapter 4).

Participants

The collected demographic information from the privacy management survey included: gender, level of education, age bracket by decade, country of residence, province/state where employed, profession or occupation, size of organization (number of employees).

Information was gathered related to the organization's online and mobile presence and if products or services are provided online. The type of information the organization uses, discloses or retains: credit card information, financial, medical, personal information and proprietary information.

The type of sector is disclosed: public, private or not-for-profit. The study population includes individuals who live in the United States, are employed full time and are 18 years or older. The organization uses personal information to conduct their business (see Appendix D for survey demographic information questions, and Chapter 3 and Table 4.3 for demographic results for survey 2).

Data Collection and Analysis

This research was reviewed and approved by the Saint Mary's University Research Ethics Board. Implied consent was given by participants by submission of their online survey. The data was collected in a SPSS file and also entered into Excel spreadsheets.

IBM SPSS Statistics 24, AMOS Graphics in IBM AMOS 23, and Microsoft Excel were the computer programs used to analyse the survey data. SPSS was used to do principal components analysis. AMOS Graphics was used for confirmatory factor analysis and structural equation modelling. Excel was used to create graphs for the demographic data and calculate percentages of the responses.

SPSS was used for principal components analysis. Principal components analysis (PCA) "uses the correlations among variables to develop a small set of components that empirically summarizes the correlations among the variables" (Tabachnick & Fidell, 2013, p. 25). This procedure reduced the number of variables used to create the scales and to test the hypotheses. Variables were added in SPSS and selections were made for descriptives, extraction, rotation, scores and options to perform the factor analyses according to guidelines suggested by Meyers, Gamst and Guarino (2006). KMO and Bartlett's test of sphericity was applied. Principal components was the extraction method employed. Correlation matrices were used to analyze the data. Extraction was based on Eigenvalues greater than 1 with the maximum iterations for convergence set to 25. The methods for rotation were compared using pattern matrices with Oblimin with Kaiser

Normalization (Field, 2013) and using component matrices with a varimax rotation as recommended by Meyers, Gamst & Guarino (2017). The difference between varimax and Oblimin is that varimax returns orthogonal factors and Oblimin allows the factors to not be orthogonal. PCA was chosen because I wanted an empirical summary of the data set. According to Tabachnick and Fidell (2013) varimax, a variance-maximizing procedure, is the rotation method "most commonly used" (p. 625) of the numerous rotation methods available.

There were no missing values in the data set. Small coefficients which had an absolute value below .3 were suppressed because I did not want any loadings < .5 and .3 is .2 away which is acceptable (Gaskin, 2013a). In SPSS if variables had values less than .3 in the communalities extraction column they were removed because this could cause issues correlating with other variables. The pattern matrix was analyzed to determine which variables should be eliminated from the principal components. The variables with small coefficients which had an absolute value below .7 were removed so no loadings <.7 were retained to ensure convergent validity.

"Variables presumed to measure the same construct show convergent validity if their intercorrelations are appreciable in magnitude" (Kline, 2016, p. 93). There is convergent validity because all of the variables load highly on their component in the communalities table. Over .3 is acceptable, .5 is better and the average for the factor should be ≥ .7. All

variables loaded >.7. Variables were removed if they were cross loading on different components to ensure discriminate validity. The variables with the lower loading values were also removed. Each time a variable was removed the extraction method was rerun to produce new results. Variables had to be at least > .5 to remain in the analysis. The average of the variables in each factor had to be > .7 to remain in the analysis.

"Discriminant validity is supported if the intercorrelations among a set of variables presumed to measure different constructs are not too high, but the evidence is stronger when the measures are not based on the same method" (Kline, 2016, p. 93). There is discriminate validity because there are no cross loadings within .2 (see Table 5.1).

Table 5.1

Discriminant Validity: Factor Loadings for Experienced Harms, Brand Protection, Privacy Practices, and Brand Value

	Experienced Harms	Brand Protection	Privacy Practices	Brand Value
H_COSTS	0.925			
H_TIME	0.922			
H_FINANL	0.909			
H_DBATK	0.902			
H_PRODUC	0.897			
H_ABUSE	0.887			
H_HACK	0.864			
H_SMABU	0.838			
H_STROY	0.829			
H_PWORD	0.726			
BP_H_ALN		0.856		
BP_H_BP		0.830		
BP_COMPL		0.800		
BP_PPOL		0.795		

BP_H_PPR	0.787		
BP_TR_PP	0.759		
BP_SECUR	0.755		
BP_TR_RE	0.733		
BP_ENCRY	0.729		
BP_H_PP	0.715		
PP_DISCL		0.876	
PP_FAIR		0.857	
PP_RETEN		0.829	
PP_ACCUR		0.817	
PP_SECUR		0.806	
PP_RESPO		0.779	
PP_PURPO		0.773	
PP_CONSE		0.760	
BV_ORG_B			0.829
BV_ORG_U			0.822
BV_ORG_Q			0.811
BV_ORG_G			0.789
BV_ORG_T			0.787
BV_ORG_W			0.785
BV_ORG_R			0.775
BV_ORG_C			0.712

Confirmatory factor analysis was used to evaluate construct validity. This refers to the "degree that a measure actually assesses the theoretical construct it is supposed to assess" (Meyers, Gamst & Guarino, 2006, p. 570). "In other words, construct validity represents the extent to which operationalizations of a latent construct measures the underlying theory" (St. Davčik, 2007, p. 18).

The analysis was repeated many times until criteria was met that each principal component explained at least 5% of the variance, cumulative variance was at least 75%, and Eigenvalues were greater than one (Suhr, n.d.).

The rotation of the core model converged in 5 iterations using Varimax as the rotation method as recommended by Meyers, Gamst and Guarino (2006) and Tabachnick and Fidell (2013). Principal components analyses were run and three components were extracted: privacy practices, brand protection and brand value. These three constructs are the core model to which further test constructs were added and tested. The other test constructs are privacy breaches, experienced harms, and privacy concerns. The pattern matrices were analyzed during each SPSS analysis.

It was determined that the following combination of runs (represented by X) in SPSS would be required to determine variables, components, and scales (see Table 5.2). Scales were developed for each construct Privacy Practices to Privacy Concerns (6 in all in Table 5.2) which were run and tested one at a time. Runs 1-8 represent running the model with just the (1) 3 core constructs (privacy practices, brand protection and brand value), (2) 3 core + privacy breach, (3) 3 core + experienced harms, (4) 3 core + privacy breach + experienced harms constructs, (5) 3 core + privacy concerns construct, (6) 3 core + privacy breach + privacy concerns constructs (7) 3 core + experienced harms + privacy concerns constructs, and (8) 3 core + privacy breach + experienced harms + privacy concerns constructs.

Table 5.2

SPSS Runs Required to Determine Variables, Components and Scales

	Privacy practices	**Brand protection**	**Brand value**	**Privacy breach**	**Experienced harms**	**Privacy concerns**
Scales:	X	X	X	X	X	X
1	X	X	X			
2	X	X	X	X		
3	X	X	X		X	
4	X	X	X	X	X	
5	X	X	X			X
6	X	X	X	X		X
7	X	X	X		X	X
8	X	X	X	X	X	X

Structural equation modelling (SEM) was used to analyze the structural relationships between measured variables and latent constructs using a combination of factor analysis and multiple regression analysis. This confirmatory technique was used to determine if the models are valid in AMOS (Analysis of MOment Structures) Graphics. Estimates for the parameters are calculated that fit the model based on mean and covariance structures, which make the data fit as closely as possible (UCDHSC Center for Nursing Research, 2006). Meyers, Gamst and Guarino (2006) suggested standardized estimates, modification indices and a threshold of 4 for the output options in AMOS. It was determined that the following combination of runs in AMOS would be required to build and test Privacy-Brand Models (see Table 5.3).

Table 5.3

AMOS Runs Required to Build and Test Privacy-Brand Models

	Privacy practices	**Brand protection**	**Brand value**	**Privacy breach**	**Experienced harm**	**Privacy concerns**
1	X	X	X			
2	X	X	X	X		
3	X	X	X		X	
4	X	X	X	X	X	
5	X	X	X			X
6	X	X	X	X		X
7	X	X	X		X	X
8	X	X	X	X	X	X

The privacy-brand model was analysed using structural equation modelling (SEM). Structural equation modelling, also known as path analysis or confirmatory factor analysis (CFA), are actually special types of SEM (Tabachnick & Fidell, 2013). Structural equation modelling "is a collection of statistical techniques that allow a set of relationships between one or more IVs, either continuous or discrete, and one or more DVs, either continuous or discrete, to be examined" (Tabachnick & Fidell, 2013, p. 681). The independent variables are the organization's privacy practices, online brand protection, privacy breach, experienced harm and privacy concerns. The dependent variable is brand value.

A theoretical framework was built to examine the relationships among the core privacy-brand model constructs: privacy practices, online privacy-brand protection and brand value. Privacy breaches, experienced harms, and privacy concern constructs were

added to the core privacy-brand model and tested for statistical significance. Refinements were made to the model as necessary.

Confirmatory factor analysis (CFA) assess model fit using comparative fit index (CFI) > 0.95, goodness-of-fit index (GFI) > 0.90 for good fit. Although there is no threshold level, practice suggests ≤ 0.08 for root mean square error of approximation (RMSEA) to indicate a model with a good fit (St. Davčik, 2007). Meyers et al. (2017) suggest RMSEA "values between .07 and .08 indicate a moderate fit, values between .08 and .10 indicate a marginal fit, and values in excess of .10 indicate a poor fit" (p. 517).

Results

Scale Development

"Proper scale development and validation provide the necessary foundation to facilitate future quantitative research in the organizational sciences (Wright, Quick, Hannah & Hargrove, 2017, p. 1). The following eight best practice recommendations for scale construction are provided by Wright et al. (2017):

#1: provide a theoretical justification for each scale item

#2: devote proper attention to initial scale development and content validity

#3: pilot test the preliminary scale

#4: conduct an item analysis, factor analysis, reliability analysis, and validity analysis of the preliminary scale

#5: assess reliability, validity, and factor structure of the revised scale in a new sample

#6: establish criterion validity

#7: report confidence intervals for all reliability and validity coefficients

#8: assess scale bias in the final version of the scale (p. 2)

Hinkin (1995) and Hinkin, Tracey and Enz (1997) recommend following the seven steps when constructing a scale.

Step 1: Item Generation - Create items

Step2: Content Adequacy Assessment - Test for conceptual consistency of items

Step3: Questionnaire Administration - Determine the scale for items. Determine an adequate sample size. Administer questions with other established measures

Step 4: Factor Analysis - Exploratory to reduce the set of items. Confirmatory to test the significance of the scale.

Step 5: Internal Consistency Assessment - Determine the reliability of the scale

Step 6: Construct Validation - Determine the convergent and criterion-related validity

Step 7: Replication – Repeat the scale-testing process with a new data set (p. 4).

Scales were developed for the constructs in the privacy-brand model: privacy practices, brand protection, experienced harm, privacy breach, and brand value in this chapter. Revised scales and a scale for privacy concerns is elucidated in Chapter 6. Scales with a new sample are provided in Chapter 7. Items were created and tested for content

validity with experts in the privacy and security field. The questionnaire was administered twice, with adequate sample sizes, so the scale-testing process could be repeated with a new data set. Scales were developed using exploratory and confirmatory analyses and tested for reliability using Cronbach's alpha, which is the reliability coefficient type reported most commonly in the literature (Kline, 2016). Cronbach's alpha, also called coefficient alpha, measures "internal consistency reliability, or the degree to which responses are consistent across the items of a measure" (Kline, 2016, p. 91). Tavakol and Dennick (2011) report that there are different acceptable values of alpha, ranging from 0.70 to 0.95. Scales were tested in SPSS with the variables associated with each construct. A large pool of items was included in the survey. Items were eliminated based on the results from principal components analyses until each scale was a reasonable size and Cronbach's alpha was between 0.70 to 0.95 for each scale.

Scale: Privacy Practices

A privacy practices scale was developed composed of eight statements from the *Privacy Management Survey* (N = 315). The reliability of Cronbach's alpha based on standardized items is 0.948. Item statistics and the *Privacy Practices Scale* are described in Table 5.4.

Table 5.4

Privacy Practices Scale and Item Statistics (N = 315)

#	VAR Name	Question	Mean	Std. Deviation
1	PP_DISCL	My organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.	6.30	1.278
2	PP_FAIR	My organization collects information by fair and lawful means.	6.30	1.264
3	PP_RETEN	My organization retains personal information only as long as necessary for the fulfillment of the purposes, which it was collected, except with the consent of the individual or as required by law.	6.09	1.371
4	PP_ACCUR	My organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.	6.14	1.240
5	PP_SECUR	My organization protects personal information by security safeguards appropriate to the sensitivity of the information.	6.13	1.293
6	PP_RESPO	My organization is responsible for personal information under its control	6.12	1.324
7	PP_PURPO	My organization identifies the purposes for which personal information is collected at or before the time the information is collected.	6.03	1.315
8	PP_CONSE	My organization requires the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate.	6.00	1.401

Scale: Brand Protection

A brand protection scale was developed composed of ten statements from the *Privacy Management Survey* (N = 315). The reliability of Cronbach's alpha based on standardized items is 0.950. Item statistics and the *Brand Protection Scale* are described in Table 5.5.

Table 5.5

Brand Protection Scale and Item Statistics (N = 315)

#	VAR Name	Question	Mean	Std. Deviation
1	BP_H_PP	My organization has a privacy policy.	6.18	1.257
2	BP_PPOL	My organization has policies in place to protect personal information.	5.85	1.286
3	BP_TR_PP	My organization's privacy training covers the policies and practices established by the organization.	5.80	1.573
4	BP_COMPL	My organization ensures that policies to protect personal information are put into practice each and every day.	5.71	1.453
5	BP_H_BP	My organization has best practices use for privacy.	5.69	1.484
6	BP_H_ALN	Management provides alignment of privacy policies with privacy practices.	5.63	1.522
7	BP_H_PPR	My organization has a privacy program.	5.62	1.566
8	BP_TR_RE	My organization requires all employees who access personal information to take privacy training.	5.54	1.850
9	BP_SECUR	My organization has the security necessary to ensure the ongoing protection of personal information.	5.50	1.477
10	BP_ENCRY	My organization uses encryption when storing data.	5.48	1.567

Scale: Experienced Harm

A new experienced harms scale was developed composed of ten statements from the *Privacy Management Survey* (N = 315). The reliability of Cronbach's alpha based on standardized items is 0.966. Item statistics and the *Experienced Harms Scale* are described in Table 5.6.

Table 5.6

Experienced Harms Scale and Item Statistics (N = 315)

#	VAR Name	Question	Mean	Std. Deviation
1	H_PWORD	Clients of my organization have expressed inconvenience related to changing passwords as a result of a data privacy breach.	2.68	1.746
2	H_DBATK	My organization's database of personal information has been changed maliciously.	2.13	1.514
3	H_STROY	Personal information held by my organization has been maliciously destroyed.	2.03	1.417
4	H_ABUSE	My organization has experienced digital brand abuse.	2.11	1.465
5	H_SMABU	My organization has had its brand abused on social media sites.	2.23	1.574
6	H_HACK	My organization has experienced instances of hacking.	2.57	1.802
7	H_TIME	A data breach has caused my organization to experience a loss of time.	2.35	1.736
8	H_PRODUC	A data breach has caused my organization to experience a loss of productivity.	2.38	1.763
9	H_COSTS	My organization has experienced litigation costs because of a data breach.	2.18	1.661
10	H_FINANL	My organization has experienced direct financial costs because of a data breach.	2.29	1.679

Scale: Privacy Breach

A new privacy breach scale was developed composed of six statements from the *Privacy Management Survey* (N = 315). The reliability of Cronbach's alpha based on standardized items is 0.925 (see Table 5.13). Item statistics and the *Privacy Breach Scale* are described in Table 5.7.

Table 5.7

Privacy Breach Scale and Item Statistics (N = 315)

#	VAR Name	Question	Mean	Std. Deviation
1	PB_ATTCK	My organization has had unauthorized attempts to access personal information.	2.89	1.886
2	PB_YES	My organization has experienced a data privacy breach.	2.86	1.918
3	PB_GLITC	My organization had a data breach because of system glitches.	2.65	1.767
4	PB_ATTAC	My organization had a data breach because of malicious or criminal attacks.	2.61	1.826
5	PB_EMPLO	My organization had a data breach because of employee negligence.	2.58	1.756
6	PB_MSTOL	My organization has had a mobile device (i.e. laptop) lost or stolen that contained encrypted personal information.	2.56	1.846

Scale: Brand Value

The brand value scale used in this thesis is based on a scientifically validated scale found in Barnes and Mattson (2008). A modified brand value scale was developed composed of eight statements from the *Privacy Management Survey* (N = 315). The

reliability of Cronbach's alpha based on standardized items is 0.941 (see Table 5.9). Item statistics and the

Brand Value Scale are described in Table 5.8.

Table 5.8

Brand Value Scale and Item Statistics (N = 315)

#	VAR Name	Question	Mean	Std. Deviation
1	BV_ORG_B	My organization is a good brand.	5.69	1.225
2	BV_ORG_Q	What my organization delivers feels right for	5.50	1.372
3	BV_ORG_U	The uniqueness of my organization stands out.	5.31	1.406
4	BV_ORG_W	What I get from my organization is worth the cost	5.37	1.368
5	BV_ORG_T	I feel I am able to trust my organization completely.	5.39	1.472
6	BV_ORG_G	My organization does me good.	5.57	1.368
7	BV_ORG_R	What my organization delivers feels right for me	5.52	1.336
8	BV_ORG_C	What I get from my organization is worth the cost	5.94	1.496

The variables which were eliminated from the modified brand value scale were:

BV_ORG_P	I feel great pride identifying with my organization.
BV_ORG_S	My organization is a satisfying buy.

A summary of the Reliability Statistics is provided in Table 5.9 as represented by Cronbach's Alpha. The number of items included in each scale is also provided.

Table 5.9

Reliability Statistics Summary

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Privacy practices	0.947	0.948	8
Brand protection	0.948	0.950	10
Brand value	0.940	0.941	8
Privacy breach	0.925	0.925	6
Experienced harms	0.965	0.966	10
Privacy concerns	0.958	0.959	10

Model Development

The runs listed in Table 5.3 are described next. First, I will discuss analysis of the core model constructs: privacy practices, brand protection, and brand value, and the addition of the items used in the scale for the privacy breach construct.

The four components: privacy practices, brand protection, privacy breach and brand value were analyzed using confirmatory factor analysis in AMOS. Standardized estimates were calculated (see Figure 5.1). The Beta standardized coefficients were added to the Initial Privacy-Brand Model (see Figure 5.2).

The hypothesized models were tested using IBM SPSS AMOS version 24's maximum likelihood factor analysis (Meyers, Gamst & Guarino, 2006). The scales were developed to assess privacy practices, brand protection, privacy breaches and brand protection in this initial model. The model was evaluated by four fit measures: (a) the chi square, (b) the comparative fit index (CFI), (c) the Normed fit index (NFI), and (d) the root mean square error of approximation (RMSEA). (χ^2 = 1317 (N = 315), p = .000; NFI =

.859; CFI = .900; RMSEA = .081, p = .000). The chi square had a value of 1317 (*N* = 315), *p* = .000. The CFI and the NFI are measures of relative fit comparing the hypothesized model with the null model with acceptable values ≥ .95. Both the CFI and NFI yielded values of .900 and .859, respectively, indicating a poor fit of the model. The RMSEA measures the discrepancy between the sample coefficients and the population coefficients with values closer to zero indicative of a well-fitting model. The RMSEA was .081, indicating a marginal fit since it was between .08 and .10 (Meyers et al., 2017). Acceptable absolute, relative, and parsimonious fit measures are provided in Table 5.10.

Table 5.10

Acceptable Absolute, Relative, and Parsimonious Fit Measures

Fit Measures					
Absolute indexes		Relative indexes		Parsimonious indexes	
Test	Target Value	Test	Target Value	Test	Target Value
χ^2	p > .05	CFI	≥ .95	AGFI	≥ .90
χ^2 / df	≤ 2.00**	NFI	≥ .90	PGFI>	>.50
GFI	>.95*	IFI	> .90	PNFI	>.50
RMSR	≤.05	TLI	≥ .95		
RMSEA	<.06***[1]				

Note. From *Applied Multivariate Research: Design and Interpretation* by L. S. Meyers, G. Gamst and A. J. Guarino, 2017, p. 517 (see List of Abbreviations).
*Values between .90 and .95 indicate an acceptable level of fit.
**Values up to about 5.00 may be acceptable (Bollen, 1989).
***Values between .07 and .08 indicate a moderate fit, values between .08 and .10 indicate a marginal fit, and values in excess of .10 indicate a poor fit (Browne & Cudeck, 1993; Muthén & Muthén, 2010).
[1]Dr. Deitz explained that RMSEA, which was once acceptable at .10, has been lowered.

Kline (2006) suggests reporting chi-square estimate, df, p-value, CFI, RMSEA, and SRMR (Dr. G. Deitz, personal communication, March 6, 2017). Meyers et al. (2017) prefer to report "the RMSEA, the GFI, the CFI, the IFI, and the TLI" (p. 520) along with the chi square. Iacobucci (2009) suggests not being too "overly concerned with χ^2 – it simply will not fit if the sample size is 50 or more. Instead, see if χ^2 /df is about 3 or under. Do not be overly critical if the CFI is not quite .95, or the SRMR not quite .09" (p. 95). For further information on reporting of SEM see Bentler (2007).

Estimates for the correlations between the constructs were added to the Initial Privacy-Brand Model (see Figure 5.2). Covariances were found to be statistically significant (*** $p \leq .001$) between Privacy practices and Brand protection and Privacy practices and Brand Value and Brand protection and Brand value thus supporting Hypotheses: H1, H2 and H3.

Hypothesis 1. An organization's privacy practices (PP) will be significantly and positively associated with its brand protection (BP). **H1: PP → BP**

Hypothesis 2. An organization's privacy practices (PP) will be significantly and positively associated with its brand value (BV). **H2: PP → BV**

Hypothesis 3. An organization's brand protection (BP) will be significantly and positively associated with its brand value (BV). **H3: BP → BV**

The relationships between privacy breach and privacy practices (-.08), brand protection (.10) and brand value (-.11) were low resulting in a poor fit so it was decided to exclude privacy breaches from the model. It was surmised that if people did not

experience a privacy breach then this was not important to them since only 19% agreed that their organization has experienced a data privacy breach.

Once the scales were created for privacy practices, brand protection and brand value, factor analyses were ran to create the components. Variables for privacy practices ranged between .764 to .881. Variables for brand protection ranged from .712 to .855. Variables for brand value ranged from .728 to .842 (see Table 5.1). Confirmatory factor analysis was ran in AMOS (see Figure 5.1). The standardized estimates were calculated and improved the model fit.

Chi square had a value of 1263 (N = 315), p = .000, indicating that a match was not acceptable between the proposed model and the observed data. CFI and NFI yielded values of .874 and .842, respectively, indicating a poor fit of the model. The RMSEA was .102, indicating a poor fit since it is > .10 (Meyers et al., 2017). Standardized estimates of the Confirmatory factor analysis for privacy practices, brand protection and brand value are provided in Figure 5.1.

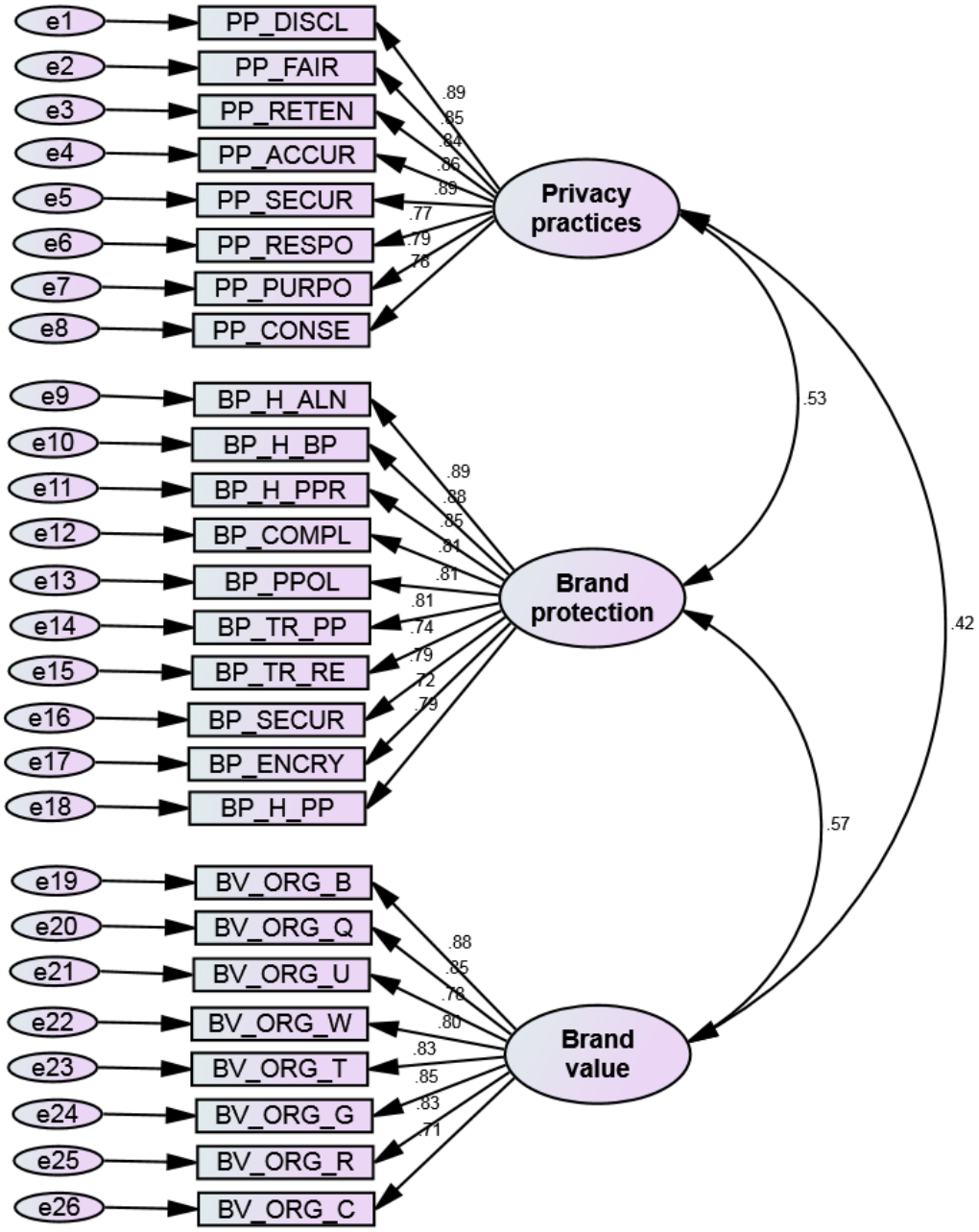


Figure 5.1. Standardized Estimates of Confirmatory Factor Analysis of Privacy Practices, Brand Protection and Brand Value After Scale Development.

The Privacy-Brand Model including Privacy Practices, Brand Protection and Brand Value, after scale development, is shown in Figure 5.2.

Figure 5.2. Privacy-Brand Model including Privacy Practices, Brand Protection and Brand Value.

Privacy breaches were added and factor analysis was run in SPSS. It was decided to omit PB_REPY from the privacy breaches scale since its value was only .688. The privacy breach scale was rerun in SPSS for 6 variables, which ranged from .786 to .892. Standardized estimates of confirmatory factor analysis of privacy practices, brand protection, privacy breach and brand value, after scale development, are provided in Figure 5.3 (χ^2 = 1590, (*N* = 315), p = .000; NFI = .836; CFI = .877; RMSEA = .089, p= <.001). The CFI and NFI yielded values of .877 and .836, respectively, indicating a poor fit of the model. The RMSEA was .089, indicating a marginal fit since it is between .08 and .10 (Meyers et al., 2017).

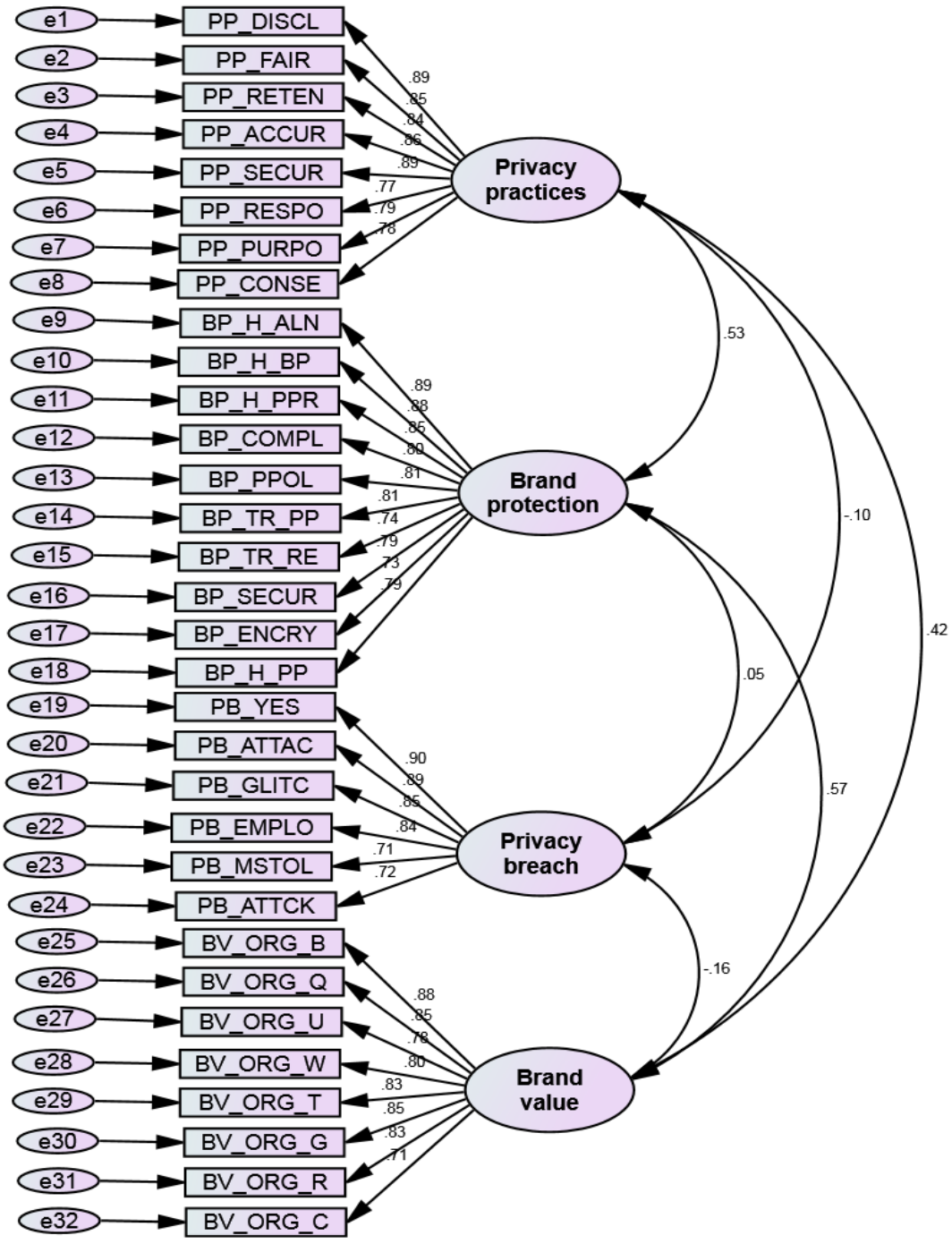


Figure 5.3. Standardized Estimates of Confirmatory Factor Analysis of Privacy Practices, Brand Protection, Privacy Breach and Brand Value.

Estimates for the correlations between the constructs were added to the Initial Privacy-Brand Model (see Figure 5.4).

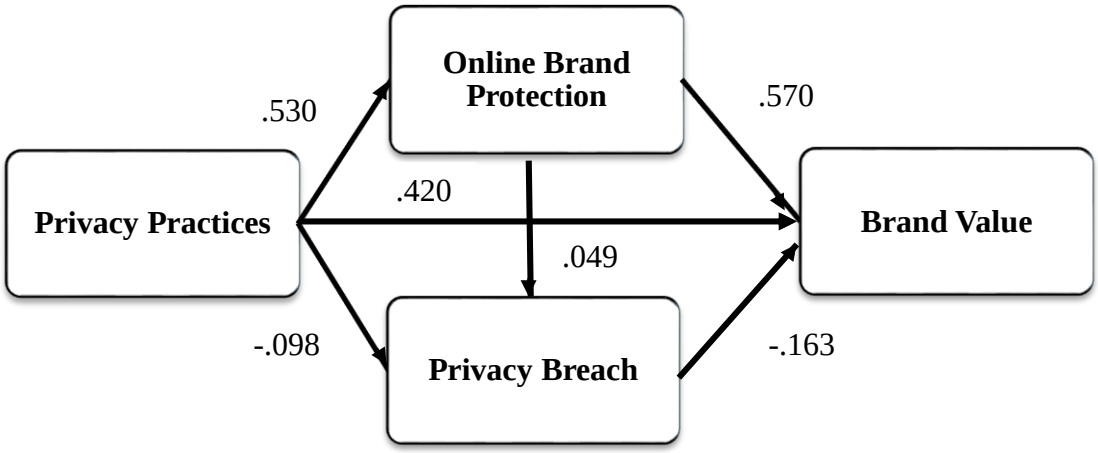


Figure 5.4. Privacy-Brand Model including Privacy Practices, Brand Protection, Privacy Breach and Brand Value.

Based upon the poor fit of the model I chose to exclude privacy breach. This is justified as only 19% of respondents reported a breach in their organization and such the perceived valence might be surmised to be low. I proceeded to retest the model by adding experienced harms, which included ten variables. Factor analysis was run and loadings ranged from .726 to .925. Standardized estimates of confirmatory factor analysis of privacy practices, brand protection, experienced harms, and brand value, after scale development, are provided in Figure 5.5 ($\chi^2 = 2243$, ($N = 315$), p = .000; NFI = .819; CFI = .859; RMSEA = .095, p= <.001). The CFI and NFI yielded values of .859 and .819,

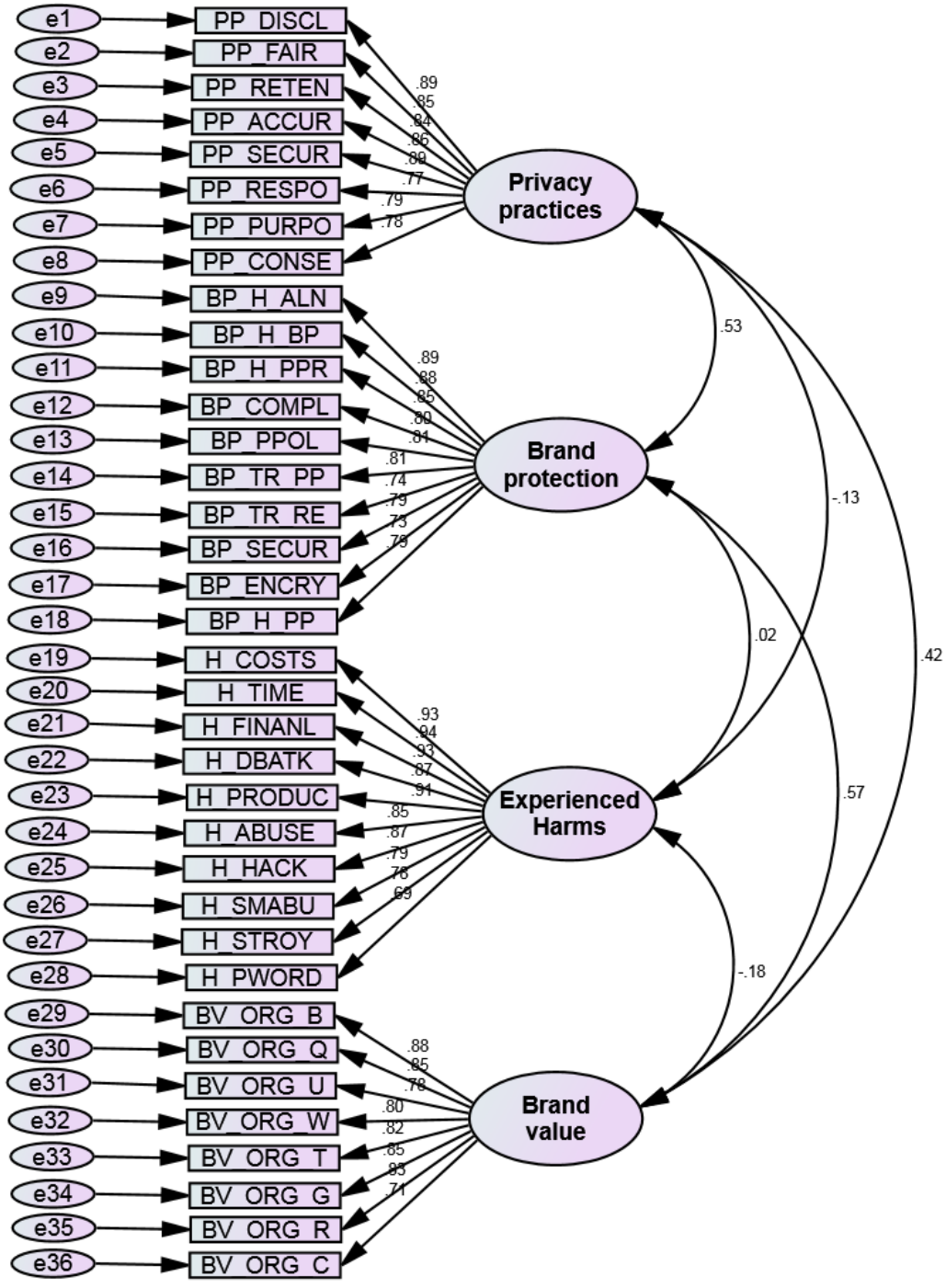


Figure 5.5. Standardized Estimates of Confirmatory Factor Analysis of Privacy Practices, Brand Protection, Experienced Harms, and Brand Value.

respectively, indicating a poor fit of the model. The RMSEA was .095, indicating a marginal fit since it is between .08 and .10 (Meyers et al., 2017).

The Privacy-Brand Model including Privacy Practices, Brand Protection, Experienced Harms, and Brand Value is provided in Figure 5.6.

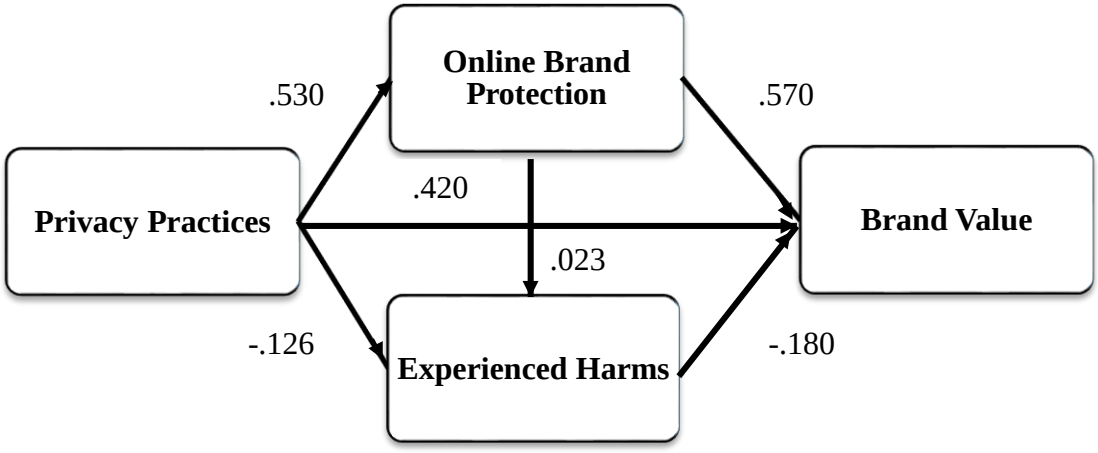


Figure 5.6. Privacy-Brand Model with Standardized Estimates from Confirmatory Factor Analysis.

Discussion

Scales have been created. Theoretical justification for each scale item has been explained in the literature review in Chapter 2 and in the development in the survey instrument in Chapter 3. Proper attention has been devoted to initial scale development and content validity has been provided by experts' opinions. A pilot test was conducted of the survey instrument which included the preliminary scale items. Item analysis, factor analysis, reliability analysis, and validity analysis of the preliminary scale was conducted. Reliability, validity, and factor structure of the revised scale in a new sample is discussed in Chapters 6 and 7.

Components were extracted using principal components analyses with the Varimax extraction method in SPSS. The components examined in this chapter are: privacy practices, brand protection, brand value, privacy breach, and experienced harms. AMOS was used to make confirmatory factor analysis with standardized estimates. Analyses have led to a provisionally accepted privacy-brand model with privacy practices, brand protection and brand values. The survey statements related to the variables used in the model are provided in Tables 5.8, 5.11, 5.14, 5.17 and 5.20.

Privacy concerns will be added in Chapter 6 for the expanded privacy-brand model. Beliefs, behaviors, privacy classification, risk and training will be analyzed during future research.

Hypotheses

Hypothesis 1. An organization's privacy practices (PP) will be significantly and positively associated with its brand protection (BP). **H1: PP → BP**

Hypothesis 2. An organization's privacy practices (PP) will be significantly and positively associated with its brand value (BV). **H2: PP → BV**

Hypothesis 3. An organization's brand protection (BP) will be significantly and positively associated with its brand value (BV). **H3: BP → BV**

Hypothesis 4. An organizations' privacy practices (PP) will be significantly and negatively associated with experienced harms (EH). **H4: PP → -EH**

Hypothesis 5. An organizations' efforts at brand protection (BP) will be significantly and negatively associated with experienced harms (EH). **H5: BP → -EH**

Hypothesis 6. An organization's experienced harms (EH) will be significantly and negatively associated with brand value (BV). **H6: EH → -BV**

Table 5.11

Summary of Statistically Significant Relationships of Hypotheses

Hypothesis				Estimate	S.E.	C.R.	P
H1	Privacy practices	↔	Brand protection	.672	.094	7.151	***
H2	Privacy practices	↔	Brand value	.558	.091	6.133	***
H3	Brand protection	↔	Brand value	.800	.106	7.586	***
H4	Privacy practices	↔	Experienced harms	-.222	.104	-2.126	.033
H5	Brand protection	↔	Experienced harms	.044	.109	.400	.689
H6	Brand value	↔	Experienced harms	-.350	.117	-2.984	.003

Note: P < 0.05 *, P < 0.01 **, P < 0.001 ***

H1. There is a statistically significant relationship (*** $p \leq .001$) between Privacy practices and Brand protection.

H2. There is a statistically significant relationship (*** $p \leq .001$) between Privacy practices and Brand value.

H3. There is a statistically significant relationship (*** $p \leq .001$) between Brand protection and Brand value.

H4. There is a statistically significant relationship (* $p \leq .05$) between Privacy practices and Experienced harms.

H5. There is not a significant relationship between Brand protection and Experienced harms.

H6. There is a statistically significant relationship (** $p \leq .01$) between Experienced harms and Brand value.

H1, H2 and H3 were found to be statistically significant (*** $p \leq .001$) while H4 was found to be statistically significant (* $p \leq .05$) and H6 was found to be statistically significant (** $p \leq .01$). H5 was found not to be statistically significant.

CHAPTER 6 – STUDY 3: EXPANDED MODEL WITH PRIVACY CONCERNS

In this chapter, the proposed privacy-brand value model from Chapter 5 is now extended with the addition of the privacy concerns construct. These privacy concerns are explained with percentage findings from the *Privacy-Management Survey*. A scale is developed for privacy concerns and hypotheses related to privacy concerns are tested.

Expanded Privacy-Brand Model

Privacy concerns were added onto the Initial Privacy-Brand Model creating an Expanded Privacy-Brand Model (see Figure 6.1).

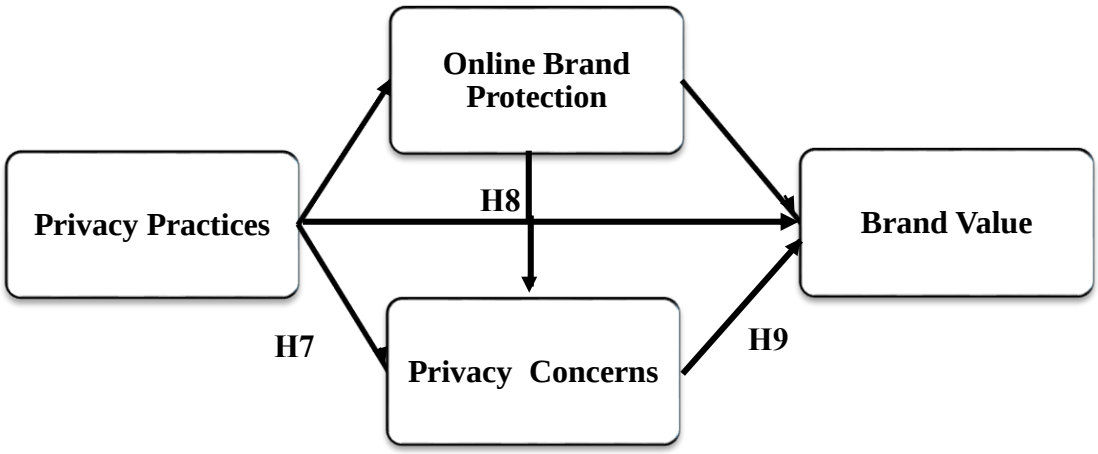


Figure 6.1. Expanded Privacy-Brand Model including Privacy Practices, Brand Protection, Privacy Concerns and Brand Value.

Hypothesis 7. An organization's privacy concerns will be significantly and positively associated with its privacy practices. **H7: PP → PC**

Hypothesis 8. An organization's privacy concerns will be significantly and positively associated with its brand protection. **H8: BP → PC**

Hypothesis 9. An organization's brand value will be significantly and positively associated with its privacy concerns. **H9: PC → BV**

Method

A mixed method approach of interpretivism and positivism methodologies were employed to both explore and test participants' privacy concerns. Open-ended questions were used to gather the concerns of one's privacy online. Statements of privacy concerns were collected in the *Preliminary Privacy Concerns Survey* (McLeod & McLeod, 2011) and in the *Privacy Management Survey* and were discussed in detail in Chapter 4. The privacy concerns collected in study 1 were included as statements on the *Privacy Management Survey* in study 2 to gather data to empirically test the hypotheses discussed in Chapter 2. SPSS was used to run principal components analyses. These factors were entered into AMOS to run model fits during confirmatory factor analyses.

Participants

For a description of participants (N = 315) for study 2 see Table 4.3.

Data Collection and Analysis

See Chapter 4 for a description of the data collection for study 2.

During analyses model fits were determined to be good if GFI, NFI and CFI statistics were equal to or above 0.90, AGFI above 0.90, and RMSEA below 0.08 (St. Davčik, 2014). See Table 5.10 for good, acceptable, moderate, marginal, and poor fits according to Meyers et al., (2017).

Convergent validity for the subconstructs is determined if: (1) item lambda coefficients are above 0.70. (2) each path is significant (3) each path loading is greater than twice its associated standard error. Discriminant validity is met if the intercorrelations between pairs of latent variables are less than 0.60.

Results

Privacy Concerns

A summary of the privacy concerns collected on the *Privacy Management Survey* using a 7-point Likert Scale from Strongly Disagree to Strongly Agree are provided in Figure 6.2.

The following concerns were measured via 48 statements on the *Privacy Management Survey*. This section summarizes the results and provides advice on how to avoid these privacy concerns.

It was found that viruses / spyware / malware / EXE files / multimedia files were the top privacy concern by 85% (moderately agreed, agreed and strongly agreed combined) of participants. It is advised not to open emails or click on links in emails that you are not familiar with the sender. This is a common way viruses / spyware / malware / EXE files are executed. This concern was closely followed by identity theft (84%).

Privacy Concerns

- Viruses/spyware/malware/EXE files/multimedia files
- Identity theft
- Personal data obtained is shared with others
- Protecting client's data
- No way to tell if personal data being stored is secure
- Personal information is readily available
- Risks are not communicated to the public
- Lack of privacy control online
- Mobile privacy
- Increase number of mobile devices
- Wireless access at public hot spots
- Privacy of passwords
- Information seen or intercepted by a third party
- Online registration is easily compromised
- Lack of privacy rights
- Location tracking
- Personal information is accessed without permission
- Tracking purchase habits concerned
- Personal information is used without permission
- Network traffic is leaking private data
- Government having their personal information
- People with personal data do not care about its security
- Privacy online is an illusion, it does not exist
- Export of data to jurisdictions with lax privacy laws
- Someone may hijack their account and ruin their reputation
- Photographs online
- Wireless access at home
- Email messages
- Someone may hijack their system and perform illegal activities where their system is the only traceable element
- Wanted their personal information protected they would not put it online
- Online credit card transactions
- Online shopping
- Online banking
- Wireless access at work

Figure 6.2. Privacy Concerns Summary.

Steps the USA.gov site suggests that you can take to protect yourself from identity theft.

> (1) Secure your social security number. (2) Don't respond to unsolicited requests for personal information (your name, birthdate, social security number, or bank account number) by phone, mail, or online. (3) Watch out for "shoulder surfers." Shield the keypad when typing your passwords on computers and at ATMs. (4) Collect mail promptly. Ask the post office to put your mail on hold when you are away from home. (5) Pay attention to your billing cycles. If bills or financial statements are late, contact the sender. (6) Review your receipts. Ask for carbon copies and incorrect charge slips as well. Promptly compare receipts with account statements. Watch for unauthorized transactions. (7) Shred receipts, credit offers, account statements, and expired cards, to prevent "dumpster divers" from getting your personal information. (8) Store personal information in a safe place at home and at work. (9) Install firewalls and virus-detection software on your home computer. (10) Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases (11) Order your credit report once a year and review to be certain that it doesn't include accounts that you have not opened. Check it more frequently if you suspect someone has gained access to your account information (USA.gov, n.d.).

It was discovered that if there are concerns for online privacy 83% will refrain from interacting with a Web site. This is a strong deterrent for electronic commerce.

Eighty-two percent of respondents are concerned that personal data obtained is shared with others. If there are concerns for online privacy 81% use protection behaviors such as removing personal information from lists and 79% are refusing information disclosure or transactions. Andrade, Kaltcheva and Weitz (2002) found that the concern for self-disclosure was alleviated by the completeness of a privacy policy and the company's reputation while being offered a reward intensified the concern for self-disclosure.

There were 79% who are concerned about protecting client's data and 78% concerned that there is no way to tell if personal data being stored is secure. Securing data is an important measure that is necessary for the protection of personal information. Proper physical barriers should be installed such as locked access to servers etc. As well as network security by installing firewalls, end point monitoring software, usernames, and passwords. These are just a few suggestions, a Security expert said that this would be a four hour lecture. Security should be included in your privacy policy to reassure clients that data being stored is secure to relieve this privacy concern.

Although Dinev and Hart (2004) found that the "perceived ability to control information may not be a major factor in mitigating privacy concerns when Internet transactions are involved" (p.420) I found that 77% are concerned about the lack of

privacy control online. Seventy-seven percent are also concerned that personal information is readily available, that risks are not communicated to the public; and are concerned about mobile privacy. Consider adding a security measure to your mobile device especially since these devices can be easily lost or stolen. Fourteen percent of the organizations had a mobile device (i.e. laptop) lost or stolen that contained encrypted personal information and 11% had a mobile device lost or stolen that contained unencrypted personal information.

If you choose the finger scan method have a backup password. My android phone locked me out permanently after not recognizing my finger on multiple attempts. The cell phone could not be unlocked by Samsung either. The backup password was the only way to unlock it. I have since switched to a numerical code to unlock my phone. Forty-nine percent were concerned about the increase number of mobile devices.

It was found that 76% are concerned about the privacy of wireless access at public hot spots. Wireless access at public hot spots is something that users should be aware that is not private and should not work with personal information without having their own protective measures in place. Privacy expectations at home, work and public hot spots were researched in the first study (see McLeod & McLeod, 2011).

There were 75% concerned about privacy of passwords and about information seen or intercepted by a third party. If there is a data breach passwords should be changed as soon as possible. Passwords created should be complex not simple words. It is

recommended to have passwords of 12 characters or greater. A password of 15 characters is virtually uncrackable. Using a password manager or password vault to store passwords in are worth considering. Some password managers to consider are LastPass, 1Password and Dashlane (New York Times, 2016).

Seventy-one percent were concerned that online registration is easily compromised. This may prevent the use of online sites if online registration is necessary.

Seventy percent were concerned about the lack of privacy rights and location tracking. With the increasing use of GPS by personal users and rental car companies' location tracking is becoming more of a privacy concern.

Personal information is accessed without permission and tracking purchase habits concerned 68% of respondents. There are many reward programs in place, which track purchases such as Air Miles.

Sixty-seven percent were concerned that their personal information is used without permission and that network traffic is leaking private data. The government having their personal information concerned 66% of participants. If they do not have concerns for online privacy 66% use their personal information.

Sixty-five percent were concerned about people who have personal data do not care about its security; agreed that privacy online is an illusion, it does not exist and were concerned about the export of data to jurisdictions with lax privacy laws. Organizations

who store their personal information in a secure, reputable jurisdiction should promote this fact to relieve this concern for many.

Sixty-four percent were concerned that someone may hijack their account and ruin their reputation; and concerned about the privacy of their photographs online. It is encouraging to realize that privacy-enhancing technologies are adopted by 63% if they have concerns for online privacy. Sixty-two percent were concerned about the privacy of wireless access at home. 61% were concerned about the privacy of my email messages and are concerned that someone may hijack their system and perform illegal activities where their system is the only traceable element.

Fifty-seven percent agreed that if they wanted their personal information protected they would not put it online. One piece of advice that I will pass along that an Engineer gave me ten years ago, during a discussion about privacy, was not to put anything on the Internet that you would not want to see on the front page of a newspaper.

There were 57% concerned about online credit card transactions. An alternative to using a credit card online is to setup an account such as PayPal to pay online. This may also help the 55% who are concerned about online shopping. Even with all the guarantees that many of the financial institutions have in place 53% are concerned about online banking. Personally I find online banking to be very convenient.

Half of the participants were concerned about the privacy of wireless access at work. There were 43% who have concerns for online privacy use protection behaviors such as

falsifying information. It was found that 34% have personally been the victim of what they felt was an improper invasion of privacy of their personal information. Eighteen percent of their organizations have been the victim of an improper invasion of privacy of personal information. There were 14% concerned about Facebook and deleted their account.

During one analysis four components were created for privacy concerns using principal components analysis in SPSS. Themes have been assigned to variables related to privacy concerns and the related survey statements. These components are: Privacy Conscious Aware, Tradeoffs Tolerant, Social Networking / Online Privacy Pragmatic and Breach Aware.

Under the theme Privacy Conscious Aware the survey statements included “I read license agreements fully before I agree to them.” and “I read a website’s privacy policy before I register my information.”

Under the theme Tradeoffs Tolerant the survey statements are: I feel that privacy policies and privacy practices in my organization are not aligned. I feel there are gaps between privacy practices and privacy training in my organization. I am willing to provide my personal information in exchange for convenience. I am willing to provide my personal information in exchange for money.

Social Networking / Online Privacy Pragmatic theme statements included I am engaged in social networking over the Internet. I use the privacy settings in social

networking over the Internet. I believe that privacy training helps to protect my organization's brand. I am sensitive to online information privacy concerns.

In the theme Breach Aware the statements included I am aware that Employment and Social Development Canada has a hard drive missing that contained the Social Insurance number, name, date of birth, home address, telephone number, loan amounts and balances for more than half a million student loan recipients from 2000 to 2006. I am aware of the privacy breach in 2007 at the parent company of TJ Maxx that affected 90 million records.

Scale: Privacy Concerns

Forty-eight statements on the *Privacy Management Survey* for privacy concerns with a Cronbach's alpha based on standardized items = 0.968 have been reduced to 10 variables to make a new privacy concerns scale. The reliability of Cronbach's alpha based on standardized items is 0.959 (N = 315). Item statistics for the *Privacy Concerns Scale* are provided in Table 6.1.

Table 6.1

Privacy Concerns Scale (N = 315)

#	Privacy Concern Variable	Statement	Mean	Std. Deviation
1	PC_WIRPB	I am concerned about the privacy of wireless access at public hot spots.	5.43	1.611
2	PC_SHARE	I am concerned that personal data obtained is shared with others.	5.43	1.344
3	PC_PIAVL	I am concerned that personal information is readily available and that risks are not communicated to the public.	5.32	1.465
4	PC_PASWD	I am concerned about privacy of passwords.	5.28	1.588
5	PC_RIGHT	I am concerned about the lack of privacy rights.	5.25	1.557
6	PC_LOCAT	I am concerned about location tracking.	5.15	1.661
7	PC_REGIS	I am concerned that online registration is easily compromised.	5.09	1.550
8	PC_EXPOR	I am concerned about export of data to jurisdictions with lax privacy laws.	5.04	1.578
9	PC_NETTR	I am concerned that network traffic is leaking private data.	4.98	1.581
10	PC_REPUT	I am concerned that someone may hijack my account and ruin my reputation.	4.93	1.682

Principal components analysis was the extraction method used in SPSS. Varimax was the rotation method, which converged in 6 iterations. The rotated component matrix for privacy concerns, privacy practices, brand protection and brand value was analyzed. Privacy concerns, which included ten variables, ranged from .749 to .893.

Standardized estimates of confirmatory factor analysis of privacy practices, brand protection, privacy concerns and brand value, after scale development, are provided in Figure 6.3 (χ^2 = 1896, (*N* = 315), p = .000; NFI = .835; CFI = .880; RMSEA = .084, p= <.001). The CFI and NFI yielded values of .880 and .835, respectively, indicating a poor fit of the model. The RMSEA was .084, indicating that it was a marginal fit since it was between .08 and .10 (Meyers et al., 2017). The *Expanded Privacy-Brand Model* including Privacy Practices, Brand Protection, Privacy Concerns and Brand Value is provided in Figure 6.4.

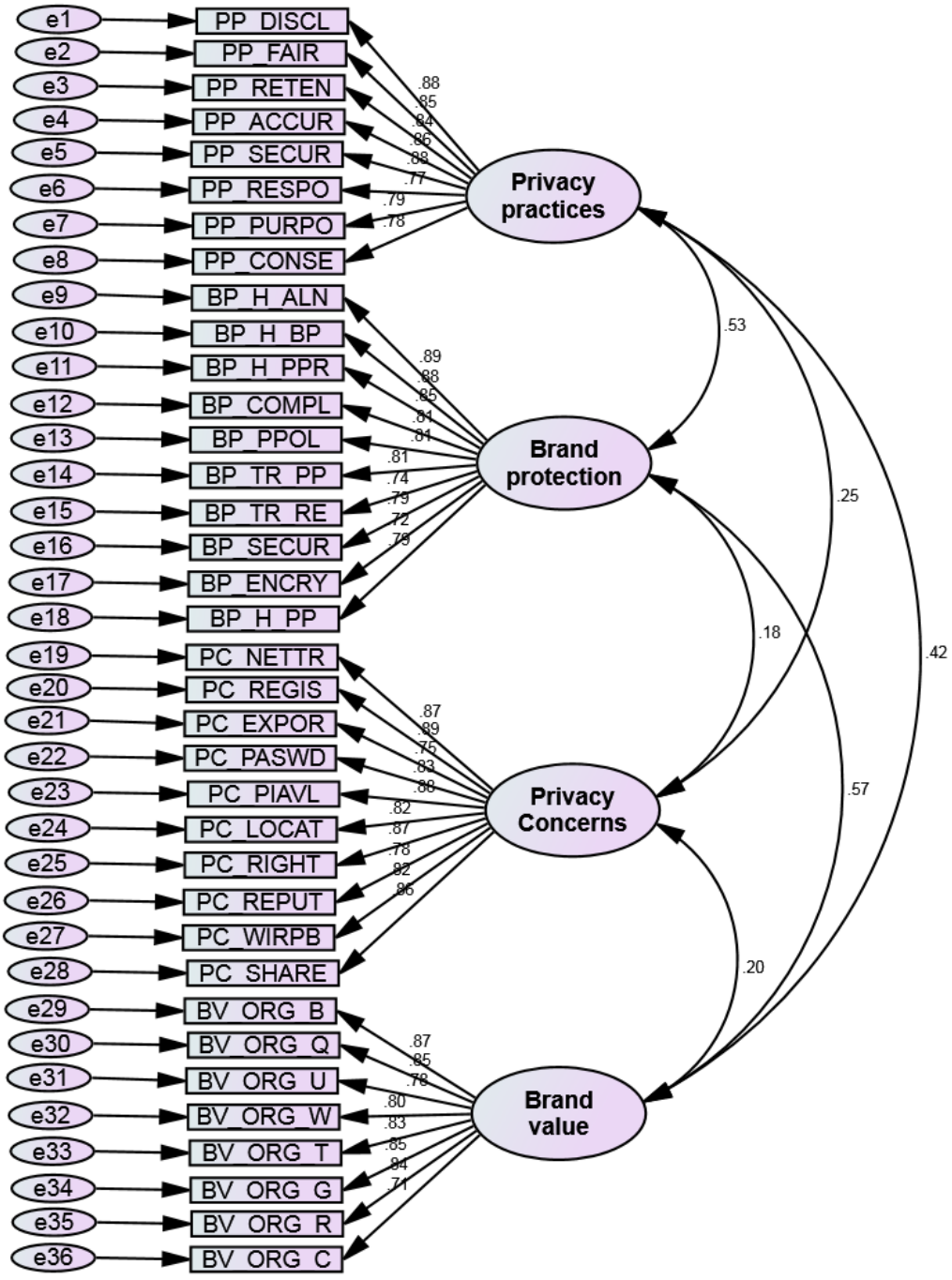


Figure 6.3. Privacy Concerns Added to Privacy Practices, Brand Protection and Brand Value Confirmatory Factor Analysis.

Expanded Privacy-Brand Model

Estimates for the correlations between the constructs were added to the Expanded Privacy-Brand Model (see Figure 6.4). The only relationship that was not found statistically significant at (*** $p \leq .001$) was between brand protection and privacy concerns (** $p = .003$).

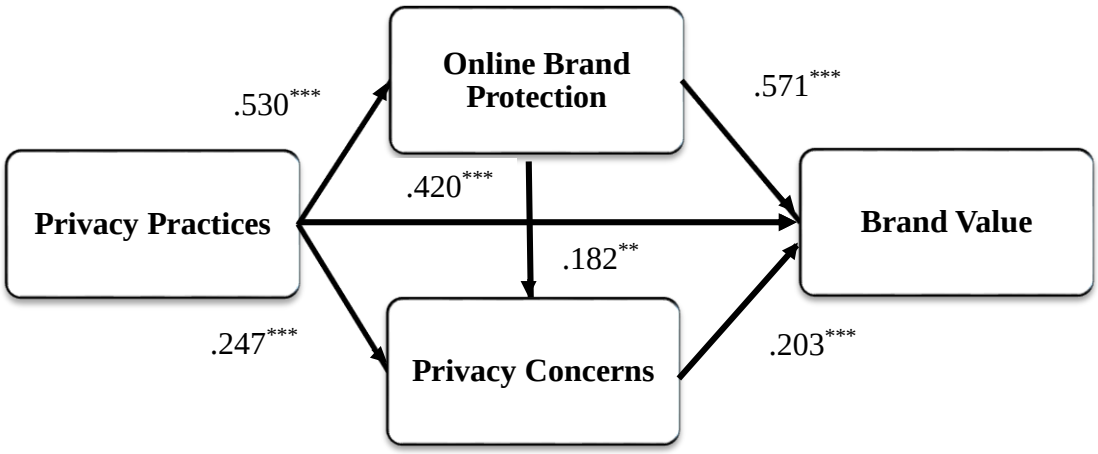


Figure 6.4. Expanded Privacy-Brand Model including Privacy Practices, Brand Protection, Privacy Concerns and Brand Value.

Privacy breaches were added and standardized estimates of the confirmatory factor analysis of privacy practices, brand protection, privacy concerns, privacy breach and brand value, are provided in Figure 6.5 ($\chi^2 = 2295$, ($N = 315$), p = .000; NFI = .827; CFI = .881; RMSEA = .076, p= <.001). The CFI and NFI yielded values of .881 and .827, respectively, indicating a poor fit of the model. The RMSEA was .076, indicating a moderate fit since it is between .07 and .08 (Meyers et al., 2017).

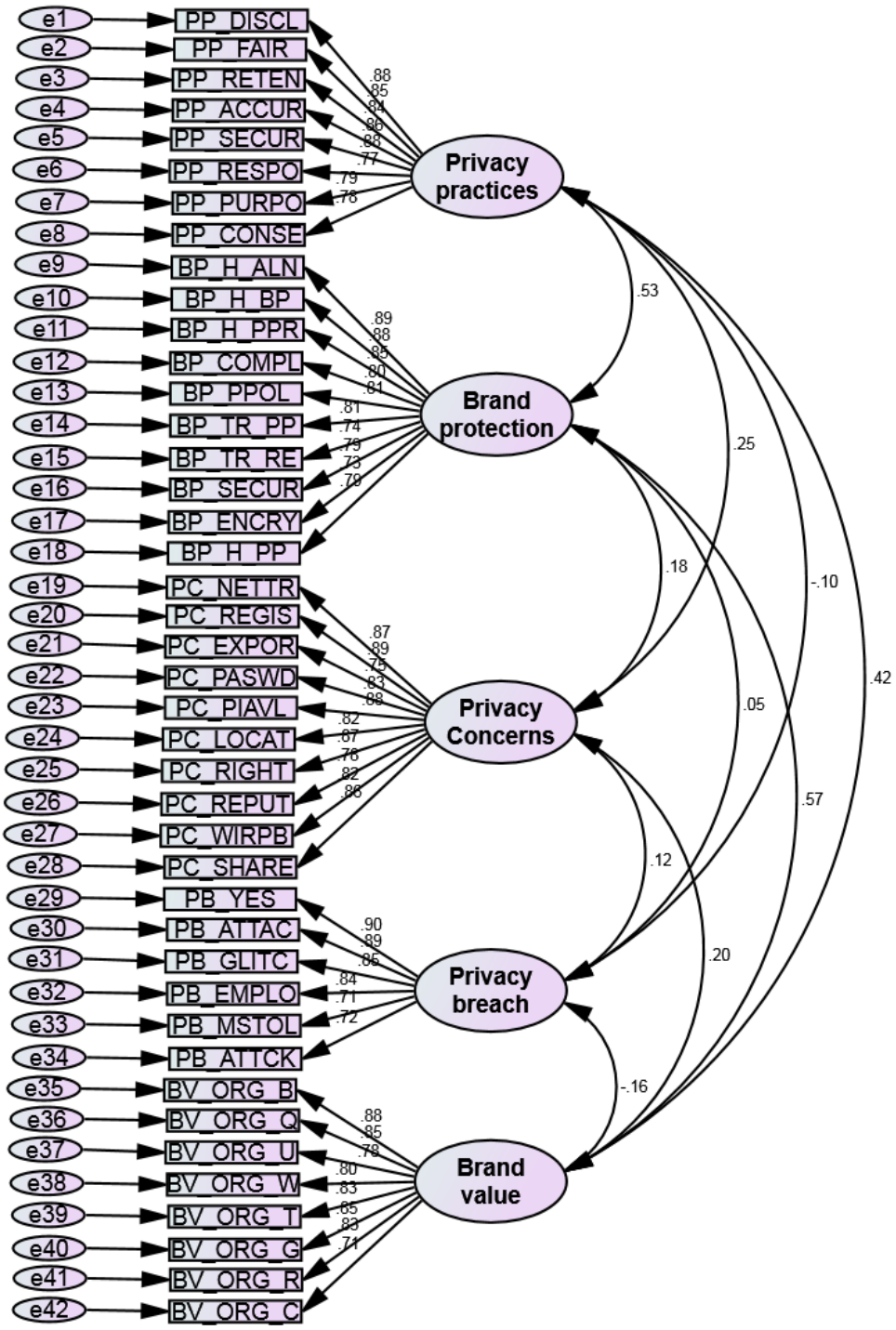


Figure 6.5. Privacy Breach Added to Privacy Practices, Brand Protection, Privacy Concerns and Brand Value Confirmatory Factor Analysis.

Experienced harms were added and standardized estimates of the confirmatory factor analysis of privacy practices, brand protection, privacy concerns, experienced harms, and brand value, are provided in Figure 6.6 (χ^2 = 2682, (*N* = 315), p = .000; NFI = .824; CFI = .875; RMSEA = .080, p= <.001). The CFI and NFI yielded values of .875 and .824, respectively, indicating a poor fit of the model. The RMSEA was .08, indicating a moderate fit (Meyers et al., 2017).

Standardized estimates of the confirmatory factor analysis of privacy practices, brand protection, privacy concerns, privacy breach, experienced harms, and brand value, are provided in Figure 6.7 (χ^2 = 3359, (*N* = 315), p = .000; NFI = .810; CFI = .866; RMSEA = .078, p= <.001). The CFI and NFI yielded values of .866 and .810, respectively, indicating a poor fit of the model. The RMSEA was .078, indicating a moderate fit since it is between .07 and .08 (Meyers et al., 2017).

Hypotheses

Hypothesis 7. An organization's privacy practices (PP) will be significantly and positively associated with its privacy concerns (PC). **H7: PP → PC**

Hypothesis 8. An organization's brand protection (BP) will be significantly and positively associated with its privacy concerns (PC). **H8: BP → PC**

Hypothesis 9. An organization's privacy concerns (PC) will be significantly and positively associated with its brand value (BV). **H9: PC → BV**

There is a statistically significant relationship between Privacy practices and Privacy concerns (*** $p \leq .001$). There is a statistically significant relationship (** $p \leq .01$) between Brand protection and Privacy concerns. There is a statistically significant relationship between Brand value and Privacy concerns (*** $p \leq .001$) (see Table 6.2).

Table 6.2

Statistically Significant Relationships of Privacy Concerns Related Hypotheses

				Estimate	S.E.	C.R.	P
H7	Privacy practices	↔	Privacy concerns	.350	0.088	3.992	***
H8	Brand protection	↔	Privacy concerns	.273	0.091	3.011	.003
H9	Brand value	↔	Privacy concerns	.319	0.096	3.329	***

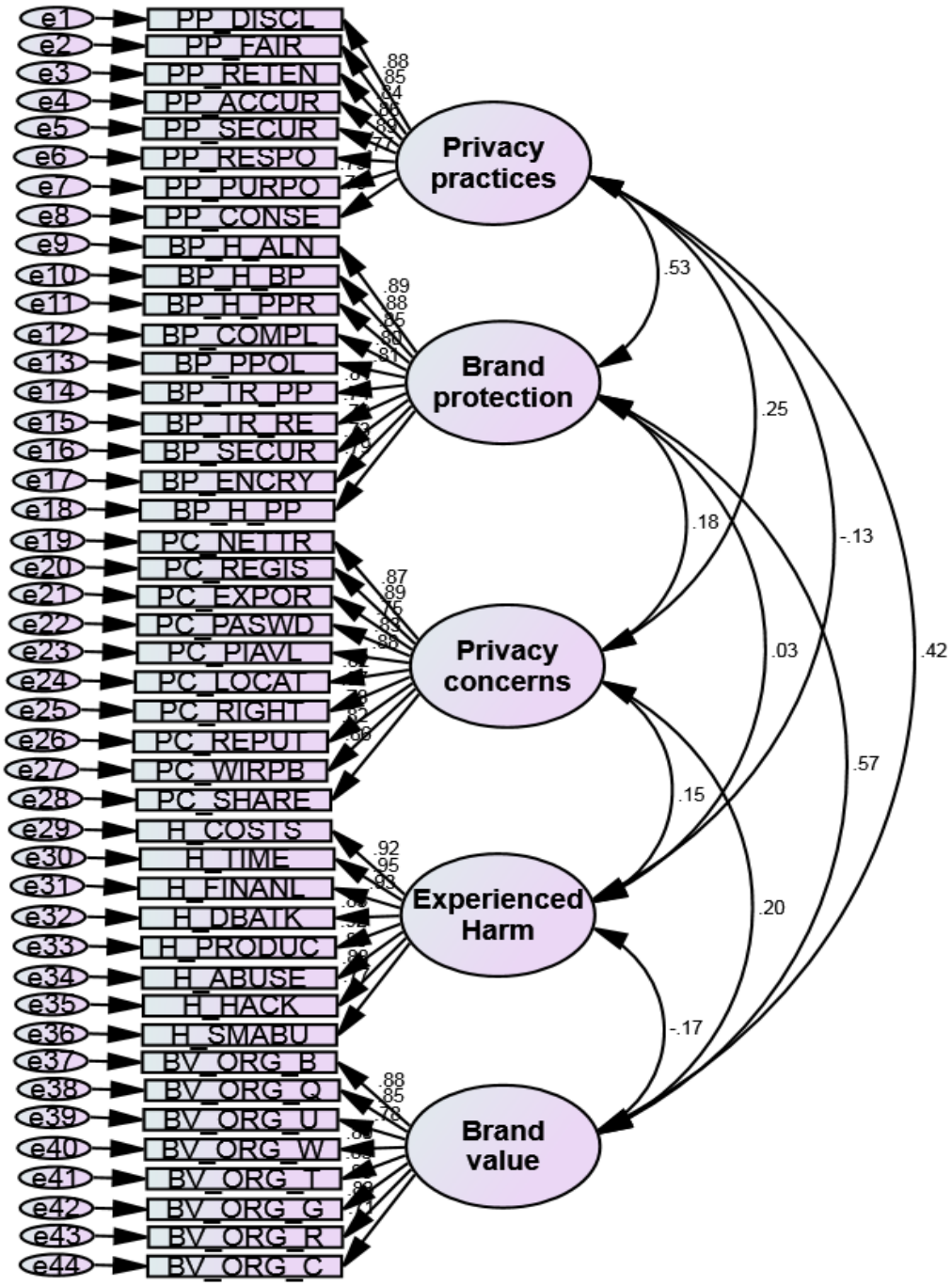


Figure 6.6. Confirmatory Factor Analysis with Experienced Harms Added to Privacy Practices, Brand Protection, Privacy Concerns and Brand Value.

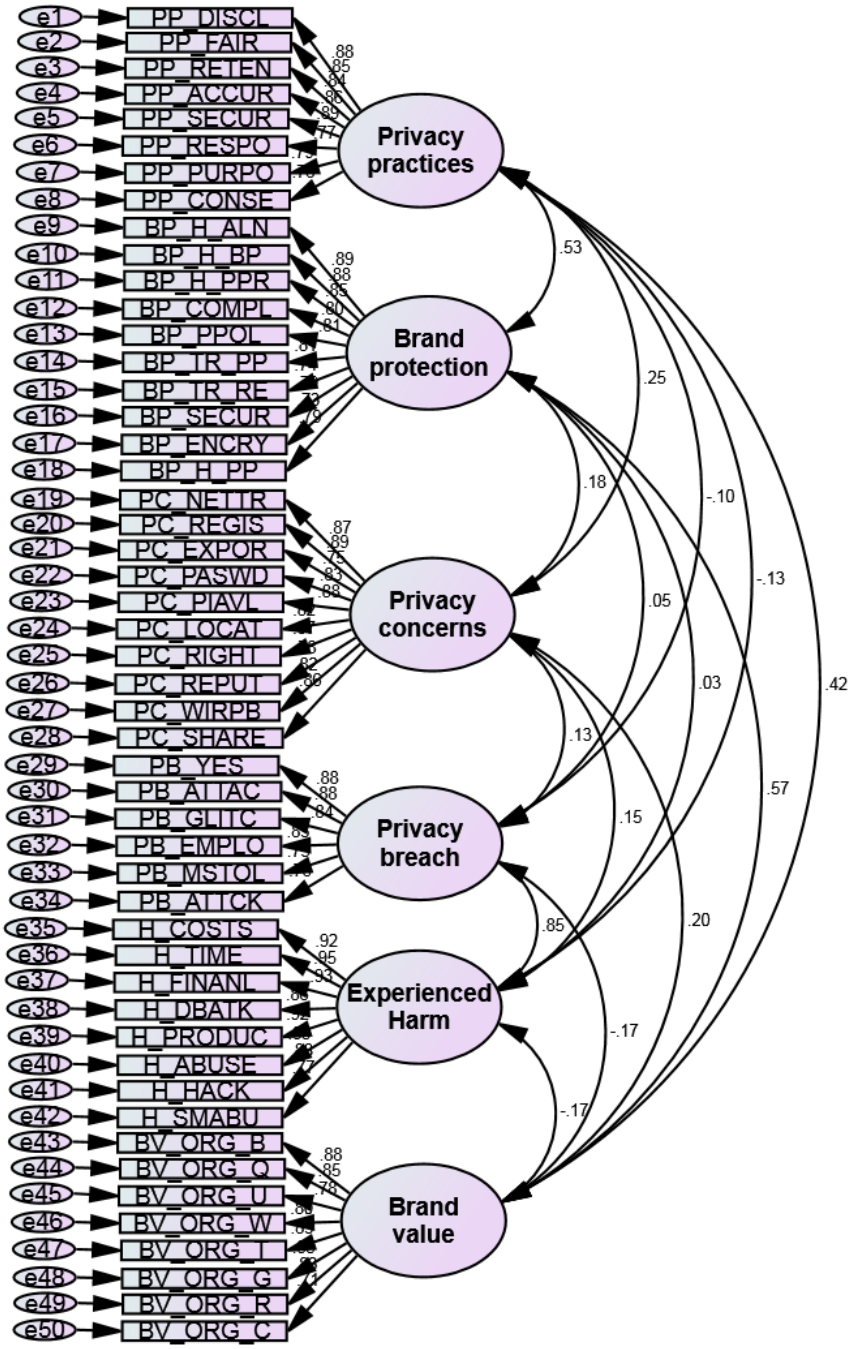


Figure 6.7. Confirmatory Factor Analysis of Privacy Practices, Brand Protection, Privacy Concerns, Privacy Breach, Experienced Harms, and Brand Value.

When I included Privacy breaches I found a high correlation (.85) between Privacy breach and Experienced Harms (see Figure 6.7) so I reran principal components analysis and discovered that they extracted onto the same component. I ran pattern matrices and rotated component matrices. I started my analyses again from the beginning and built new scales to improve the model fit.

Total Variance Explained

The total variance explained by 5 components extracted was 76.356. This was determined by the cumulative % of the total variance. Gaskin (2013a) recommends that the cumulative % of the total variance be > 60% so the total variance explained is very good. I was expecting six components to be extracted but it was discovered that Experienced harm and Privacy breach loaded onto the same component. This is understandable because many of the statements related to experiencing harm were caused because of a data privacy breach. The Experience harm items loaded higher so these were retained for further analyses. The five components extracted were PP: Privacy practices, PC: Privacy concerns, EH: Experienced harms, BV: Brand value and BP: Brand protection.

KMO and Bartlett's Test

The Kaiser-Meyer-Olkin Measure of Sampling Adequacy was .926. A KMO > .7 is fine, >.8 is good and >.9 is great (Gaskin, 2003a). My KMO of .926 is great.

Reliability Analyses

Reliability analyses were ran for each of the five components to validate their scales. All Cronbach's Alphas were between .927 and .947 and found to be reliable.

New Scales

A new privacy practices scale was developed composed of eight statements from the *Privacy Management Survey* (*N* = 315). The reliability of Cronbach's alpha based on standardized items is 0.945. Item statistics and the *Privacy Practices Scale* are described in Tables 6.3 and 6.4. Descriptive statistics and intercorrelations for all variables for each scale are displayed in Tables 6.5, 6.8, 6.11, 6.14 and 6.17.

Table 6.3

Item Statistics for Privacy Practices

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PP_DISCL	42.70	61.043	.854	.774	.935
PP_FAIR	42.71	61.727	.826	.718	.936
PP_RETEN	42.92	60.541	.811	.702	.937
PP_ACCUR	42.87	62.137	.821	.724	.937
PP_SECUR	42.88	60.868	.852	.758	.935
PP_MINIM	43.11	61.523	.736	.557	.943
PP_PURPO	42.97	62.018	.772	.629	.940
PP_RESPO	42.89	62.294	.750	.620	.941

Table 6.4

Privacy Practices Scale

#	VAR Name	Question	Mean	Std. Deviation
1	PP_DISCL	My organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.	6.30	1.28
2	PP_FAIR	My organization collects information by fair and lawful means.	6.30	1.26
3	PP_RETEN	My organization retains personal information only as long as necessary for the fulfillment of the purposes, which it was collected, except with the consent of the individual or as required by law.	6.09	1.37
4	PP_ACCUR	My organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.	6.14	1.24
5	PP_SECUR	My organization protects personal information by security safeguards appropriate to the sensitivity of the information.	6.13	1.29
6	PP_MINIM	My organization limits the collection of personal information to that which is necessary for the purposes identified by the organization.	5.90	1.41
7	PP_PURPO	My organization identifies the purposes for which personal information is collected at or before the time the information is collected.	6.03	1.32
8	PP_RESPO	My organization is responsible for personal information under its control	6.12	1.32

Descriptive statistics and intercorrelations for variables in privacy practices scale are presented in Table 6.5. All correlations are significant at the 0.01 level (2-tailed).

Table 6.5

Descriptive Statistics and Intercorrelations for Variables in Privacy Practices Scale

#	PP_VAR	M	SD	1	2	3	4	5	6	7	8
1	PP_DISCL	6.30	1.28	--							
2	PP_FAIR	6.30	1.26	.796**	--						
3	PP_RETEN	6.09	1.37	.789**	.683**	--					
4	PP_ACCUR	6.14	1.24	.769**	.720**	.730**	--				
5	PP_SECUR	6.13	1.29	.767**	.720**	.757**	.811**	--			
6	PP_MINIM	5.90	1.41	.661**	.630**	.653**	.616**	.663**	--		
7	PP_PURPO	6.03	1.31	.644**	.676**	.654**	.640**	.668**	.654**	--	
8	PP_RESPO	6.12	1.32	.653**	.710**	.589**	.620**	.683**	.574**	.702**	--

**. Correlation is significant at the 0.01 level (2-tailed).

A new brand protection scale was developed composed of six statements from statements on the *Privacy Management Survey* (*N* = 315). The reliability of Cronbach's alpha based on standardized items is .927. Item statistics for Brand Protection are provided in Table 6.6 and the *Brand Protection Scale* is described in Table 6.7.

Table 6.6

Item Statistics for Brand Protection

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
BP_PIAS	25.30	54.681	.839	.777	.907
BP_AUDIT	25.11	54.488	.858	.791	.905
BP_ABUSE	25.04	55.743	.776	.622	.916
BP_H_MOD	24.98	56.780	.784	.623	.915
BP_CO_ST	25.01	56.968	.739	.568	.921
BP_RECOR	24.75	58.916	.738	.553	.921

Table 6.7

Brand Protection Scale

#	VAR Name	Question	Mean	Std. Deviation
1	BP_PIAS	My organization conducts privacy impact assessments (PIAs).	4.74	1.77
2	BP_AUDIT	My organization conducts privacy audits.	4.93	1.76
3	BP_ABUSE	My organization has a privacy program to prevent digital brand abuse.	4.99	1.80
4	BP_H_MOD	My organization uses privacy management models.	5.06	1.71
5	BP_CO_ST	My organization provides communication to stakeholders and users regarding data privacy awareness.	5.03	1.77
6	BP_RECOR	My organization reviews holdings, disposes of transitory records and classifies remaining records at the appropriate security level.	5.29	1.62

Descriptive statistics and intercorrelations for variables in brand protection scale are presented in Table 6.8. All correlations are significant at the 0.01 level (2-tailed).

Table 6.8

Descriptive Statistics and Intercorrelations for Variables in Brand Protection Scale

#	BP_VAR	M	SD	1	2	3	4	5	6
1	BP_PIAS	4.74	1.77	--					
2	BP_AUDIT	4.93	1.76	.863**	--				
3	BP_ABUSE	4.99	1.80	.739**	.726**	--			
4	BP_H_MOD	5.06	1.71	.686**	.713**	.680**	--		
5	BP_CO_ST	5.03	1.77	.648**	.666**	.590**	.679**	--	
6	BP_RECOR	5.29	1.62	.644**	.680**	.621**	.627**	.644**	--

**. Correlation is significant at the 0.01 level (2-tailed).

Six statements for privacy concerns from the *Privacy Management Survey* have been selected through SPSS analysis to make a new privacy concerns scale. The reliability of Cronbach's alpha based on standardized items is 0.944 (N = 315). Item statistics for Privacy Concerns are provided in Table 6.9 and the *Privacy Concerns Scale* is described in Table 6.10.

Table 6.9

Item Statistics for Privacy Concerns

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PC_REGIS	26.17	45.641	.866	.810	.929
PC_NETTR	26.27	45.454	.855	.804	.930
PC_PIAVL	25.94	47.350	.828	.724	.933
PC_SHARE	25.83	48.705	.835	.746	.934
PC_PASWD	25.98	46.328	.802	.666	.937
PC_LOCAT	26.10	45.400	.805	.675	.937

Table 6.10

Privacy Concerns Scale

#	VAR Name	Question	Mean	Std. Deviation
1	PC_REGIS	I am concerned that online registration is easily compromised.	5.09	1.55
2	PC_NETTR	I am concerned that network traffic is leaking private data.	4.98	1.58
3	PC_PIAVL	I am concerned that personal information is readily available and that risks are not communicated to the public.	5.32	1.47
4	PC_SHARE	I am concerned that personal data obtained is shared with others.	5.43	1.34
5	PC_PASWD	I am concerned about privacy of passwords.	5.28	1.59
6	PC_LOCAT	I am concerned about location tracking.	5.15	1.66

Descriptive statistics and intercorrelations for variables in privacy concerns scale are presented in Table 6.11. All correlations are significant at the 0.01 level (2-tailed).

Table 6.11

Descriptive Statistics and Intercorrelations for Variables in Privacy Concerns Scale

#	PC_VAR	M	SD	1	2	3	4	5	6
1	PC_REGIS	5.09	1.55	--					
2	PC_NETTR	4.98	1.58	.875**	--				
3	PC_PIAVL	5.32	1.47	.764**	.716**	--			
4	PC_SHARE	5.43	1.34	.716**	.699**	.803**	--		
5	PC_PASWD	5.28	1.59	.729**	.720**	.726**	.763**	--	
6	PC_LOCAT	5.15	1.66	.740**	.770**	.690**	.739**	.665**	--

**. Correlation is significant at the 0.01 level (2-tailed).

A new experienced harms scale was developed composed of four statements from the *Privacy Management Survey* (*N* = 315). The reliability of Cronbach's alpha based on standardized items is 0.947. Item statistics for Experienced Harms are provided in Table 6.12 and the *Experienced Harms Scale* is described in Table 6.13.

Table 6.12

Item Statistics for Experienced Harms

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
H_BRVAL	6.45	19.414	.901	.823	.923
H_COSTS	6.33	17.661	.906	.837	.921
H_IDTHF	6.37	19.264	.830	.694	.944
H_REVNUE	6.38	19.383	.861	.750	.935

Table 6.13

Experienced Harms Scale

#	VAR Name	Question	Mean	Std. Deviation
1	H_BRVAL	My organization has experienced damaged brand value because of a data breach.	2.06	1.45
2	H_COSTS	My organization has experienced litigation costs because of a data breach.	2.18	1.66
3	H_IDTHF	My organization has experienced identity theft.	2.14	1.56
4	H_REVNUE	My organization has experienced lost revenue because of a data breach.	2.13	1.51

Descriptive statistics and intercorrelations for variables in experienced harms scale are presented in Table 6.14. All correlations are significant at the 0.01 level (2-tailed).

Table 6.14

Descriptive Statistics and Intercorrelations for Variables in Experienced Harms Scale

#	H_VAR	M	SD	1	2	3	4
1	H_BRVAL	2.06	1.45	--			
2	H_COSTS	2.18	1.66	.887**	--		
3	H_IDTHF	2.14	1.56	.809**	.795**	--	
4	H_REVNUE	2.13	1.51	.819**	.849**	.762**	--

**. Correlation is significant at the 0.01 level (2-tailed).

The brand value scale used in this thesis is based on a scientifically validated scale found in Barnes and Mattson (2008). A modified brand value scale was developed composed of seven statements from the *Privacy Management Survey* (*N* = 315). The reliability of Cronbach's alpha based on standardized items is 0.944. Item statistics for Brand Value are provided in Table 6.15 and the *Brand Value Scale* is described in Table 6.16.

Table 6.15

Item Statistics for Brand Value

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
BV_ORG_G	32.92	49.356	.867	.843	.931
BV_ORG_S	32.98	50.070	.859	.800	.932
BV_ORG_T	33.10	48.666	.830	.790	.935
BV_ORG_R	32.96	50.263	.836	.751	.934
BV_ORG_B	32.79	51.829	.825	.754	.935
BV_ORG_Q	32.98	50.608	.789	.744	.938
BV_ORG_U	33.17	51.578	.709	.602	.945

Table 6.16

Brand Value Scale

#	VAR Name	Question	Mean	Std. Deviation
1	BV_ORG_G	My organization does me good.	5.57	1.37
2	BV_ORG_S	My organization is a satisfying buy.	5.50	1.32
3	BV_ORG_T	I feel I am able to trust my organization	5.39	1.47
4	BV_ORG_R	What my organization delivers feels right	5.52	1.34
5	BV_ORG_B	My organization is a good brand	5.69	1.22
6	BV_ORG_Q	What my organization delivers feels right	5.50	1.37
7	BV_ORG_U	The uniqueness of my organization stands	5.31	1.41

The variables which were eliminated, based on principal components analysis, from the modified brand value scale were:

BV_ORG_C	What I get from my organization is worth the cost.
BV_ORG_P	I feel great pride identifying with my organization
BV_ORG_W	What I get from my organization is worth the cost.

Descriptive statistics and intercorrelations for variables in brand value scale are presented in Table 6.17. All correlations are significant at the 0.01 level (2-tailed).

Table 6.17

Descriptive Statistics and Intercorrelations for Variables in Brand Value Scale

#		M	SD	1	2	3	4	5	6	7
1	BV_ORG_G	5.57	1.37	--						
2	BV_ORG_S	5.50	1.32	.873**	--					
3	BV_ORG_T	5.39	1.47	.862**	.808**	--				
4	BV_ORG_R	5.52	1.34	.819**	.790**	.823**	--			
5	BV_ORG_B	5.69	1.22	.690**	.705**	.670**	.696**	--		
6	BV_ORG_Q	5.50	1.37	.659**	.652**	.616**	.662**	.830**	--	.
7	BV_ORG_U	5.31	1.41	.586**	.626**	.554**	.563**	.719**	.741**	--

**. Correlation is significant at the 0.01 level (2-tailed).

Descriptive statistics and correlations for two variables from each scale are displayed in Table 6.18.

Table 6.18

Descriptive Statistics and Correlations for Two Variables from Each Scale

	M	SD	1	2	3	4	5	6	7	8	9	10
1. PP_DISCL	6.30	1.28	--									
2. PP_FAIR	6.30	1.26	.796**	--								
3. BP_PIAS	4.74	1.77	.166**	.189**	--							
4. BP_AUDIT	4.93	1.76	.211**	.225**	.863**	--						
5. PC_REGIS	5.09	1.55	.177**	.228**	.081	.077	--					
6. PC_NETTR	4.98	1.58	.152**	.202**	.104	.084	.875**	--				
7. H_BRVAL	2.06	1.45	-.097	-.039	.128*	.128*	.130*	.111*	--			
8. H_COSTS	2.18	1.66	-.104	-.025	.163**	.157**	.136*	.096	.887**	--		
9. BV_ORG_G	5.57	1.37	.291**	.314**	.311**	.344**	.096	.110	-.097	-.091	--	
10. BV_ORG_S	5.50	1.32	.260**	.262**	.337**	.342**	.105	.133*	-.097	-.071	.873**	--

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Standardized estimates of the confirmatory factor analysis of privacy practices, brand protection, privacy concerns, experienced harms, and brand value are provided in Figure 6.8 (χ^2 = 1144, (*N* = 315), p = .000; NFI = .882; CFI = .922; RMSEA = .074, p= <.001). The CFI and NFI yielded values of .922 and .882, respectively, indicating a good fit of the model. The RMSEA was .074, indicating a moderate fit since it is between .07 and .08 (Meyers et al., 2017).

To improve the model fit covariances were added to the error terms that had large values that were on the same factor as indicated in the modification indices. For example, MI=117 for e26↔e27. Since these errors were on the same factor, brand value, they were covaried to improve the model fit. The standardized estimates of the confirmatory factor analysis of privacy practices, brand protection, privacy concerns, experienced harms, and brand value with covariances to the error terms are provided in Figure 6.9. (χ^2 = 683 (*N* = 315), p = .000; NFI = .929; CFI = .971; RMSEA = .046, p= .000). The CFI and NFI yielded values of .971 and .929, respectively, indicating a good fit of the model. The RMSEA was .046, also indicating a good fit since it is < .06 (Meyers et al., 2017).

Factors that had high standardized residual covariances were removed to improve the fit of the model. The variables that were removed included: BV_ORG_B, PP_SECUR, PP_PURPO, BV_ORG_R and PP_RESPO. Standardized estimates of the confirmatory factor analysis of privacy practices, brand protection, privacy concerns, experienced harms, and brand value after checking standardized residual covariances are provided in

Figure 6.10 (χ^2 = 481 (*N* = 315), p = .000; NFI = .937; CFI = .973; RMSEA = .047, p= .000). The CFI and NFI yielded values of .973 and .937 respectively, indicating a good fit of the model. The RMSEA was .047 also indicating a good fit since it was < .06 (Meyers et al., 2017).

The following steps were taken to build the structural equation model (SEM). Confirmatory factor analyses were ran on Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value variables included in the model (see Figure 6.8). To improve the model the error terms were constrained and CFA was reanalyzed (see Figure 6.9). To make further improvements high standardized residual covariances were removed and the CFA was run again (see Figure 6.10). Then a SEM of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value was built (see Figure 6.11). SEM was ran again after more error terms were covaried (see Figure 6.12).

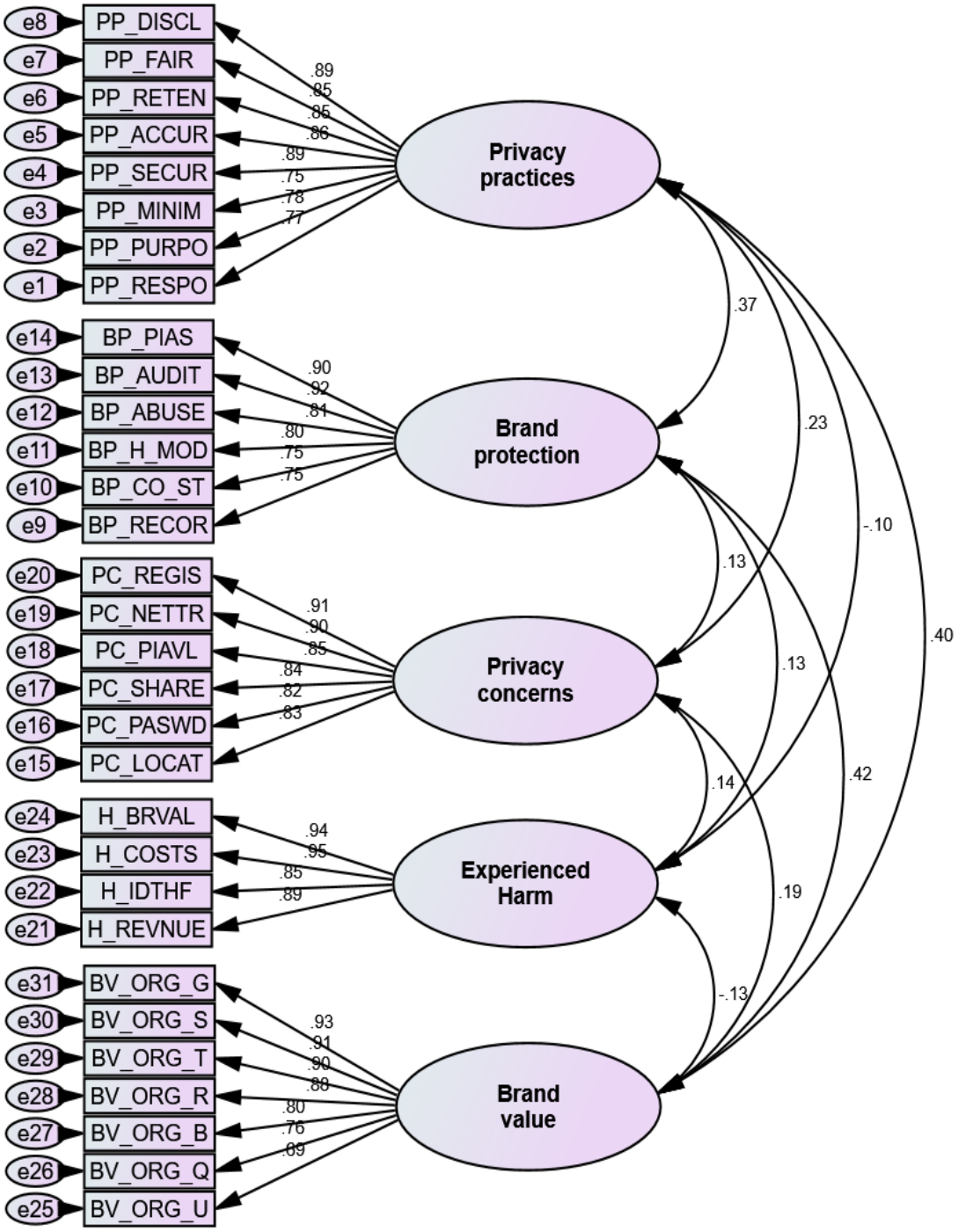


Figure 6.8. Confirmatory Factor Analysis of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

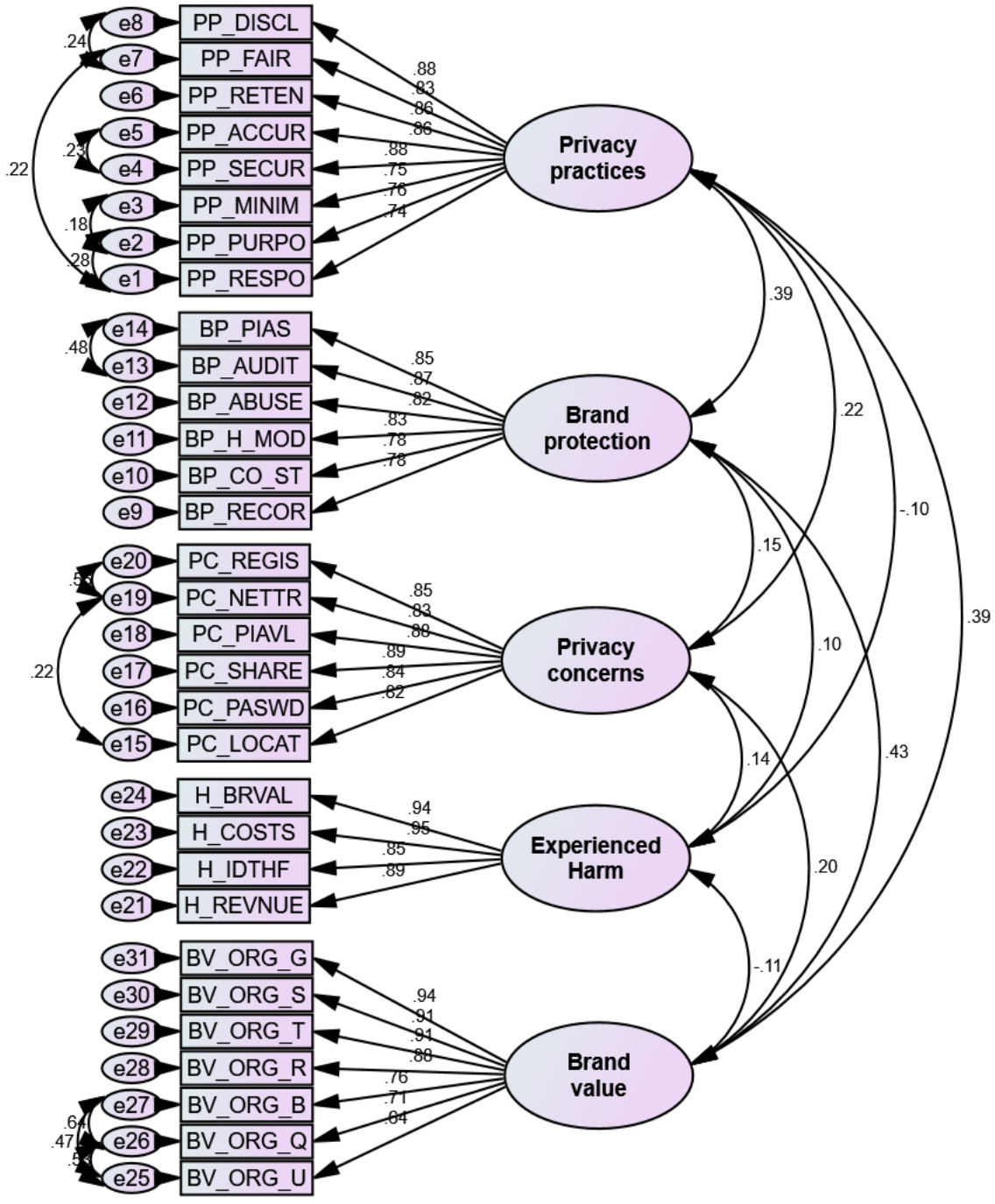


Figure 6.9. Confirmatory Factor Analysis of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value with Error Terms Constrained.

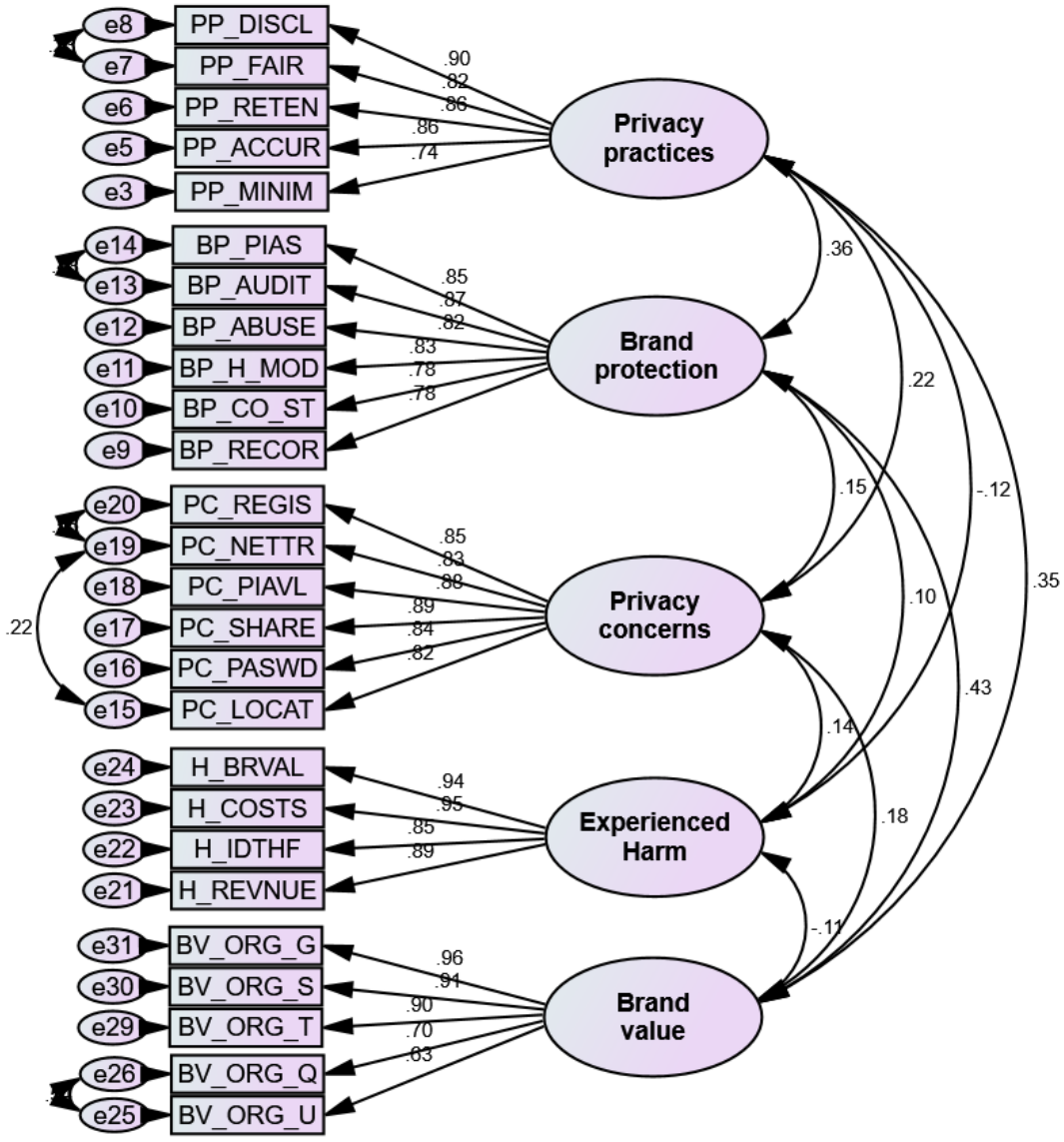


Figure 6.10. Confirmatory Factor Analysis of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value with Error Terms Constrained and High Standardized Residual Covariances Removed.

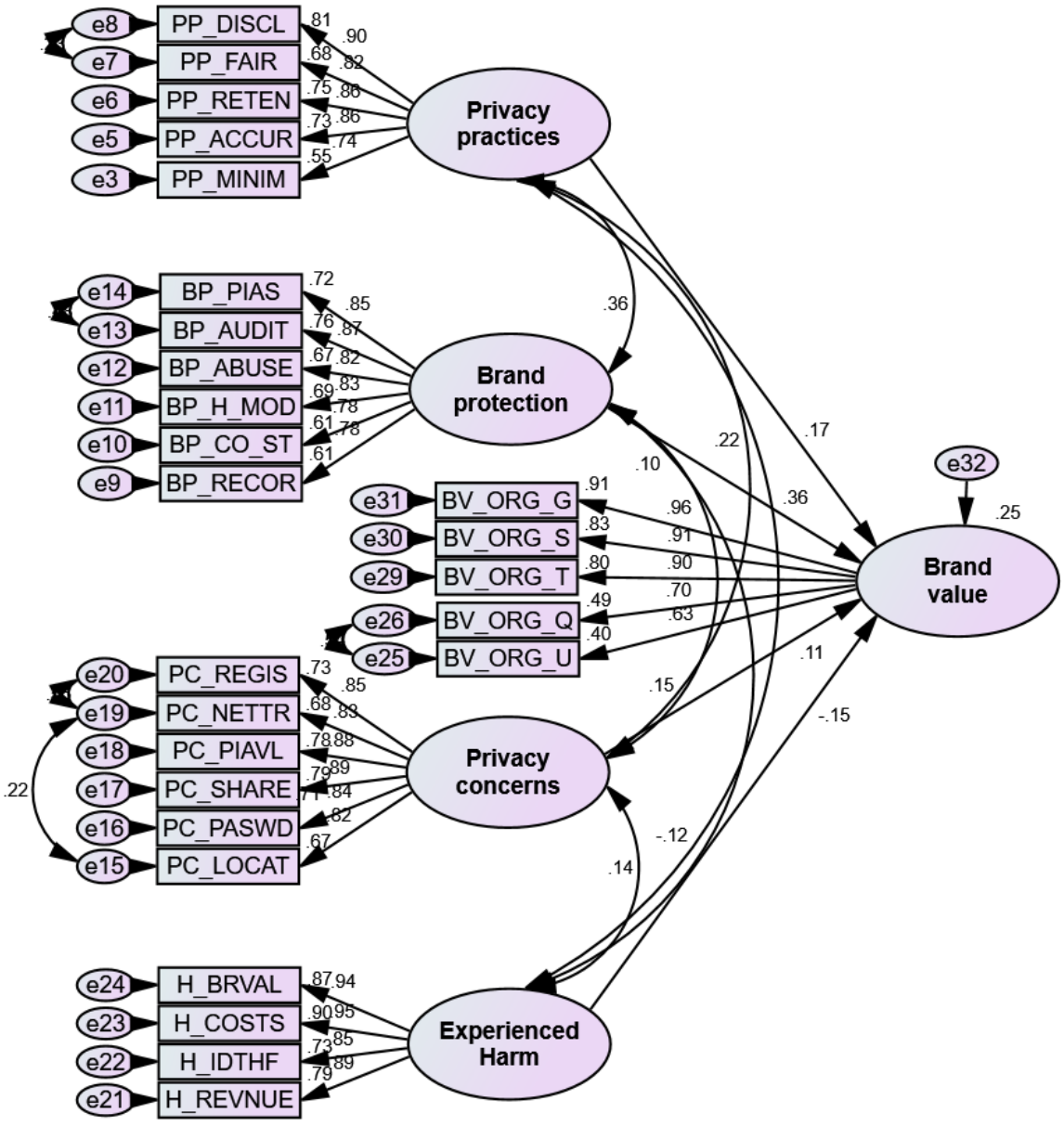


Figure 6.11. Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value After Error terms were Covaried and Standardized Residual Covariances were Addressed.

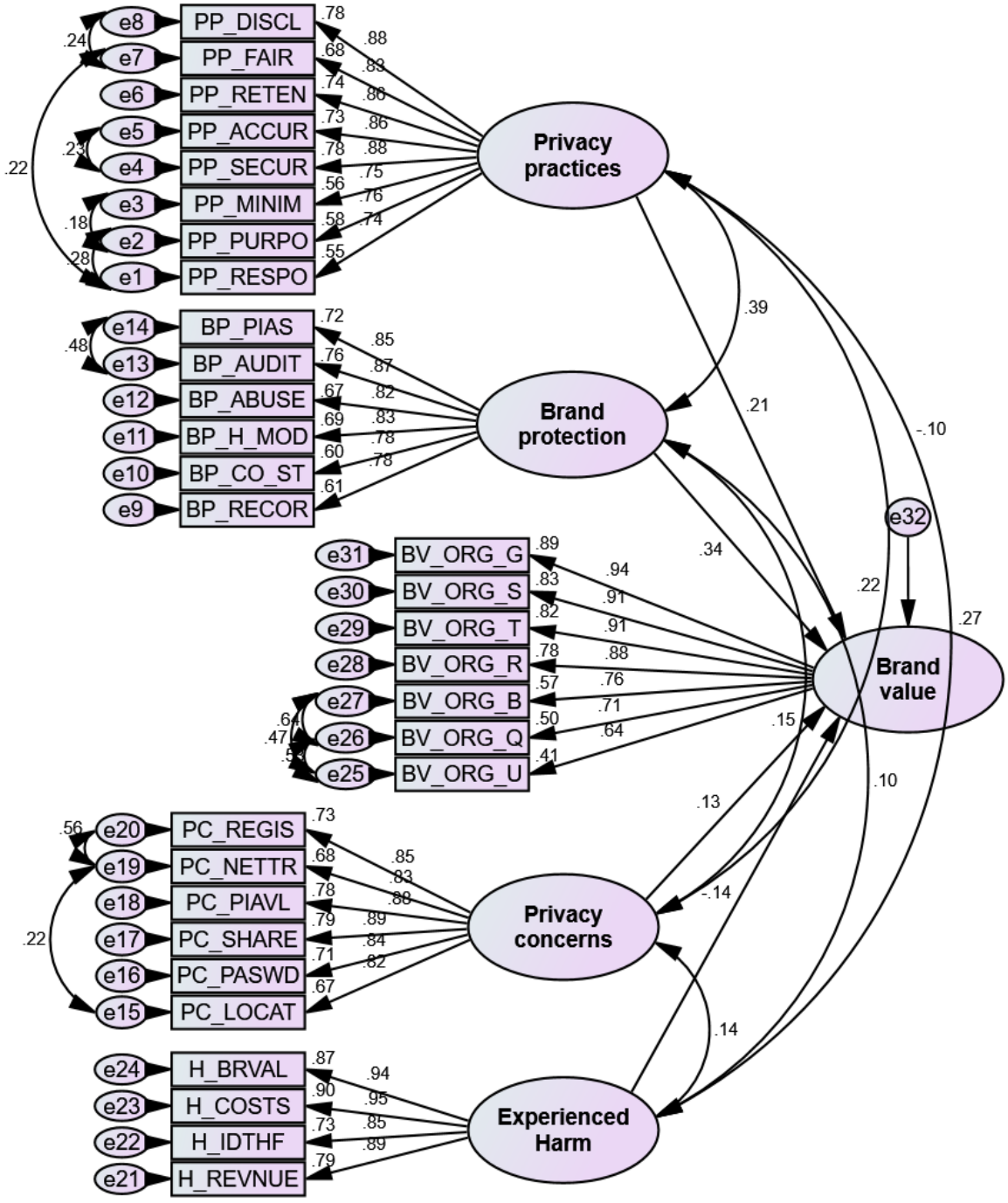


Figure 6.12. Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value After Error terms were Covaried.

The next step after I changed my Measurement Model (see Figure 6.10) into a Structural Model (see Figure 6.11) was to test for mediation. When comparing Figures 6.9 and 6.10 I made the decision to add the variables back in that I removed during the Standardized Residual Covariances stage. The model fit was good for both. I did not want to reduce the number of statistically significant relationships by eliminating some of my variables if it was not necessary.

There were statistically significant relationships (*** $p \leq .001$) found between Privacy practices and Brand value and between Brand protection and Brand value thus supporting Hypotheses H2 and H3 (see Table 6.19) There was a statistically significant relationship (** $p < .01$) found between Experienced harm and Brand value which supported H6. A statistically significant relationship (* $p \leq .05$) was found between Privacy concerns and Brand value thus supporting H9.

Table 6.19

Regression Weights of Structural Equation Model

			Estimate	**S.E.**	**C.R.**	**P**
H2. Brand_value	←	Privacy_practices	0.195	0.057	3.442	***
H3. Brand_value	←	Brand_protection	0.243	0.046	5.255	***
H6. Brand_value	←	Experienced_Harm	-0.097	0.036	-2.676	0.007**
H9. Brand_value	←	Privacy_concerns	0.083	0.036	2.288	0.022*

Note: P < 0.05 *, P < 0.01 **, P < 0.001***

A structural equation model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value was created in AMOS after the error terms were covaried (see Figure 6.13).

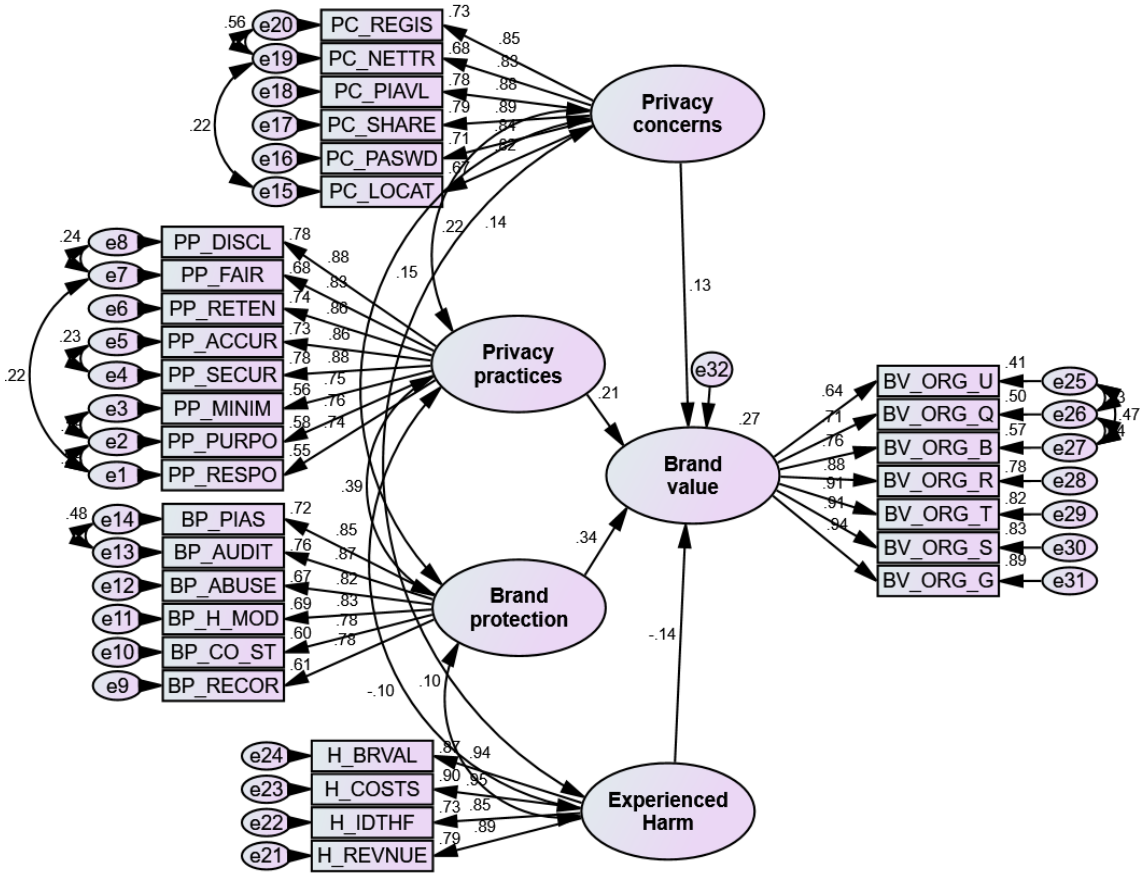


Figure 6.13. Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value After Error terms were Covaried.

Mediation

The Privacy-brand Model was tested and found to have excellent model fit. The coefficients of determinations in the model were excellent. R^2 values ranged from .41 to .90 (see Figure 6.12). "R squared" indicates the "proportion of the variance in the dependent variable that is predictable from the independent variable" (Coefficient of Determination, 2016). To test for mediation of the model I downloaded Gaskin's Userdefined Estimand (Gaskin, 2016b) and opened it in AMOS. The two paths were named A and B that were tested for indirect effects. To test for H1 the path from Privacy practices to Privacy concerns was named A. To do this I opened the parameter box and assigned A to the regression weight. B was assigned to the regression weight for the parameter completing the indirect effect from Privacy concerns to Brand value (see Figure 6.14). A will be multiplied by B to get the statistics needed to determine if mediation is occurring. This was repeated by changing the regression weights for the other indirect paths to test the hypotheses for mediation. The following hypotheses were tested for mediation:

H10 (Mediation). Privacy concerns mediate the positive effect of Privacy practices on Brand value.

H11 (Mediation). Experienced harms mediate the negative effect of Privacy practices on Brand value.

H12 (Mediation). Privacy concerns mediate the positive effect of Brand protection on Brand value.

H13 (Mediation). Experienced harms mediate the negative effect of Brand protection on Brand value.

H14 (Mediation). Experienced harms mediate the negative effect of Privacy concerns on Brand value.

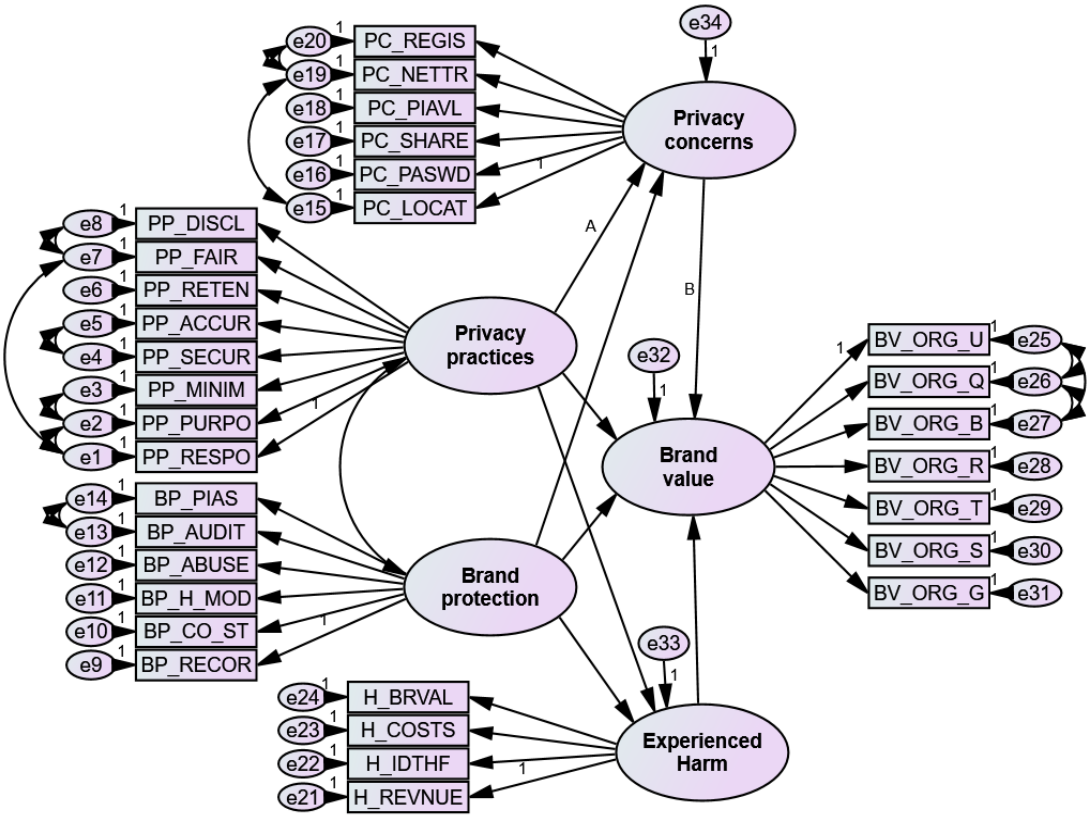


Figure 6.14. Indirect Effects (A and B) Tested for Mediation in Structural Equation Model.

Bootstrapping

Bootstrap was applied to test for mediation. Bias was corrected for at 90% confidence intervals. The Mediatied Privacy-brand Model is displayed in Figure 6.15. A summary of the significant findings for the Mediation Hypotheses is presented in Table 6.20.

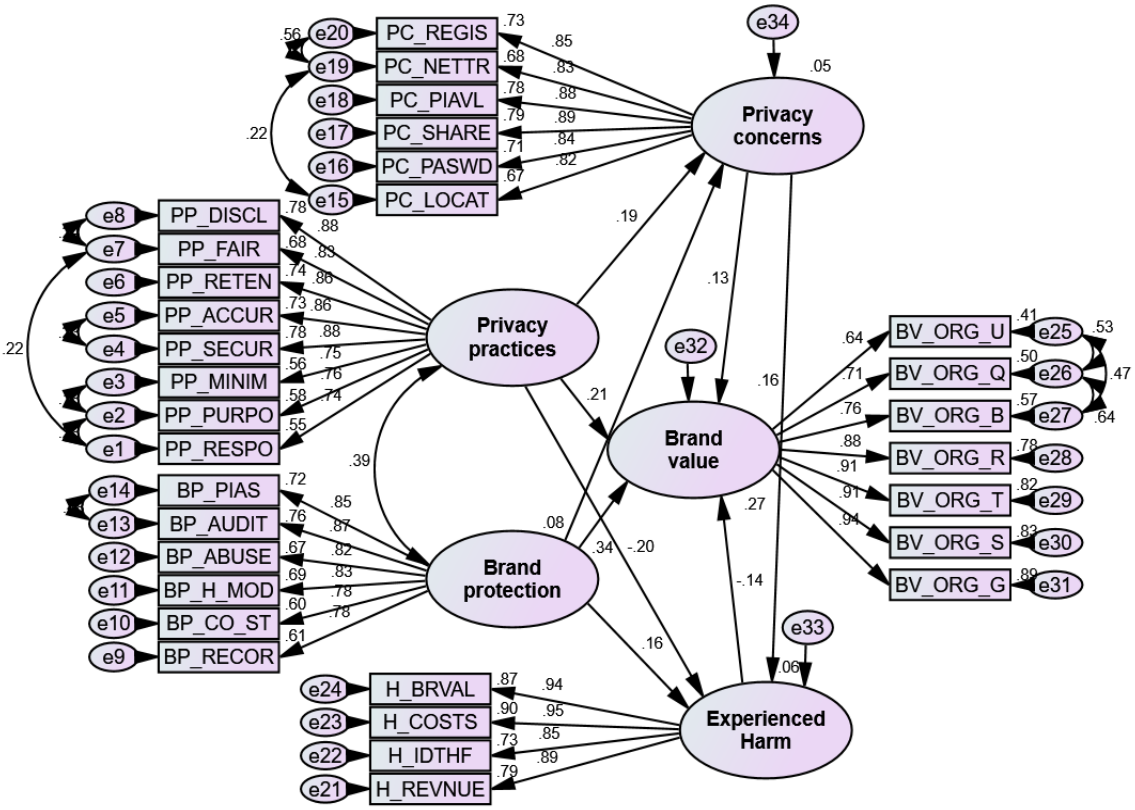


Figure 6.15. Mediation Tested of Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

Table 6.20

User Defined Estimands for Mediation Hypotheses

Hypothesis (mediation)		Estimate	Lower	Upper	P	Conclusion
H10	PP→ PC→ BV	0.021	0.004	0.054	0.030	*Significant
H11	PP→ EH→ BV	0.022	0.007	0.055	0.002	**Significant
H12	BP→ PC→ BV	0.007	-0.001	0.035	0.172	Not significant
H13	BP→ EH→ BV	-0.017	-0.038	-0.007	0.002	**Significant
H14	PC→ EH→ BV	-0.015	-0.031	-0.007	0.001	***Significant

Note: P < 0.05 *, P < 0.01 **, P < 0.001 ***

A Structural equation model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value was built in AMOS and is presented in Figure 6.16.

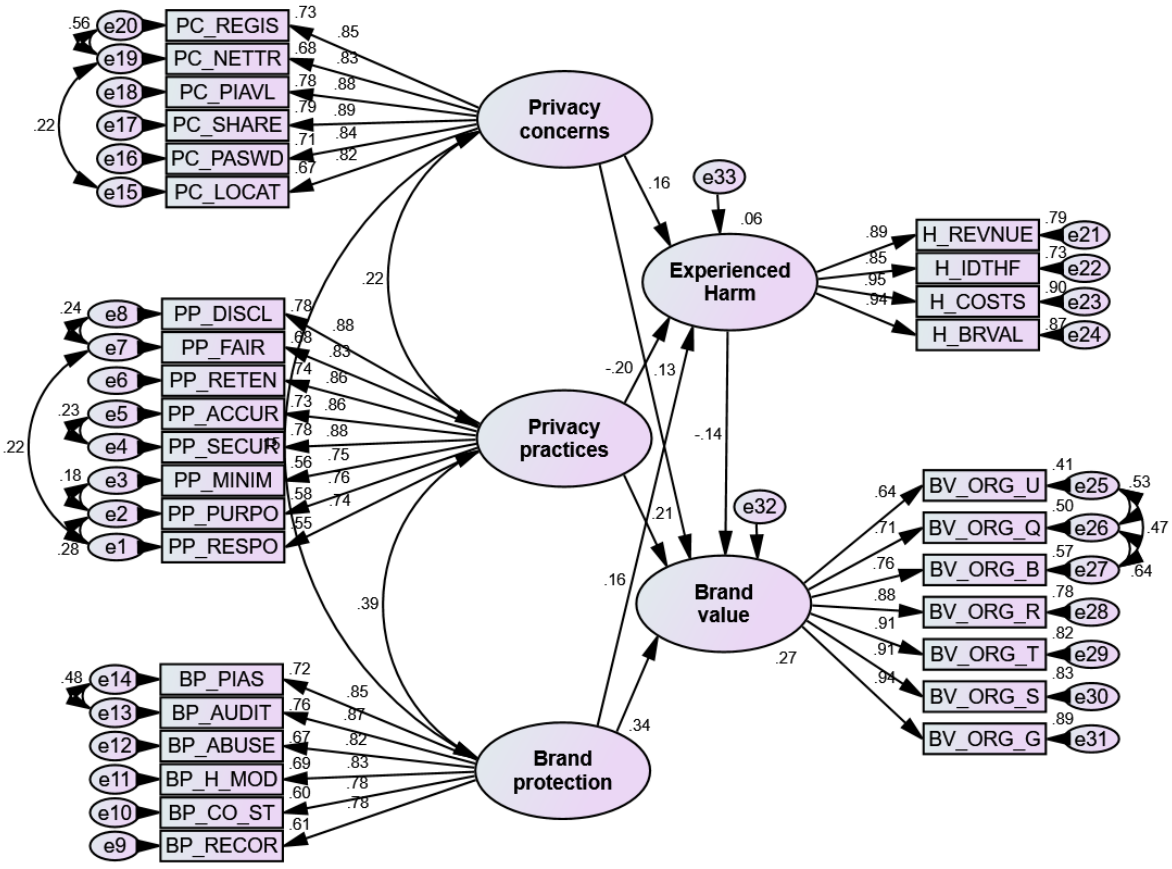


Figure 6.16. Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

Expanded Privacy-Brand Model

The expanded Privacy-Brand Model created in this thesis is shown in Figure 6.17. It was determined that Experienced harms mediates the effects between privacy concerns,

privacy practices, brand protection, and brand value. Standardized regression weights (see Table 6.21) were added to the model from the text output produced in AMOS.

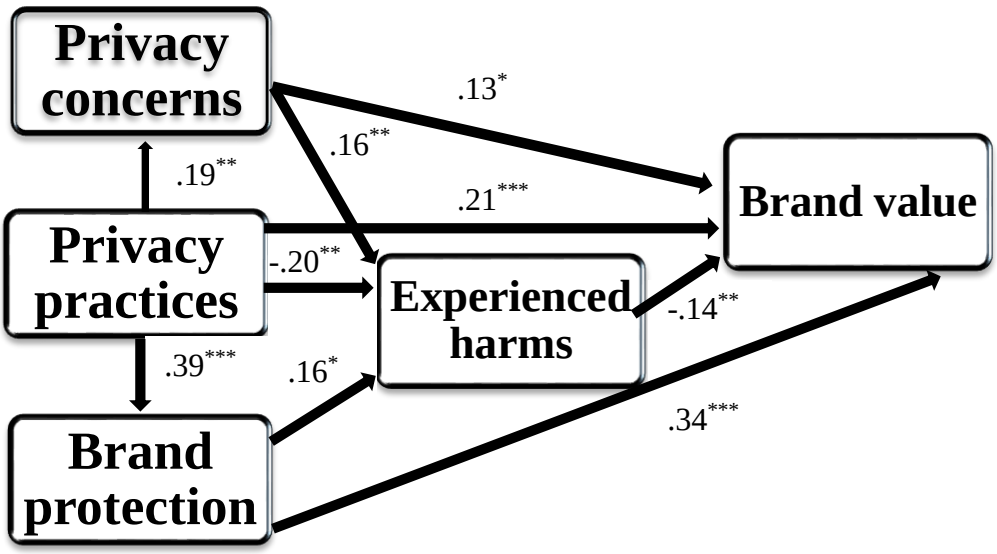


Figure 6.17. Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value.

Table 6.21

Standardized Regression Weights

Privacy_concerns	←	Privacy_practices	.186
Privacy_concerns	←	Brand_protection	.075
Experienced_Harm	←	Brand_protection	.158
Experienced_Harm	←	Privacy_concerns	.156
Experienced_Harm	←	Privacy_practices	-.198
Brand_value	←	Privacy_concerns	.126
Brand_value	←	Experienced_Harm	-.145
Brand_value	←	Brand_protection	.341
Brand_value	←	Privacy_practices	.213

Discussion

This chapter provided a summary of the qualitative data collected on the *Privacy Management Survey* describing privacy concerns of the participants (see Chapter 4). The quantitative data collected from participants rating their privacy concerns on a 7-point Likert Scale from strongly disagree to strongly agree was discussed in this chapter.

New scales were developed for privacy practices, brand protection, experienced harms, brand value and privacy concerns. A new Expanded Privacy-Brand Model (see Figure 6.17) was developed as well as a Mediated Structural Equation Model (see Figure 6.16) for my Privacy-Brand Model.

For the mediated, structural equation Privacy-Brand Model I developed ($\chi^2(414) = 689$, χ^2 /df = 1.666, p = .000; NFI = .929; CFI = .971; RMSEA = .046, p = <.001). The chi square had a value of 689, with 414 degrees of freedom, (N = 315), p = .000. The CFI and NFI yielded values of .971 and .929, respectively, indicating a good fit of the model. The RMSEA was .046, also indicating a good fit since it is < .06 (Meyers et al., 2017).

The mediated hypothesis H14 was found to be statistically significant (*** $p \leq .001$), H11 and H13 were statistically signigicant (** $p \leq .01$), H10 was found to be statistically significant (* $p \leq .05$) while H12 was found to not be statistically significant.

Experienced harms mediates the effect between Privacy concerns and Brand value (*** $p \leq .001$). Experienced harms mediates the effects between Privacy practices and Brand value and between Brand protection and Brand value (** $p \leq .01$). Privacy concerns mediates the effect between Privacy practices and Brand value (* $p \leq .05$).

Privacy concerns does not mediate the effect between Brand protection to Brand value (see Table 6.20).

CHAPTER 7 – HOLD OUT SAMPLE

Sample Two – Hold Out Sample

A hold out sample (N = 205), was analyzed to confirm the mean values obtained, scales developed and Privacy-Brand Model created with the first sample collected (N = 315). The hold out sample was used to conduct an analysis of internal consistency (IC).

Method

Participants (N = 205)

Demographic information was collected about the participants and their organizations. The survey was distributed to two random samples representative of the population 18 years or older, employed in the United States and who work with personal information. Sample 1 consisted of 315 participants and Sample 2 consisted of 205 participants.

The demographic information for the data set for study 3 (N = 205) is presented in this section. The gender of the survey participants included 54 males, which equals 26%, and 74% or 151 of the 205 participants were females. Thirty-seven percent of participants were between 25 to 34 years old. This was followed by 21% between the ages of 45 to 54 and 18% who were 35 to 44 years old. The participants were well educated with 39% having a Bachelor's degree. This was followed by 17% having some college or university but no degree; 16% having an Associated degree; and 11% having a Master's degree;

17% had some college or university, but no degree; and 9% had completed high school. All participants were from the United States.

Thirty-two percent of the respondents were Clerical/Labour/Other Support. Middle Management accounted for 28%; 14% Technical and Senior Management and 12% were Others. Other levels of positions provided were: Account manager, administrative secretary, Associate, customer service, dental hygienist, Direct provider, Junior management, Owner, Owner/Partner, Physical therapist, Doctor, Physician, professional, Professor, RN, Sr. Account Executive and Substitute teacher.

The profession or occupation of the participants were broken down as 18% Administrative support; 17% were Medical and 13% were in Sales and Marketing; 12% were in Information Technology; 9% were in Financial; 4% were Professor / Teacher; 3% were Human Resources; 2% were in Science; 1% in Engineering; 0.5% Legal, Security, and Transport and 0% were in Arts and Entertainment, Law Enforcement, a Privacy Officer or Students and 19% responded as others. There were a variety of professions represented by the sample. Some of the other occupations included: Analyst, Business owner, Clinician, computers, Concierges, Construction, consultant, Counseling, Customer Service Representative, deli, distribution, Educational provider, Food Service, Funeral director, Health care, Hospitality hotel restaurant, insurance, Manager, media, Non Profit Management, non-profit, Pet sitter, production worker, Public Administration, Real Estate

Manager, retail, self-employed, Senior Manager, Social worker, Union Organizer and wait staff.

Public organizations accounted for 47% while 40% were private organizations, 12% were not-for-profit and 1% was other. It was found that 26% of participants belong in the healthcare and social assistance sector, which was higher than the 18% in sample 1; 11% in retail trade; 10% in the finance and insurance business; 8% work in educational services, which was lower than the 13% in sample 1; 4% worked in accommodation and food services; 4% work for the government; 4% professional, scientific and technical services; 3% were in manufacturing; 3% telecommunications industry; 2% in the construction trade; 2% worked with food and beverage; 2% worked with information and cultural industries; 2% were with legal; 2% worked in other services except public administration; 2% were in real estate, rental and leasing; 2% in wholesale trade; and 2% in other. One percent was with agricultural forestry, fishing and hunting; 1% for transportation and warehousing; 1% for utilities; and 0% were in arts, entertainment and recreation.

Forty-five percent of the organizations were large with over 500 employees. Twenty-two percent were medium-sized with 101 to 500 employees, while 20% were very small with between 1 to 50 employees. Ten percent were small with 51 to 100 employees and 2% did not know the size of their organization.

Ninety-three percent of the organizations used personal information while 73% used credit card information and 72% used financial information. Medical information was used by 53% and 52% used proprietary information, which were both higher than sample 1, who used 46% and 45% respectively. Five percent used other information.

Eighty-seven percent of the organizations represented had an online presence while only 57% had a mobile presence. Eighty-two percent provided products or services to the general public and 64% provided products or services online. Online purchases were made by 74% of the organizations. Seventy percent provided products or services to public and other businesses / organizations while 35% provided products or services only to other businesses / organizations. This was a bit higher than sample 1, which was 29%.

A summary of participants in study 1 is provided in Table 4.2. Demographics and survey percentages for sample 2 are provided in Table 7.1.

Table 7.1

Descriptive Statistics of Survey 2 Respondents from Sample 2 (N = 205)

Gender	Male	54 (26.3%)
	Female	151 (73.7%)
Age	18 – 24 years	12 (5.9%)
	25 – 34 years	75 (36.6%)
	35 – 44 years	36 (17.6%)
	45 – 54 years	43 (21.0%)
	55 - 64 years	32 (15.6%)
	65 - 74 years	7 (3.4%)
Education	High school graduate, diploma or the equivalent (i.e. GED)	18 (8.8%)
	Some college or university, but no degree	34 (16.6%)

	Trade/technical/vocational training	7 (3.4%)
	Associate degree	32 (15.6%)
	Bachelor's degree	80 (39.0%)
	Master's degree	22 (10.7%)
	Professional degree	5 (2.4%)
	Doctorate degree	6 (2.9%)
	Other	1 (0.5%)
Level of Position		
	Senior Management	28 (13.7%)
	Middle Management	58 (28.3%)
	Technical	29 (14.1%)
	Clerical/Labour/Other Support	66 (32.2%)
	Other	24 (11.7%)
Profession or Occupation		
	Administrative Support	37 (18.0%)
	Arts and Entertainment	0 (0.0%)
	Engineer	2 (1.0%)
	Financial	19 (9.3%)
	Human Resources	7 (3.4%)
	Information Technology	25 (12.2%)
	Law Enforcement	0 (0.0%)
	Legal	1 (0.5%)
	Medical	35 (17.1%)
	Privacy Officer	0 (0.0%)
	Professor / Teacher	8 (3.9%)
	Sales and Marketing	27 (13.2%)
	Science	3 (1.5%)
	Security	1 (0.5%)
	Student	0 (0.0%)
	Transport	1 (0.5%)
	Other	39 (19.0%)
Sector of Organization		
	Public	97 (47.3%)
	Private	81 (39.5%)
	Not-for-Profit	25 (12.2%)
	Other	2 (1.0%)

	Accommodation and Food Services	8 (3.9%)
	Administrative and Support, Waste Management and Remediation Services	0 (0.0%)
	Agriculture, Forestry, Fishing and Hunting	1 (0.5%)
	Airline	0 (0.0%)
	Arts, Entertainment and Recreation	0 (0.0%)
	Construction	5 (2.4%)
	Educational Services	16 (7.8%)
	Finance and Insurance	20 (9.8%)
	Food and Beverage	3 (1.5%)
	Government	9 (4.4%)
	Health Care and Social Assistance	54 (26.3%)
	Information and Cultural Industries	4 (2.0%)
	Legal	3 (1.5%)
	Management of Companies and Enterprises	4 (2.0%)
	Manufacturing	7 (3.4%)
	Mining, Quarrying, and Oil and Gas Extraction	2 (1.0%)
	Other Services (except Public Administration)	4 (2.0%)
	Professional, Scientific and Technical Services	9 (4.4%)
	Public Administration	1 (0.5%)
	Real Estate and Rental and Leasing	5 (2.4%)
	Retail Trade	22 (10.7%)
	Telecommunications Industry	6 (2.9%)
	Transportation and Warehousing	2 (1.0%)
	Utilities	1 (0.5%)
	Wholesale Trade	5 (2.4%)
	Other	14 (6.8%)
Size of Organization	Very small (1-50 employees)	40 (19.5%)
	Small (51-100 employees)	21 (10.2%)
	Medium (101 - 500 employees	46 (22.4%)
	Large (>500 employees)	93 (45.4%)
	Do not know	5 (2.4%)
Information used by Organization	Personal information	191 (93.2%)
	Credit card information	150 (73.2%)

	Financial information	147 (71.7%)
	Medical information	109 (53.2%)
	Proprietary information	106 (51.7%)
	Other information	11 (5.4%)
Organization Information	Has an online presence	179 (87.3%)
	Has a mobile presence	117 (57.1%)
	Provides products or services online	131 (63.9%)
	Purchases online	152 (74.1%)
	Provides products or services directly to the general public	169 (82.4%)
	Provides products or services both to the public and to other businesses/ organizations	144 (70.2%)
	Provides products or services only to other businesses/organizations	72 (35.1%)
	Provides products or services that do not fall into any of the above categories	61 (29.8%)
Country	United States	205 (100%)

To compare demographic information between sample 1 and sample 2 see Table 7.2.

Table 7.2

Descriptive Statistics of Survey 2 Respondents from Sample 1 (N = 315) and from Sample 2 (N = 205)

		Sample 1 *N* = 315	Sample 2 *N* = 205
Gender	Male	73 (23.2%)	54 (26.3%)
	Female	242 (76.8%)	151 (73.7%)
Age	18 – 24 years	29 (9.2%)	12 (5.9%)
	25 – 34 years	138 (43.8%)	75 (36.6%)
	35 – 44 years	65 (20.6%)	36 (17.6%)
	45 – 54 years	51 (16.2%)	43 (21.0%)
	55 - 64 years	27 (8.6%)	32 (15.6%)
	65 - 74 years	5 (1.6%)	7 (3.4%)
Education	High school graduate, diploma or the equivalent (i.e. GED)	31 (9.8%)	18 (8.8%)
	Some college or university, but no degree	53 (16.8%)	34 (16.6%)
	Trade/technical/vocational training	17 (5.4%)	7 (3.4%)
	Associate degree	42 (13.3%)	32 (15.6%)
	Bachelor's degree	132 (41.9%)	80 (39.0%)
	Master's degree	31 (9.8%)	22 (10.7%)
	Professional degree	4 (1.3%)	5 (2.4%)
	Doctorate degree	4 (1.3%)	6 (2.9%)
	Other	1 (0.3%)	1 (0.5%)
Level of Position	Senior Management	36 (11.4%)	28 (13.7%)
	Middle Management	89 (28.3%)	58 (28.3%)
	Technical	50 (15.9%)	29 (14.1%)
	Clerical/Labour/Other Support	115 (36.5%)	66 (32.2%)
	Other	25 (7.9%)	24 (11.7%)
Profession or Occupation	Administrative Support	67 (21.3%)	37 (18.0%)
	Arts and Entertainment	8 (2.5%)	0 (0.0%)
	Engineer	4 (1.3%)	2 (1.0%)
	Financial	13 (4.1%)	19 (9.3%)

	Human Resources	14 (4.4%)	7 (3.4%)
	Information Technology	33 (10.5%)	25 (12.2%)
	Law Enforcement	3 (1.0%)	0 (0.0%)
	Legal	6 (1.9%)	1 (0.5%)
	Medical	39 (12.4%)	35 (17.1%)
	Privacy Officer	0 (0.0%)	0 (0.0%)
	Professor / Teacher	12 (3.8%)	8 (3.9%)
	Sales and Marketing	38 (12.1%)	27 (13.2%)
	Science	4 (1.3%)	3 (1.5%)
	Security	0 (0.0%)	1 (0.5%)
	Student	1 (0.3%)	0 (0.0%)
	Transport	2 (0.6%)	1 (0.5%)
	Other	71 (22.5%)	39 (19.0%)
Sector of Organization	Public	148 (47.0%)	97 (47.3%)
	Private	121 (38.4%)	81 (39.5%)
	Not-for-Profit	40 (12.7%)	25 (12.2%)
	Other	6 (1.9%)	2 (1.0%)
	Accommodation and Food Services	14 (4.4%)	8 (3.9%)
	Administrative and Support, Waste Management and Remediation Services	1 (0.3%)	0 (0.0%)
	Agriculture, Forestry, Fishing and Hunting	4 (1.3%)	1 (0.5%)
	Airline	1 (0.3%)	0 (0.0%)
	Arts, Entertainment and Recreation	12 (3.8%)	0 (0.0%)
	Construction	9 (2.9%)	5 (2.4%)
	Educational Services	40 (12.7%)	16 (7.8%)
	Finance and Insurance	26 (8.3%)	20 (9.8%)
	Food and Beverage	5 (1.6%)	3 (1.5%)
	Government	15 (4.8%)	9 (4.4%)
	Health Care and Social Assistance	57 (18.1%)	54 (26.3%)
	Information and Cultural Industries	3 (1.0%)	4 (2.0%)
	Legal	8 (2.5%)	3 (1.5%)
	Management of Companies and Enterprises	1 (0.3%)	4 (2.0%)
	Manufacturing	14 (4.4%)	7 (3.4%)

	Mining, Quarrying, and Oil and Gas Extraction	0 (0%)	2 (1.0%)
	Other Services (except Public Administration)	9 (2.9%)	4 (2.0%)
	Professional, Scientific and Technical Services	21 (6.7%)	9 (4.4%)
	Public Administration	1 (0.3%)	1 (0.5%)
	Real Estate and Rental and Leasing	2 (0.6%)	5 (2.4%)
	Retail Trade	32 (10.2%)	22 (10.7%)
	Telecommunications Industry	7 (2.2%)	6 (2.9%)
	Transportation and Warehousing	3 (1.0%)	2 (1.0%)
	Utilities	2 (0.6%)	1 (0.5%)
	Wholesale Trade	6 (1.9%)	5 (2.4%)
	Other	22 (7.0%)	14 (6.8%)
Size of Organization	Very small (1-50 employees)	83 (26.3%)	40 (19.5%)
	Small (51-100 employees)	27 (8.6%)	21 (10.2%)
	Medium (101 - 500 employees	63 (20.0%)	46 (22.4%)
	Large (>500 employees)	139 (44.1%)	93 (45.4%)
	Do not know	3 (1.0%)	5 (2.4%)
Information used by Organization	Personal information	286 (90.8%)	191 (93.2%)
	Credit card information	235 (74.6%)	150 (73.2%)
	Financial information	222 (70.5%)	147 (71.7%)
	Medical information	144 (45.7%)	109 (53.2%)
	Proprietary information	142 (45.1%)	106 (51.7%)
	Other information	16 (5.1%)	11 (5.4%)
	Has an online presence	282 (89.5%)	179 (87.3%)
	Has a mobile presence	177 (56.2%)	117 (57.1%)
	Provides products or services online	184 (58.4%)	131 (63.9%)
	Purchases online	246 (78.1%)	152 (74.1%)
	Provides products or services directly to the general public	258 (81.9%)	169 (82.4%)
	Provides products or services both to the public and to other businesses/ organizations	218 (69.2%)	144 (70.2%)

	Provides products or services only to other businesses/organizations	92 (29.2%)	72 (35.1%)
	Provides products or services that do not fall into any of the above categories	99 (31.4%)	61 (29.8%)
Country	United States	315 (100%)	205 (100%)

Data Collection and Analysis

A pilot study or soft launch of my survey was conducted on January 8th, 2016 with 30 participants. Once I verified the survey data to be accurate, the official launch of my *Privacy Management Survey* continued on January 14th, 2016. Sample 1 consisted of 315 complete surveys. Sample 2 (N = 205) was collected on February 12th, 13th and 14th, 2016. Two open-ended questions were asked regarding concerns about the privacy of personal information and about network traffic. The remaining questions were answered by selecting the best answer on the seven-point scale that is anchored with "strongly disagree" and "strongly agree." Data collection for study 2 is described in Chapter 4.

Data was analyzed using IBM SPSS version 24 principal components analysis. Dimension reduction was applied to reduce the number of variables. Models were created using IBM AMOS 24. Standardized estimates of privacy practices, experienced harms, brand protection and brand value from Sample 1 are provided in Figure 5.3. Privacy concerns are included in Figure 6.9 with the standardized estimates for privacy practices, experienced harms, brand protection and brand value.

Results

Scales are developed for the constructs: brand protection, brand value, experienced harm, privacy concerns and privacy practices in this chapter for the second data sample (N = 205) and compared to the scales developed for the first data sample (N = 315) from the Privacy Management Survey. The scales are a contribution to the literature. The scales are used in the quantitative research developing a privacy-brand model and enhanced model. Scales were developed and tested using reliability analysis in SPSS. Analyzing the total score descriptive statistics indicated if the scale would be more internally consistent if an item were removed. Cronbach's alpha coefficient was also examined to determine the internal consistency of the scales. Tavakol & Dennick (2011) report that there are different acceptable values of alpha, ranging from 0.70 to 0.95. Privacy breach was found in sample 1 to collapse onto the same component with experienced harms. The Scales for the variables retained were tested using reliability analysis and are provided in Table 7.3 for Sample 1 (N = 315) and in Table 7.2 for Sample 2 (N = 205).

Table 7.3

Reliability Analysis Statistics, Sample One (N = 315)

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Brand protection	0.948	0.950	10
Brand value	0.940	0.941	8
Experienced harms	0.965	0.966	10
Privacy breach	0.925	0.925	6
Privacy concerns	0.958	0.959	10
Privacy practices	0.947	0.948	8

Table 7.4

Reliability Analysis Statistics, Sample Two (N = 205)

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Brand protection	0.950	0.951	8
Brand value	0.942	0.942	6
Experienced harms	0.975	0.975	10
Privacy concerns	0.956	0.957	13
Privacy practices	0.886	0.895	5

The statements retained for each scale for both samples are provided and compared in Tables 7.5 to 7.9. The mean values for each sample are also included.

Table 7.5

Brand Protection Scales

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
1	n/a	BP_ABUSE	My organization has a privacy program to prevent digital brand abuse.	4.99	5.02
2	n/a	BP_AUDIT	My organization conducts privacy audits.	4.93	5.11
3	n/a	BP_CO_ST	My organization provides communication to stakeholders and users regarding data privacy awareness.	5.03	5.24
4	n/a	BP_H_MOD	My organization uses privacy management models.	5.06	5.04
5	n/a	BP_PIAS	My organization conducts privacy impact assessments (PIAs).	4.74	4.87
6	n/a	BP_RECOR	My organization reviews holdings, disposes of transitory records and classifies remaining records at the appropriate security level.	5.29	5.36
n/a	1	BP_H_BP	My organization has best practices use for privacy.	5.69	5.68
n/a	2	BP_H_DBP	My organization has a policy in place so employees know what to do if there is a data breach.	5.46	5.48
n/a	3	BP_H_PPR	My organization has a privacy program.	5.62	5.60
n/a	4	BP_TR_AS	My organization extends privacy training to all stakeholders (i.e. employees, clients).	4.73	4.95

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
n/a	5	BP_TR_CL	My organization educates clients to help manage the risk of client loss resulting from corporate identity theft.	4.95	5.03
n/a	6	BP_TR_FR	My organization provides mandatory training on personal privacy protection at least every two years.	5.19	5.40
n/a	7	BP_TR_PA	My organization trains employees about the federal *Privacy Act (PA).*	5.30	5.47
n/a	8	BP_TR_PR	My organization extends training on personal privacy protection to partners.	4.79	4.88

Table 7.6

Brand Value Scales

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
1	1	BV_ORG_B	My organization is a good brand.	5.69	5.76
n/a	n/a	BV_ORG_C	What I get from my organization is worth the cost.	4.94	4.96
2	2	BV_ORG_G	My organization does me good.	5.57	5.60
n/a	n/a	BV_ORG_P	I feel great pride identifying with my organization.	5.41	5.48
3	n/a	BV_ORG_Q	What my organization delivers feels right for me.	5.50	5.59
4	n/a	BV_ORG_R	What my organization delivers feels right for me.	5.52	5.55
5	3	BV_ORG_S	My organization is a satisfying buy.	5.50	5.53
6	4	BV_ORG_T	I feel I am able to trust my organization completely.	5.39	5.46
7	5	BV_ORG_U	The uniqueness of my organization stands out.	5.31	5.35
n/a	6	BV_ORG_W	What I get from my organization is worth the cost.	5.37	5.37

Table 7.7

Experienced Harms Scales

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
n/a	1	H_ABUSE	My organization has experienced digital brand abuse.	2.11	1.97
1	2	H_BRVAL	My organization has experienced damaged brand value because of a data breach.	2.06	1.99
2	n/a	H_COSTS	My organization has experienced litigation costs because of a data breach.	2.18	2.02
n/a	3	H_CUSTRS	My organization has experienced loss of customer trust because of a data breach.	2.16	1.98
n/a	4	H_DBATK	My organization's database of personal information has been changed maliciously.	2.13	1.89
n/a	5	H_DNABU	My organization has experienced abuse of its domain name.	2.06	1.98
3	6	H_IDTHF	My organization has experienced identity theft.	2.14	1.98
n/a	7	H_PS	A data breach has caused my organization to affect public safety.	1.93	1.83
4	n/a	H_REVNUE	My organization has experienced lost revenue because of a data breach.	2.13	2.07
n/a	8	H_STROY	Personal information held by my organization has been maliciously destroyed.	2.03	1.88
n/a	9	H_TM	My organization has experienced online trademark infringements.	2.08	1.97
n/a	10	H_TRAFF	My organization has experienced web traffic diversions.	2.18	1.96

Table 7.8

Privacy Concerns Scales

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
n/a	1	PC_EMAIL	I am concerned about the privacy of my email messages.	4.83	4.66
1	n/a	PC_EXPOR	I am concerned about export of data to jurisdictions with lax privacy laws.	5.04	4.73
n/a	2	PC_IDTHF	I am concerned about identity theft.	5.58	5.56
n/a	3	PC_LKCTR	I am concerned about the lack of privacy control online.	5.28	5.18
2	n/a	PC_LOCAT	I am concerned about location tracking.	5.15	5.00
3	n/a	PC_NETTR	I am concerned that network traffic is leaking private data.	4.98	4.93
n/a	4	PC_ONBNK	I am concerned about online banking.	4.40	4.25
4	5	PC_PASWD	I am concerned about privacy of passwords.	5.28	5.15
5	6	PC_PIAVL	I am concerned that personal information is readily available and that risks are not communicated to the public.	5.32	5.23
n/a	7	PC_PURCH	I am concerned about tracking purchase habits.	4.97	5.01
6	8	PC_REGIS	I am concerned that online registration is easily compromised.	5.09	4.89
7	9	PC_REPUT	I am concerned that someone may hijack my account and ruin my reputation.	4.93	4.83
8	10	PC_RIGHT	I am concerned about the lack of privacy rights.	5.25	5.16

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
9	11	PC_SHARE	I am concerned that personal data obtained is shared with others.	5.43	5.30
n/a	12	PC_VIRUS	I am concerned about viruses / spyware / malware / EXE files / Multimedia files.	5.67	5.54
n/a	13	PC_WIRHM	I am concerned about the privacy of wireless access at home.	4.82	4.73
10	n/a	PC_WIRPB	I am concerned about the privacy of wireless access at public hot spots.	5.43	5.40

Table 7.9

Privacy Practices Scales

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
1	n/a	PP_ACCUR	My organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.	6.14	6.24
2	1	PP_DISCL	My organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.	6.30	6.42
3	2	PP_FAIR	My organization collects information by fair and lawful means.	6.30	6.50

Sample 1 Scale	Sample 2 Scale	VAR Name	Question	Mean *N* = 315	Mean *N* = 205
4	n/a	PP_MINIM	My organization limits the collection of personal information to that which is necessary for the purposes identified by the organization.	5.90	6.11
5	n/a	PP_PURPO	My organization identifies the purposes for which personal information is collected at or before the time the information is collected.	6.03	5.99
6	3	PP_RESPO	My organization is responsible for personal information under its control	6.12	6.34
7	4	PP_RETEN	My organization retains personal information only as long as necessary for the fulfillment of the purposes, which it was collected, except with the consent of the individual or as required by law.	6.09	6.09
8	5	PP_SECUR	My organization protects personal information by security safeguards appropriate to the sensitivity of the information.	6.13	6.37

For comparison with sample 2 the confirmatory factor analysis of standardized estimates of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value from sample 1 (N = 315) is presented in Figure 7.1.

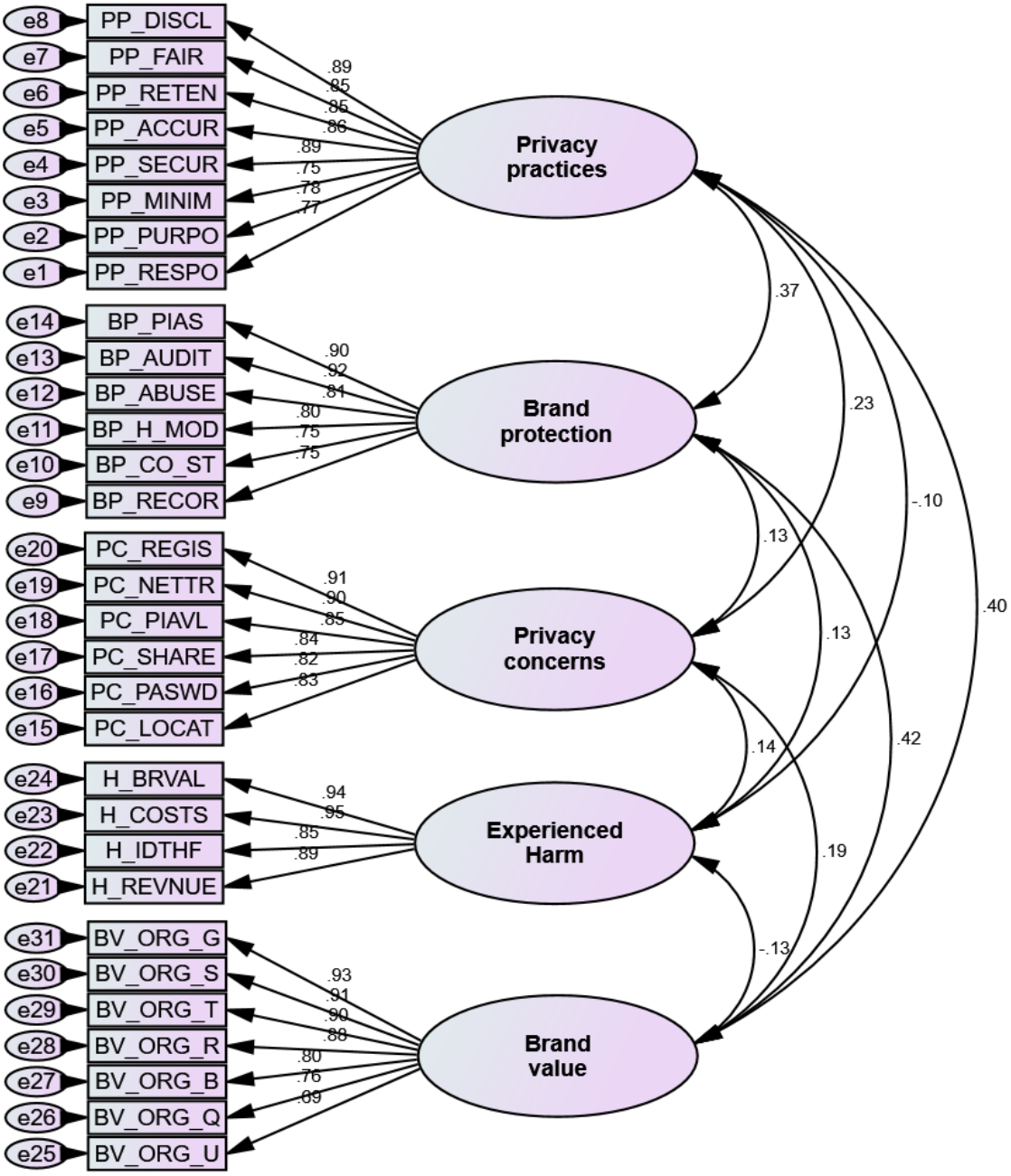


Figure 7.1. Sample 1 Confirmatory Factor Analysis of Standardized Estimates of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

The structural equation model built with sample 1 with covariances between Privacy Concerns, Privacy Practices, and Brand Protection to Experienced Harms and Brand Value is displayed in Figure 7.2.

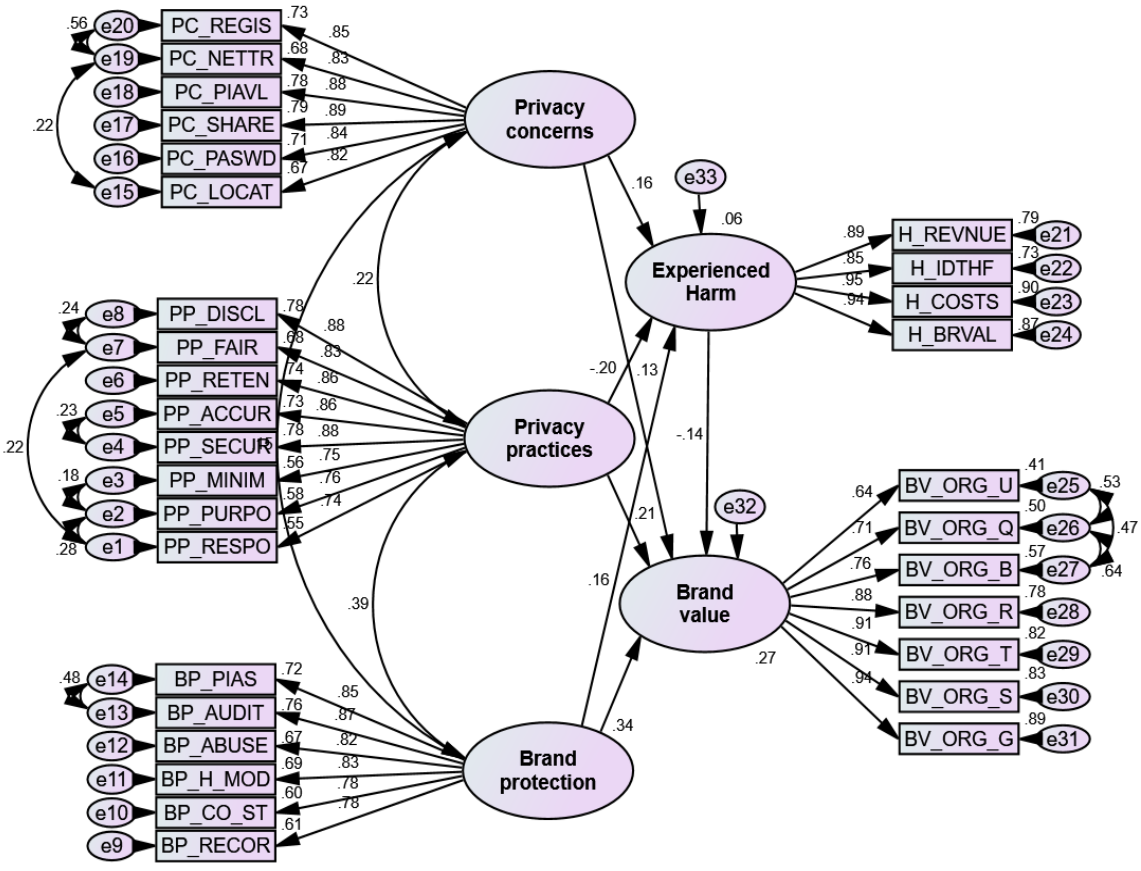


Figure 7.2. Sample 1 Structural Equation Model with Covariances between Privacy Concerns, Privacy Practices and Brand Protection to Experienced Harms and Brand Value.

To help visualize the Hypotheses they are included in the Structural Equation Model built with data from sample 1 (see Figure 7.3).

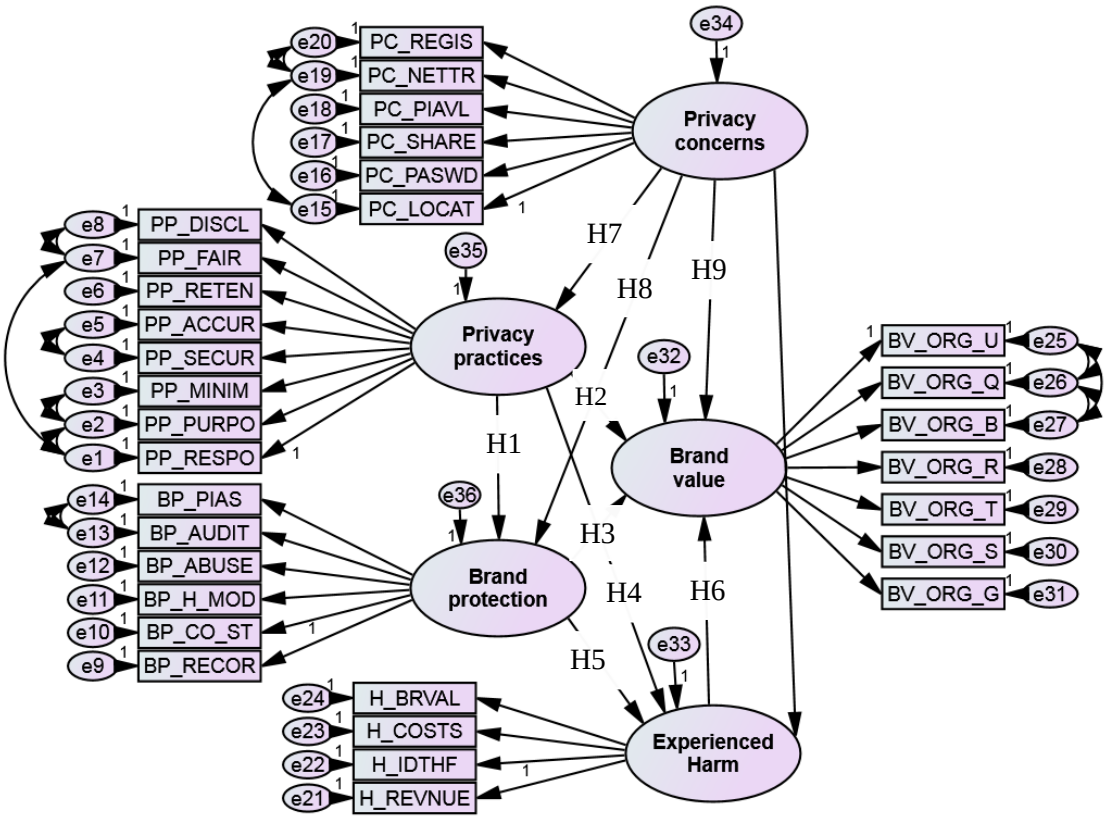


Figure 7.3. Hypotheses Included in Sample 1 Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

The mediated, structural equation Privacy-Brand Model I developed from sample 1 (N = 315) is displayed in Figure 7.4 ($\chi^2(414) = 684$, χ^2 /df = 1.653, p = .000; NFI = .929; CFI = .971; RMSEA = .046, p= <.001). The CFI and NFI yielded values of .971 and .929, respectively, indicating a good fit of the model. The RMSEA is .046 also indicating an excellent fit since it is < .06 (Meyers et al., 2017).

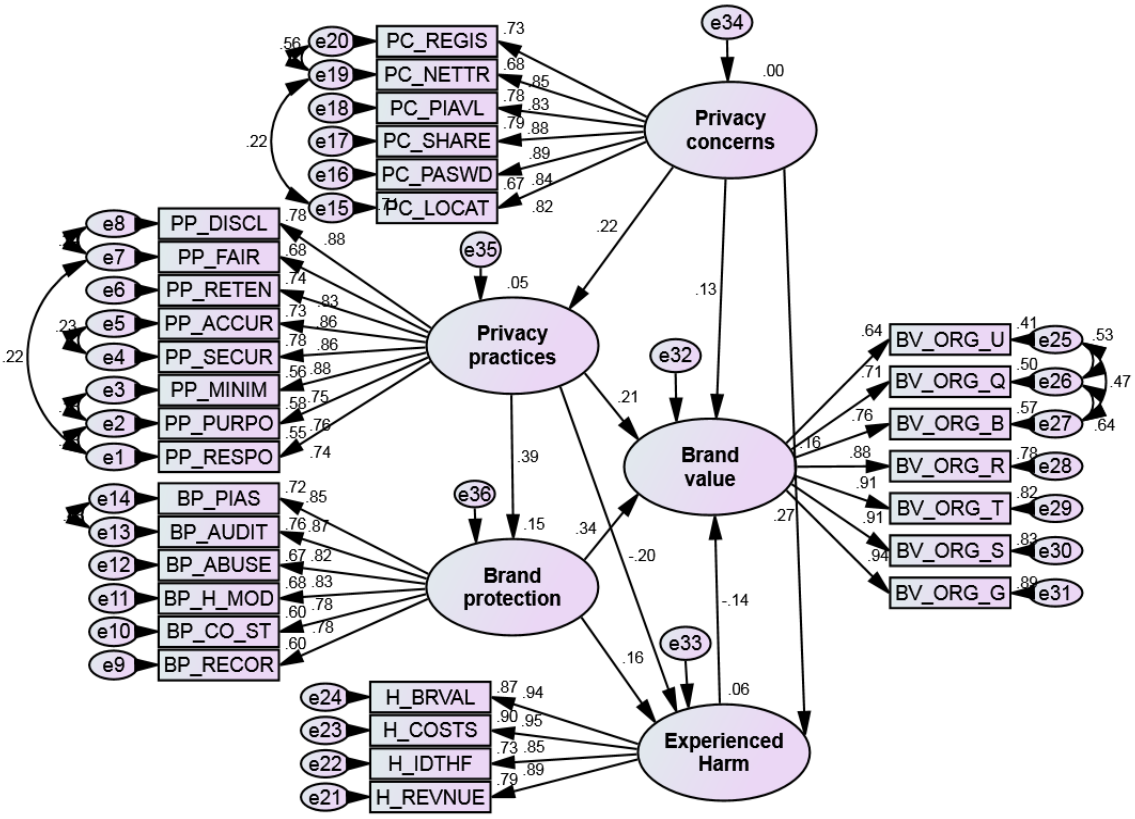


Figure 7.4. Sample 1 Structural Equation Model of Standardized Estimates of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

All hypotheses are statistically significant except for H8 Privacy concerns to Brand protection. The regression weights for sample 1 (*N* = 315) are provided in Table 7.10 and the standardized regression weights are provided in Table 7.11.

Table 7.10

Regression Weights for Sample 1 (N = 315)

			Estimate	S.E.	C.R.	P
Privacy_practices	←	Privacy_concerns	0.157	0.044	3.593	***
Brand_protection	←	Privacy_practices	0.503	0.08	6.27	***
Experienced_Harm	←	Brand_protection	0.169	0.069	2.436	0.015
Experienced_Harm	←	Privacy_practices	-0.271	0.091	-2.992	0.003
Experienced_Harm	←	Privacy_concerns	0.155	0.059	2.61	0.009
Brand_value	←	Privacy_concerns	0.084	0.036	2.323	0.020
Brand_value	←	Experienced_Harm	-0.097	0.036	-2.677	0.007
Brand_value	←	Brand_protection	0.244	0.046	5.265	***
Brand_value	←	Privacy_practices	0.194	0.057	3.413	***

Table 7.11

Standardized Regression Weights for SEM for Sample 1 (N = 315)

			Estimate
Privacy_practices	←	Privacy_concerns	0.218
Brand_protection	←	Privacy_practices	0.392
Experienced_Harm	←	Brand_protection	0.159
Experienced_Harm	←	Privacy_practices	-0.199
Experienced_Harm	←	Privacy_concerns	0.157
Brand_value	←	Privacy_concerns	0.128
Brand_value	←	Experienced_Harm	-0.145
Brand_value	←	Brand_protection	0.342
Brand_value	←	Privacy_practices	0.213

The next group of figures (7.5, 7.6 and 7.7) show the process of building models using sample 2 data. Confirmatory factor analysis for sample 2 (N = 205) of standardized estimates of Privacy Practices, Experienced Harms, Brand Protection and Brand Value in displayed in Figure 7.5.

The confirmatory factor analysis of standardized estimates for sample 2, which added Privacy Concerns to create the extended model, is presented in Figure 7.6.

Error terms were covaried to improve the model fit (see Figure 7.7).

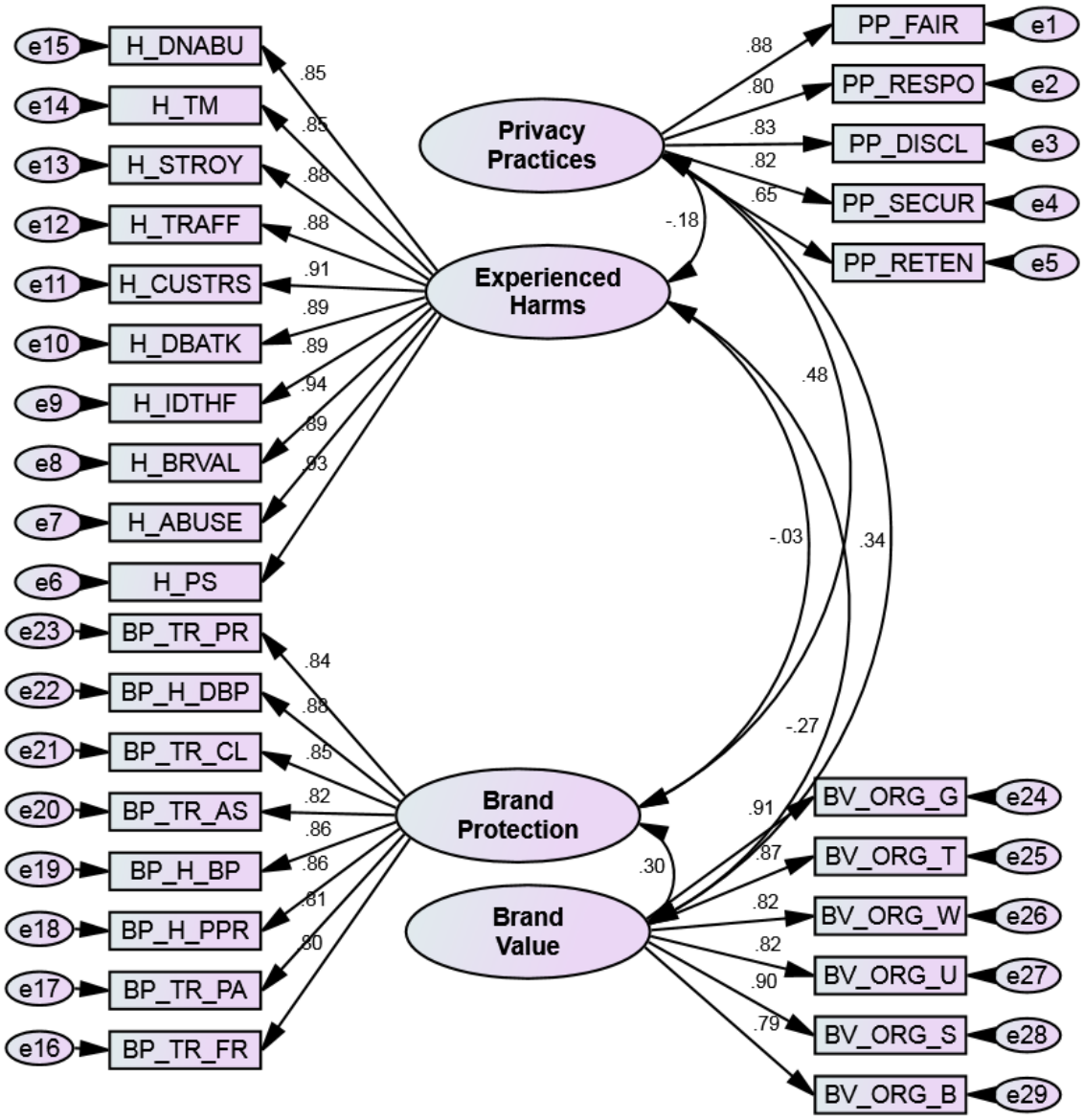


Figure 7.5. Sample 2 Confirmatory Factor Analysis of Standardized Estimates of Privacy Practices, Experienced Harms, Brand Protection and Brand Value.

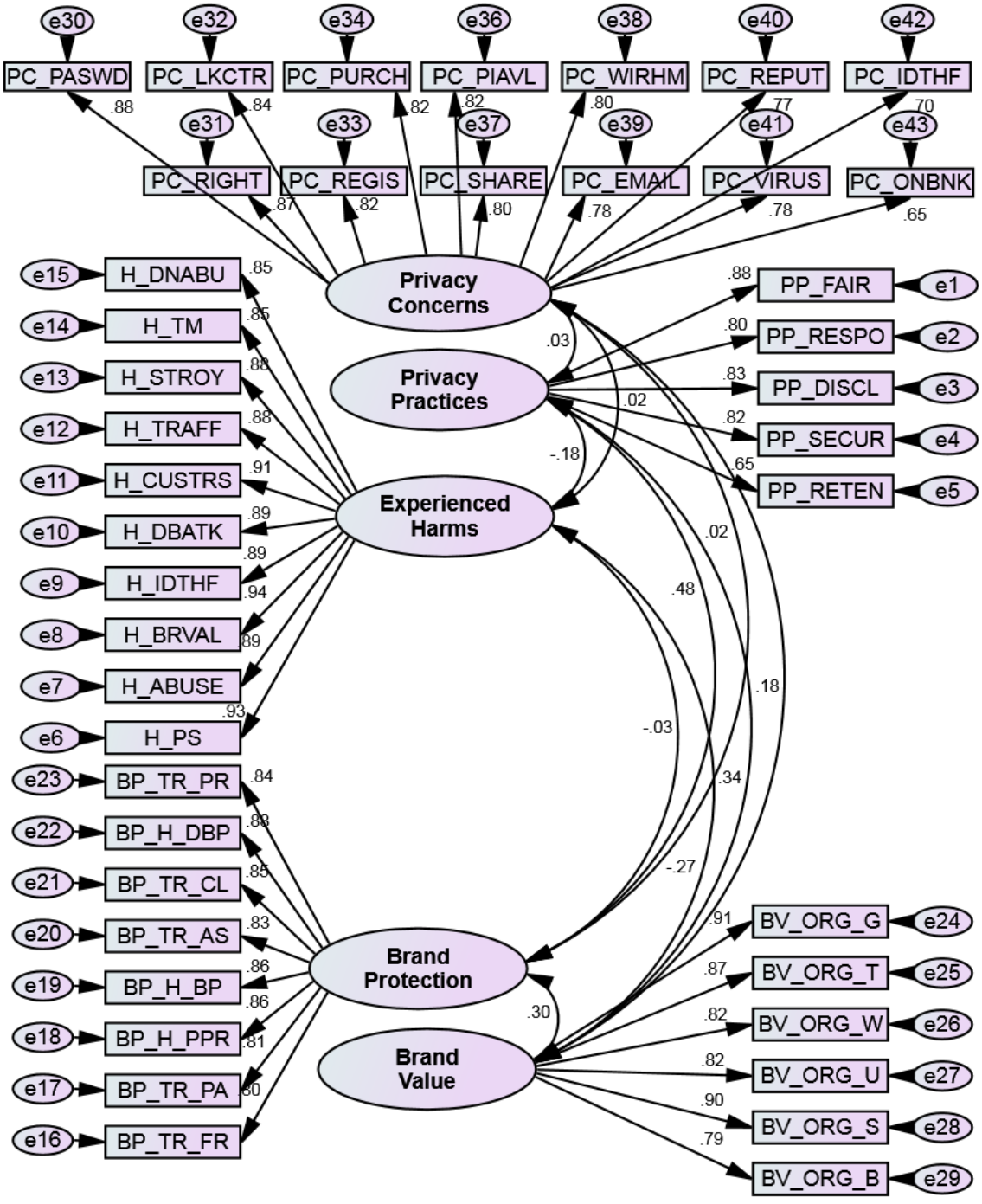


Figure 7.6. Sample 2 Confirmatory Factor Analysis of Standardized Estimates Adding Privacy Concerns to Privacy Practices, Experienced Harms, Brand Protection and Brand Value.

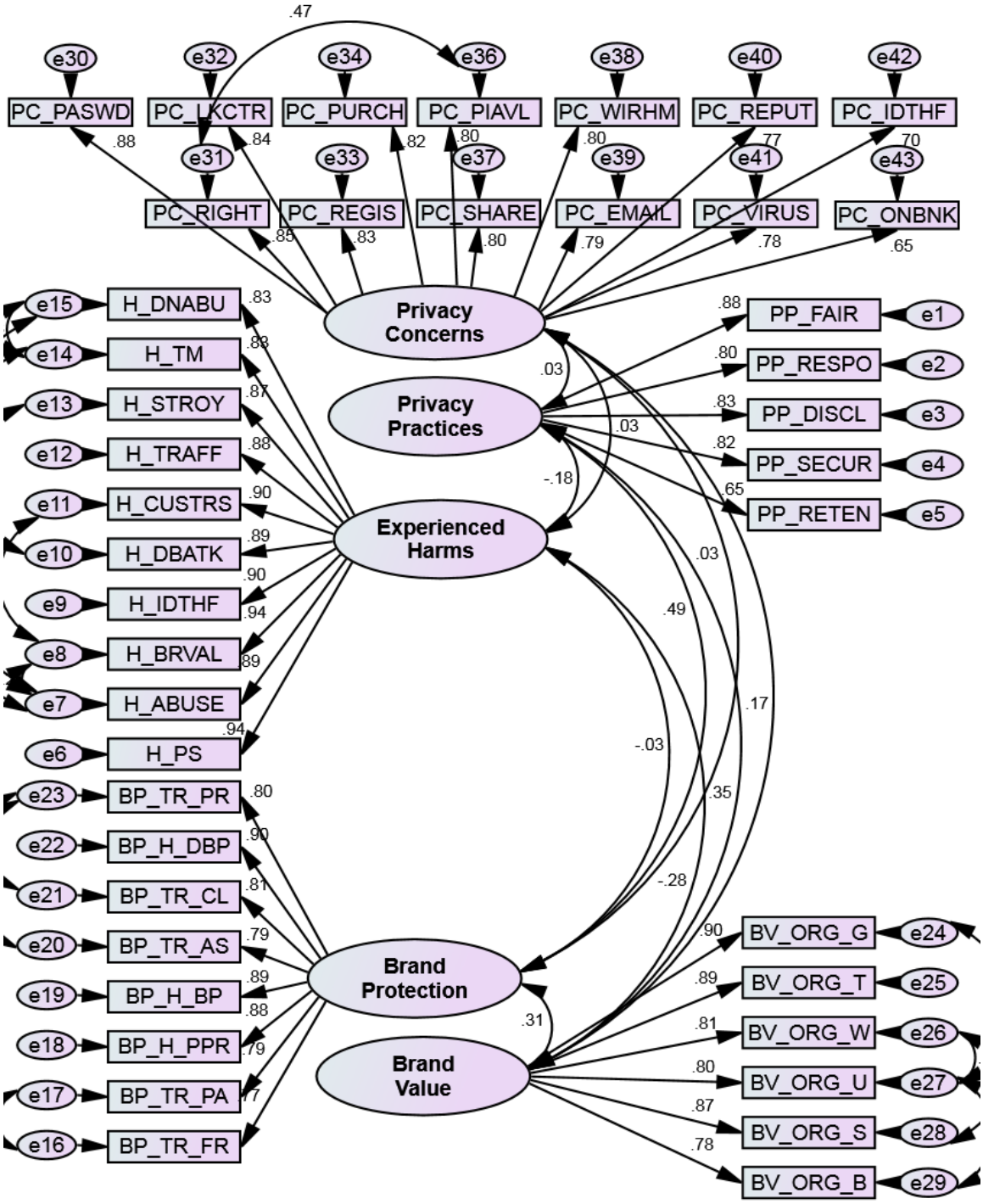


Figure 7.7. Sample 2 Confirmatory Factor Analysis of Expanded Privacy-Brand Model including Privacy Concerns with Error Terms Covaried.

A structural equation model created from my improved confirmatory factor analysis in AMOS using data from sample 2 is presented in Figure 7.8. Covariances are placed between Privacy Practices, Brand Protection, Privacy Concerns, and Experienced Harms to Brand Value.

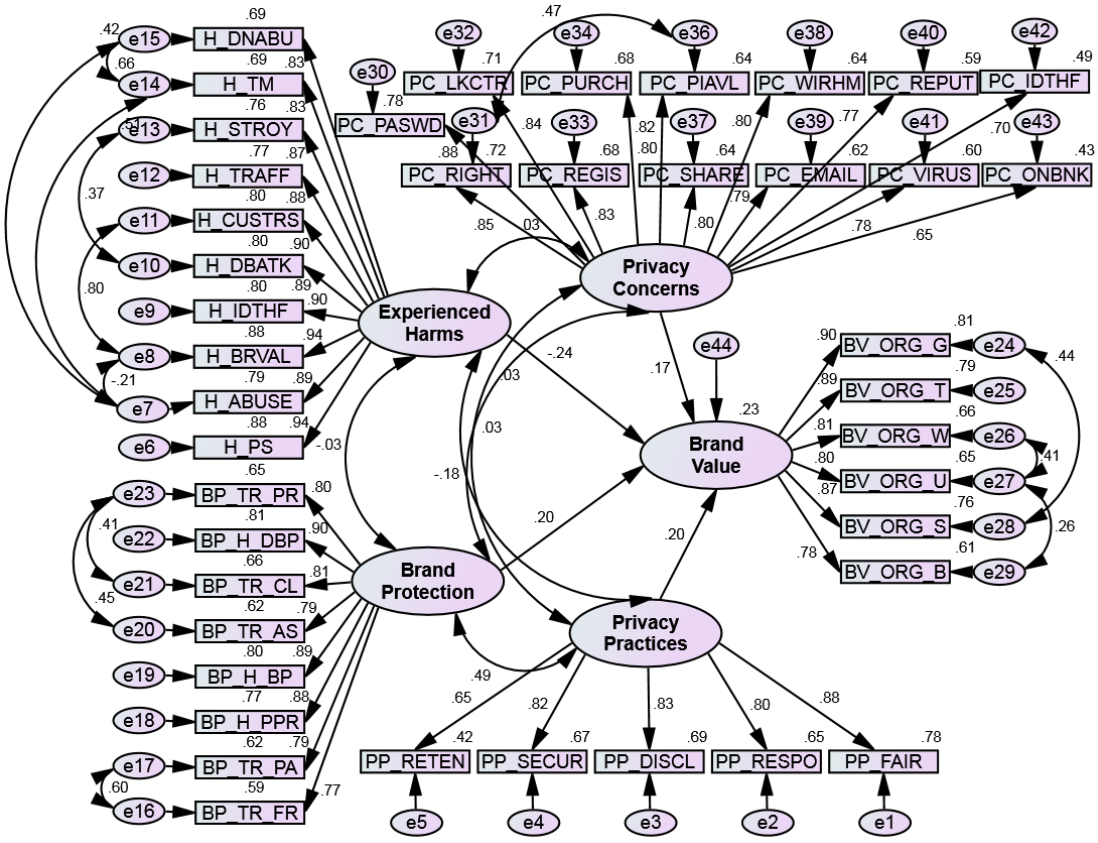


Figure 7.8. Sample 2 Structural Equation Model with Covariances Between Privacy Practices, Brand Protection, Privacy Concerns, and Experienced Harms to Brand Value.

The Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value created from data from sample 1 (N = 315) tested using data from sample 2 (N = 205) is displayed in Figure 7.9 ($\chi^2(413)$ = 736, χ^2 /df = 1.781, p = .000; NFI = .881; CFI = .943; RMSEA = .062, p= <.001). The CFI is .943 indicating a good fit of the model. NFI is .881 indicating an acceptable fit of the model. The RMSEA is .062 also indicating a good fit since it is close to .06 (Meyers et al., 2017).

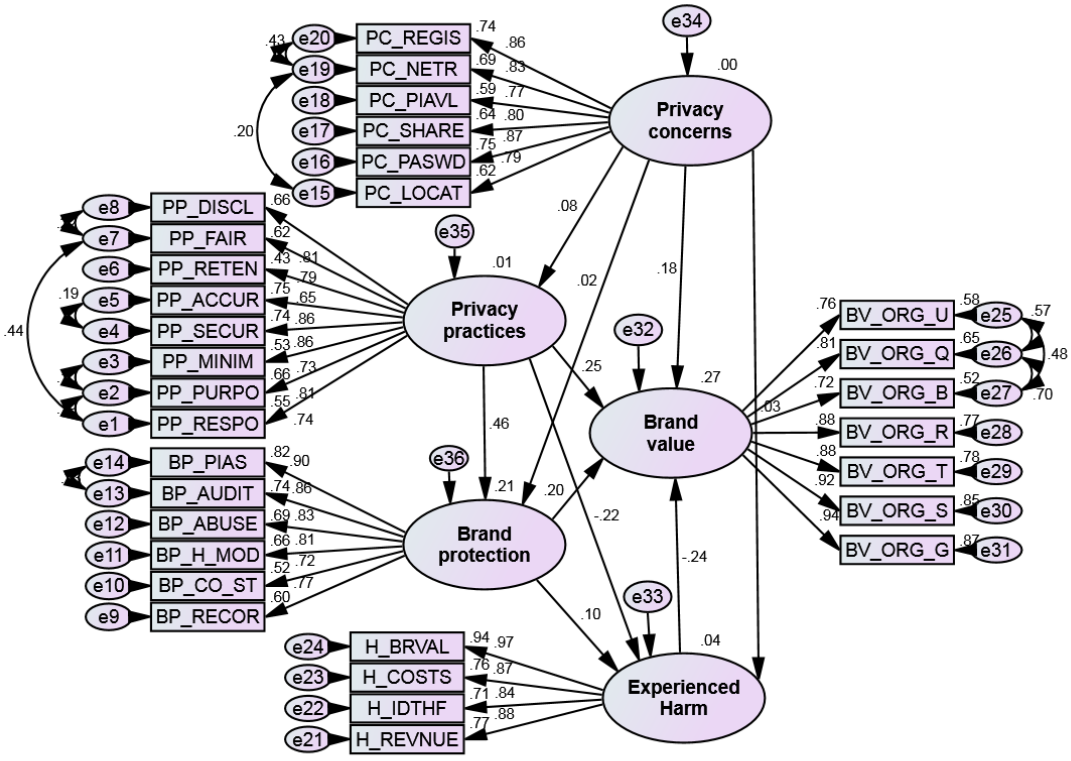


Figure 7.9. Structural Equation Model Testing All Hypotheses Using Sample 1 Model with Sample 2 Data.

All hypotheses are statistically significant except for H5. Brand protection to Experienced Harms, H7. Privacy concerns to Privacy practices, and H8. Privacy concerns to Brand protection. The regression weights for sample 2 (N = 205) are provided in Table 7.12 and the standardized regression weights are provided in Table 7.13.

Table 7.12

Regression Weights for Sample 2 (N = 205)

			Estimate	S.E.	C.R.	P
Privacy_practices	←	Privacy_concerns	.053	.048	1.107	.268
Brand_protection	←	Privacy_practices	.727	.126	5.777	***
Brand_protection	←	Privacy_concerns	.016	.068	.240	.811
Experienced_Harm	←	Privacy_practices	-.338	.134	-2.515	.012
Experienced_Harm	←	Brand_protection	.101	.083	1.218	.223
Experienced_Harm	←	Privacy_concerns	.027	.072	.370	.711
Brand_value	←	Privacy_concerns	.143	.052	2.725	.006
Brand_value	←	Experienced_Harm	-.190	.054	-3.536	***
Brand_value	←	Brand_protection	.158	.061	2.606	.009
Brand_value	←	Privacy_practices	.314	.100	3.144	.002

Table 7.13

Standardized Regression Weights for SEM for Sample 2 (N = 205)

			Estimate
Privacy_practices	←	Privacy_concerns	0.085
Brand_protection	←	Privacy_practices	0.458
Brand_protection	←	Privacy_concerns	0.017
Experienced_Harm	←	Privacy_practices	-0.216
Experienced_Harm	←	Brand_protection	0.102
Experienced_Harm	←	Privacy_concerns	0.027
Brand_value	←	Privacy_concerns	0.183
Brand_value	←	Experienced_Harm	-0.237
Brand_value	←	Brand_protection	0.200
Brand_value	←	Privacy_practices	0.250

The Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value created from data from sample 1 (N = 315) tested using data from sample 2 (N = 205) with only the constructs' hypotheses that are statistically significant connected is displayed in Figure 7.10 ($\chi^2(417) = 739$, χ^2 /df = 1.771, p = .000; NFI = .880; CFI = .944; RMSEA = .061, p= <.001). The CFI is .944 indicating a good fit of the model. NFI is .880 indicating an acceptable fit of the model. The RMSEA is .061 also indicating a good fit since it is very close to .06 (Meyers et al., 2017).

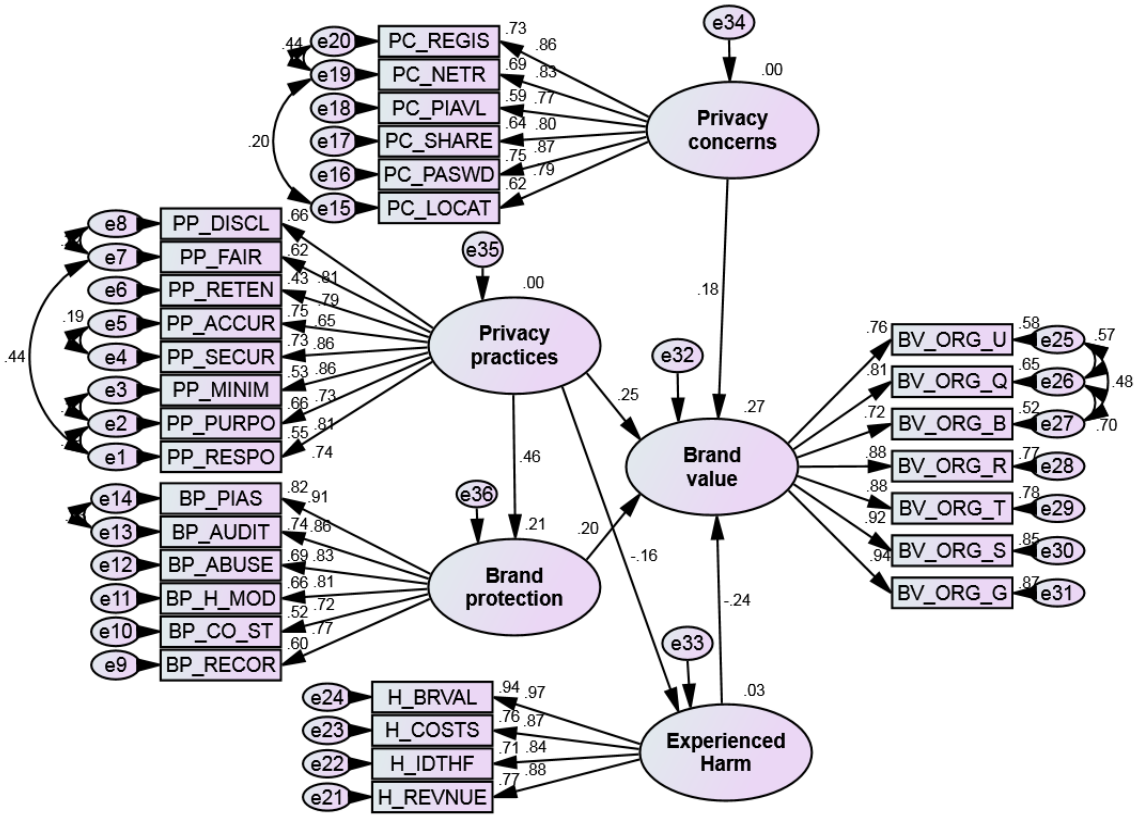


Figure 7.10. Final Structural Equation Model with Statistically Significant Hypotheses Using Sample 1 Model with Sample 2 Data.

The regression weights for sample 2 (*N* = 205) tested on sample 1 (*N* = 315) model are provided in Table 7.14 and the standardized regression weights are provided in Table 7.15.

Table 7.14

Regression Weights for Sample 2 (N = 205)

			Estimate	S.E.	C.R.	P
Experienced_Harm	←	Privacy_practices	-0.254	0.116	-2.187	0.029
Brand_protection	←	Privacy_practices	0.726	0.125	5.795	***
Brand_value	←	Privacy_concerns	0.144	0.052	2.762	0.006
Brand_value	←	Experienced_Harm	-0.189	0.053	-3.544	***
Brand_value	←	Brand_protection	0.157	0.06	2.617	0.009
Brand_value	←	Privacy_practices	0.315	0.098	3.203	0.001

Table 7.15

Standardized Regression Weights for SEM for Sample 2 (N = 205)

			Estimate
Experienced_Harm	←	Privacy_practices	-.163
Brand_protection	←	Privacy_practices	.458
Brand_value	←	Privacy_concerns	.185
Brand_value	←	Experienced_Harm	-.236
Brand_value	←	Brand_protection	.199
Brand_value	←	Privacy_practices	.252

To help visualize the Hypotheses that are statistically significant in the Structural Equation Model built with data from sample 1 and tested with data from sample 2 (see Figure 7.11).

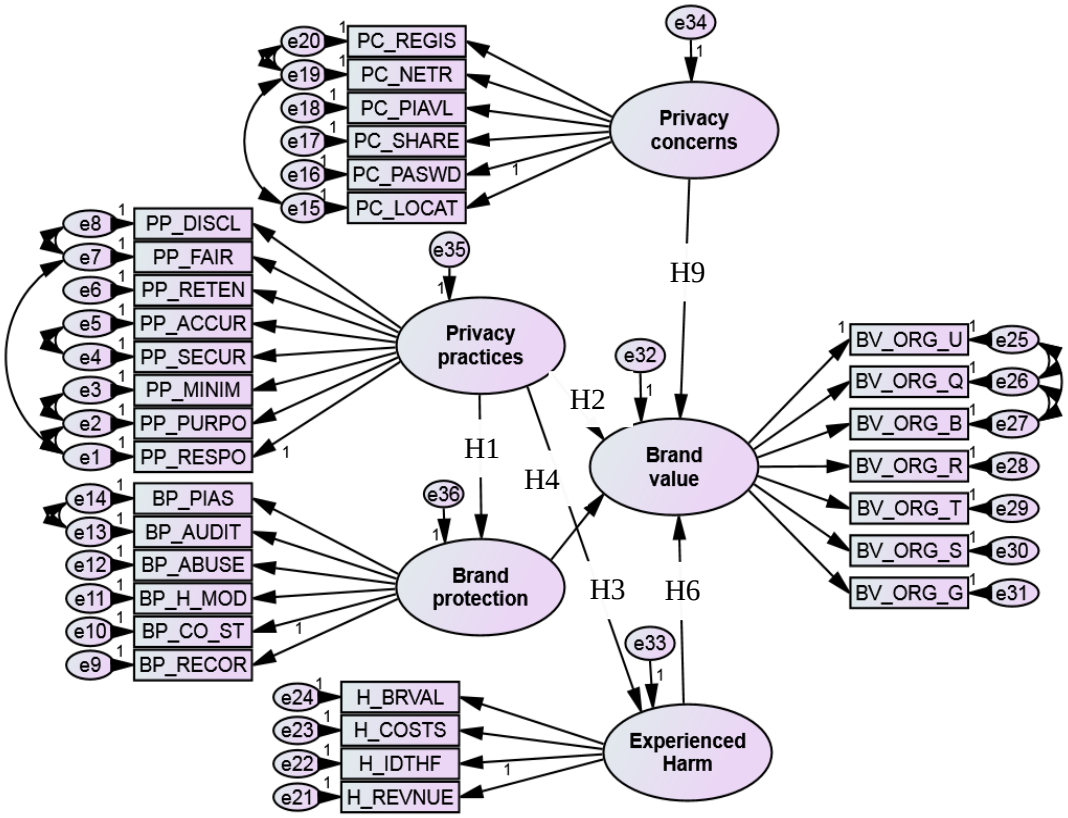


Figure 7.11. Hypotheses that are Statistically Significant in the Expanded Structural Equation Model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value.

A summary of the model fit for sample 1 (*N* = 315), sample 2 (*N* = 205) and the model made with sample 1 (*N* = 315) and tested with sample 2 (*N* = 205) data is provided in Table 7.16.

Table 7.16

Absolute, Relative, and Parsimonious Fit Measures for Models

Sample 1 (N = 315)

Fit Measures					
Absolute		Relative		Parsimonious	
Test	Value	Test	Value	Test	Value
χ^2	683	CFI	.971	PNFI	.827
GFI	.878	NFI	.929	PCFI	.864
RMR	.110	IFI	.970		
RMSEA	.046	RFI	.920		

Sample 2 (N = 205)

Fit Measures					
Absolute		Relative		Parsimonious	
Test	Value	Test	Value	Test	Value
χ^2	1347	CFI	.939	PNFI	.798
GFI	.773	NFI	.863	PCFI	.868
RMR	.136	IFI	.939		
RMSEA	.058	RFI	.852		

Tested Sample 1 (N = 315) Model with Sample 2 (N = 205) Data

Fit Measures					
Absolute		Relative		Parsimonious	
Test	Value	Test	Value	Test	Value
χ^2	739	CFI	.944	PNFI	.789
GFI	.817	NFI	.880	PCFI	.846
RMR	.153	IFI	.944		
RMSEA	.061	RFI	.866		

The Privacy-Brand model created with data from sample 1 had the best model fit ($\chi^2(414) = 689$, χ^2 /df = 1.666, p = .000; NFI = .93; CFI = .97; RMSEA = .046, p= <.001) compared to the model created from data from sample 2 (χ^2 (796) = 1347, χ^2 /df = 1.69, p = .000; NFI = .86; CFI = .94; RMSEA = .058, p=<.001). The model created with sample 1 data was selected because it had a better model fit and was tested using sample 2 data ($\chi^2(417) = 739$, χ^2 /df = 1.771, *p* = .000; NFI = .880; CFI = .944; RMSEA = .061, *p*= <.001).

My Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value created from data from sample 1 is displayed in Figure 7.12, using data from sample 2 is displayed in Figure 7.13 and using data from sample 2 tested on sample 1 model is displayed in Figure 7.14.

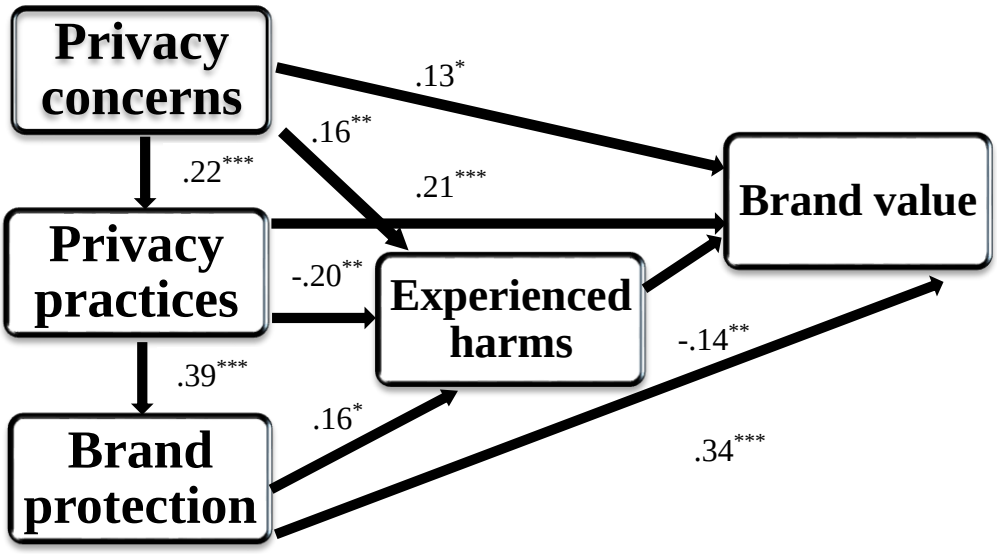


Figure 7.12. Sample 1 Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value.

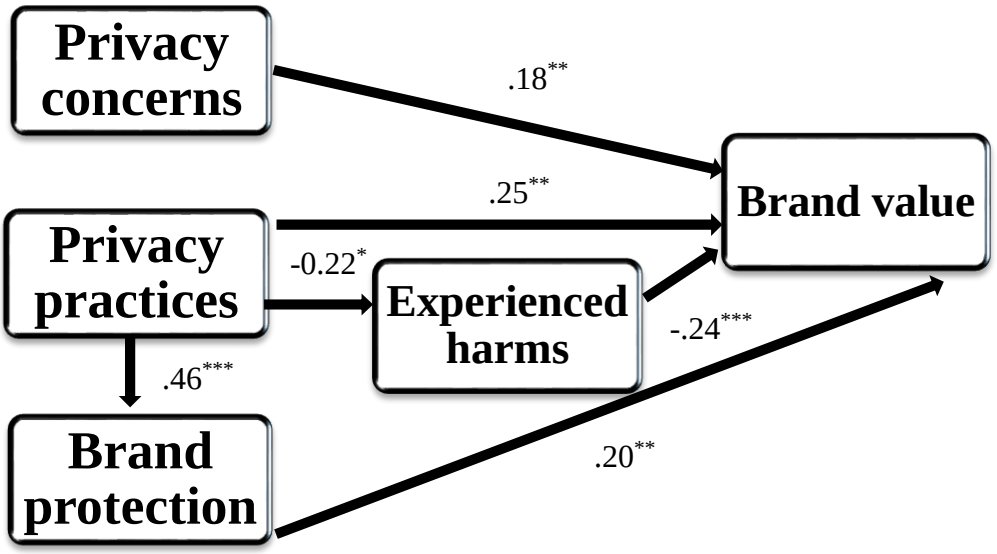


Figure 7.13. Sample 2 Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value.
Note: P < 0.05 *, P < 0.01 **, P < 0.001 ***

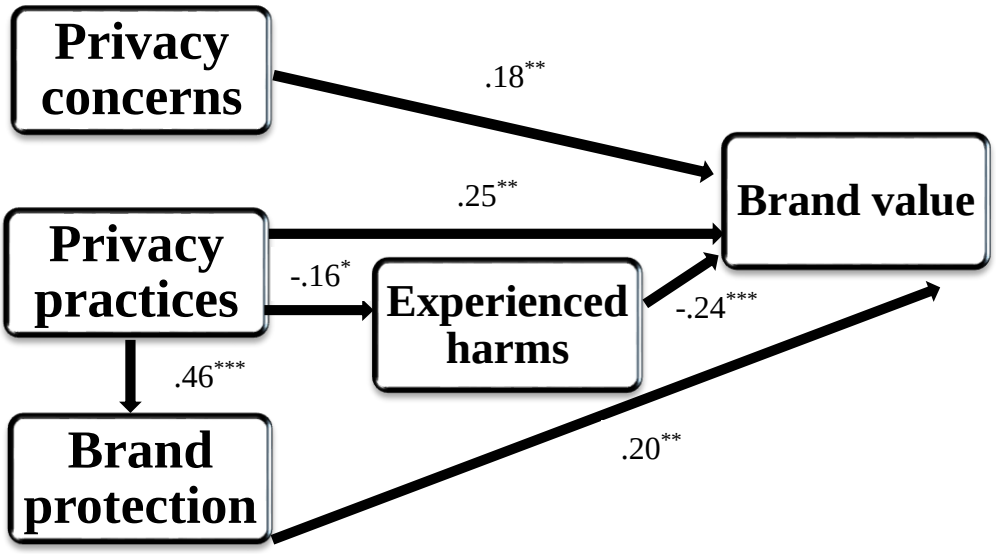


Figure 7.14. Sample 2 Tested on Sample 1 Expanded Privacy-Brand Model including Privacy Concerns, Privacy Practices, Brand Protection, Experienced Harms, and Brand Value.
Note: P < 0.05 *, P < 0.01 **, P < 0.001 ***

The Hypothesized Model

A confirmatory factor analysis (CFA), based on data from study 2 using the *Privacy Management Survey* was performed through AMOS on 13 scale items for privacy concerns, 10 scale items for experienced harms, 8 scale items for brand protection, 5 scale items for privacy practices and 6 scale items for brand value. The hypothesized model is presented in Figure 2.1 and the hypothesized expanded model is presented in Figure 6.1. The CFA model is presented in Figure 5.5 and the expanded CFA model is presented in Figure 6.6 where circles represent latent variables, and rectangles represent measured variables. If a line is absent connecting variables this implies that there is no

hypothesized direct effect. A five-factor model of privacy concerns, privacy practices, brand protection, experienced harms, and brand value is hypothesized.

Privacy concerns of email messages, identity theft, privacy control online, online banking, passwords, personal information is readily available and that risks are not communicated to the public, tracking purchase habits, online registration, hijack my account and ruin my reputation, lack of privacy rights, personal data obtained is shared with others, viruses / spyware / malware / EXE files / multimedia files, and wireless access at home serve as indicators of the privacy concerns factor.

Disclosure, collection by fair and lawful means, responsibility, retention, and security of personal information serve as indicators of the privacy practices factor.

Best practices use for privacy, data breach policy, privacy program, privacy training to all stakeholders, educates clients to help manage the risk of client loss resulting from corporate identity theft, mandatory training on personal privacy protection, trains employees about the *Privacy Act,* and provides training on personal privacy protection to partners serve as indicators of the brand protection factor.

Privacy breaches have caused digital brand abuse, damaged brand value, loss of customer trust, database of personal information changed maliciously, abuse of its domain name, identity theft, affected public safety, personal information has been maliciously destroyed, online trademark infringements, web traffic diversions serve as indicators of the experienced harms factor.

My organization is a good brand, does me good, is a satisfying buy, can trust my organization completely, uniqueness of my organization stands out, and what I get from my organization is worth the cost serve as indicators of the brand value factor.The five factors are hypothesized to covary with one another.

There were no missing data. Maximum likelihood estimation was used to estimate all models. Support was found for the hypothesized model from sample 1, which had the best model fit (χ^2 (414) = 689, χ^2 /df = 1.666, p = .000; NFI = .929; CFI = .970; RMSEA = .046, p= .000). The improved model from sample 2 (χ^2 (796) = 1347, χ^2 /df = 1.692, p = .000; NFI = .863; CFI = .939; RMSEA = .058, p= .000) had an excellent model fit.

The structural equation model of Privacy Practices, Brand Protection, Privacy Concerns, Experienced Harms, and Brand Value in the Expanded Privacy-Brand Model from sample 1 is illustrated in Figure 7.4. The Expanded Privacy-Brand Model from sample 2 is presented in Figure 7.10.

The hypotheses are confirmed statistically significant (*** $p \leq .001$) for H1. Privacy Practices ↔ Brand Protection, H2. Privacy Practices ↔ Brand Value, H3. Brand Protection ↔ Brand Value, and H6. Experienced Harms ↔ Brand Value. The hypotheses are confirmed statistically significant (* $p \leq .05$) for H4. Privacy Practices ↔ Experienced Harms and H9. Brand Value ↔ Privacy Concerns. For a summary of the significant findings of the hypotheses from samples 1 and 2 see Table 7.17.

Discussion

Two data samples were collected (N = 315 and N = 205) using the *Privacy Management Survey*. Data from the hold-out sample was analyzed in this chapter (N = 205).

New scales were developed for privacy practices, brand protection, experienced harms, brand value and privacy concerns and compared using data from sample 1 and sample 2. A new Privacy-Brand Model and an Expanded Privacy-Brand Model were developed as well as a Mediated Structural Equation Model for my Privacy-Brand Model for sample 1. A new Expanded Privacy-Brand Model was developed as well as a Structural Equation Model for my Privacy-Brand Model for sample 2.

When I created a model using each different sample the Hypotheses were tested using data from sample 2 and confirmed the statistical significance found in sample 1. H1, H2, H3, H6 were all statistically significance (*** $p \leq .001$). H4 and H9 were statistically significance (* $p \leq .05$). H5, H7, and H8 were not statistically significant in both samples (see Table 7.16).

H1. There is a statistically significant relationship (*** $p \leq .001$) between Privacy practices and Brand protection for both samples.

H2. There is a statistically significant relationship (*** $p \leq .001$) between Privacy practices and Brand value for both samples.

H3. There is a statistically significant relationship (*** $p \leq .001$) between Brand protection and Brand value for both samples.

H4. There is a statistically significant relationship (* $p \leq .05$) between Privacy practices and Experienced harms for both samples.

H5. There is not a significant relationship between Brand protection and Experienced harms for both samples.

H6. There is a statistically significant relationship (*** $p \leq .001$) between Experienced harms and Brand value for both samples.

H7. There is not a significant relationship between Privacy practices and Privacy concerns for both samples.

H8. There is not a significant relationship between Brand protection and Privacy concerns for both samples.

H9. There is a statistically significant relationship (* $p \leq .05$) between Privacy concerns and Brand value for both samples.

Table 7.17

P values Compared for Sample 1 Model and Sample 2 Model

				P sample 1	P sample 2
H1	Privacy_Practices	<-->	Brand_Protection	***	***
H2	Privacy_Practices	<-->	Brand_Value	***	***
H3	Brand_Protection	<-->	Brand_Value	***	***
H4	Privacy_Practices	<-->	Experienced_Harms	.018*	.019*
H5	Experienced_Harms	<-->	Brand_Protection	.707ns	.667ns
H6	Experienced_Harms	<-->	Brand_Value	***	***
H7	Privacy_Practices	<-->	Privacy_Concerns	.713ns	.722ns
H8	Brand_Protection	<-->	Privacy_Concerns	.834ns	.678ns
H9	Brand_Value	<-->	Privacy_Concerns	.016*	.023*

Note: P < 0.05 *, P < 0.01 **, P < 0.001 ***

When I used the model made from sample 1 that had a better fit and tested the Hypotheses using sample 2 data the Hypotheses confirmed the statistical significance found in sample 1 for H1 and H6 were statistically significance (*** $p \leq .001$), H2, H3 and H9 were statistically significance (** $p \leq .01$), H4 was statistically significance (* $p \leq .05$). H5, H7, and H8 were not statistically significant (see Table 7.17).

H1. There is a statistically significant relationship (*** $p \leq .001$) between Privacy practices and Brand protection for both samples. When Privacy practices goes up by 1, Brand protection goes up by .727.

H2. There is a statistically significant relationship (** $p \leq .01$) between Privacy practices and Brand value. When Privacy practices goes up by 1, Brand value goes up by .314.

H3. There is a statistically significant relationship (** $p \leq .01$) between Brand protection and Brand value. When Brand protection goes up by 1, Brand value goes up by .158.

H4. There is a statistically significant relationship (* $p \leq .05$) between Privacy practices and Experienced harms for both samples. When Privacy practices goes up by 1, Experienced harms goes down by .338.

H5. There is not a significant relationship between Brand protection and Experienced harms.

H6. There is a statistically significant relationship (*** $p \leq .001$) between Experienced harms and Brand value for both samples. When Experienced harms goes up by 1, Brand value goes down by .190.

H7. There is not a significant relationship between Privacy practices and Privacy concerns.

H8. There is not a significant relationship between Brand protection and Privacy concerns for both samples.

H9. There is a statistically significant relationship (** $p \leq .01$) between Privacy concerns and Brand value. When Privacy concerns goes up by 1, Brand value goes up by .143.

Table 7.18

P values Compared for Samples 1 and 2 and Sample 2 using Model Made from Sample 1

				P sample 1	*P* sample 2	*P* sample 2 using sample 1 model
H1	Privacy_Practices	<-->	Brand_Protection	***	***	***
H2	Privacy_Practices	<-->	Brand_Value	***	.002**	.001**
H3	Brand_Protection	<-->	Brand_Value	***	.009**	.009**
H4	Privacy_Practices	<-->	Experienced_Harms	.003**	.012*	.029*
H5	Experienced_Harms	<-->	Brand_Protection	.015*	ns	ns
H6	Experienced_Harms	<-->	Brand_Value	.007**	***	***
H7	Privacy_Practices	<-->	Privacy_Concerns	***	ns	ns
H8	Brand_Protection	<-->	Privacy_Concerns	ns	ns	ns
H9	Brand_Value	<-->	Privacy_Concerns	.020*	.020*	.006**

Note: P < 0.05 *, P < 0.01 **, P < 0.001 ***

CHAPTER 8 – SUMMARY AND CONCLUSIONS

Contributions and Public Significance: The Importance and Implications of the Study

The protection of data privacy is a major issue requiring C-suite attention for many reasons. New ubiquitous digital technologies, mobile and Internet of Thing devices, and global e-business mean that the privacy challenges to societies are more complex and larger than ever. At the same time, the unauthorized hacking of systems is on the rise as we saw in the 2016 U.S. Elections. Identity theft is also on the rise, causing hundreds of billions of U.S. dollars in costs as detailed in Chapter 2. In a broader sense, our standing by and allowing the disintegration of privacy is a challenge to the principles of democracy, and good governance.

Only one incident involving a breach of customer privacy could damage an organization's brand. Organizations can use my new model and seek to further defend their brand by putting new protections for security and privacy in place.

The thesis findings also have implications in terms of new training needs for privacy management practices, and new brand protection defences for digital business. Employees must become aware and trained on privacy programs and work according to their policies, practices and procedures. Clients and customers may be made aware of the practices that employees are following so that they trust the organization enough to

provide their personal information. Practically, such training may enhance an organization's ability to safeguard information.

My thesis' showing that proper management of personal information can help an organization protect its brand value is a significant advance in the management literature. The thesis impresses the importance of privacy management on organizations by showing that there are important empirical and scientifically validated linkages among privacy management, brand protection via mechanisms to protect online security and privacy, and the organizations' brand value. The models produced in this thesis are contributions to the management, management of information systems (MIS), and marketing literatures.

This thesis also extends the definition of brand protection (see chapter 2), which is yet another contribution to the marketing literature. Indeed, the extension of brand protection and the associated privacy-brand models are situated at the interdisciplinary intersection of domain knowledge in marketing and information technology and management. This thesis work is thus highly original and demanding.

I have conducted empirical testing validating the practitioners' literature of the relationship between privacy management and brand value. New scales for six constructs (privacy practices, privacy breach, privacy concerns, experienced harms, brand protection, and brand value) are created and scientifically validated. The privacy-brand model, with significant relationships among privacy practices, privacy concerns, brand

protection, and brand value, is a new and important contribution to the management, marketing, management information systems (MIS), and risk literatures.

Strength and Weaknesses of the Studies

Strengths of my research include strong research design at the intersection of multiple disciplines. A strong research design is one that shows how all the parts of the research work together to answer the central questions of a thesis. I believe I have successfully achieved strong linkages among all my major studies to answer my research questions. I was able to identify important new hypotheses and models, design an instrument that led to obtaining a high-quality data set, and identify and iteratively master appropriate methodology.

Many experts in the field reviewed my survey while in the design stage. I also had many security and privacy conference participants complete the survey and provide feedback. Indeed, many of the participants in the first study are experts in the fields of privacy, information technology and security. Real world data has been collected studying relationships in naturalistic settings. Joinson, Reips, Buchanan & Paine Schofield (2010) recommended that this type of setting to study the same relationships they studied would be valuable for future research. Survey participants have provided ecological validity to this research, which means "the findings of the researchers' inquiries actually bear any resemblance to the lived experience of those whom the researchers are studying" (Yue, 2009, p. 959-960).

Another strength is the rich data set collected from two large sample sizes of 315 and 205 providing external validity or generalizability. *External validity* "is related to the idea of generalizability: the ability to take the findings from one study and apply the same relationships and conclusions to other populations and contexts. Quantitative studies attempt to ensure generalizability through the use of representative sampling" (Yue, 2009, p. 961).

The participants selected to participate in the *Privacy Management Survey* have also provided ecological validity to this research because they had to meet the qualifications of having full time employment and working with personal information (i.e. credit cards, medical information, employee information, customer information).

The data sets are extremely rich and are valuable assets to research in this new interdisciplinary area. Obtaining and analyzing a holdout survey sample strengthened the findings of this thesis.

A weakness of this study may be that the survey data was collected from the United States only. With a rather long, in depth questionnaire, many attempts were made but it was difficult to get a large sample to volunteer to respond so Qualtrics was hired to deploy the survey. Other economies, particularly in Asia, have even more integrated technologies throughout work, social, and home than North Americans. Collecting from European countries too, where privacy concerns are heightened would be enlightening. It would be highly instrumental to collect data from Asia, Europe, South America, Middle

East, and Australasia to compare how culture and geography may impact the privacy-brand model.

Future Research

Besides adding cultural variables to the model, future research may include analyzing other variables, including behaviors, beliefs, privacy classification, and risks gathered on my surveys to see if they affect the privacy-brand model. There are many MANOVA tests that can be run on the combined 520 data surveys that could serve as an interesting area for future research. Mediated, moderated, and multi-group effects of the variables merit future research consideration.

Future dissemination of research also involves creating a practical scorecard, which organizations could use to determine how they are complying with privacy regulations and privacy practices for protecting personal information. Such a scorecard could identify areas to improve, which could help prevent data privacy breaches.

Milberg, Smith & Burke (2000) suggested more interpretive research methods be used that dictate that smaller sample sizes be utilized for future research. In their research this would allow an "in-depth examination of the firms' *actual* policies and practices and a *direct* examination of their senior manager's attitudes" (Milberg et al., 2000, p. 48) rather than *perceptions* of respondents' own environments, which was their approach. A recommendation was also made that both actual and perceived corporate management approaches and attitudes be measured and compared (Milberg et al., 2000). Smith et al.

(2011) stated that "largely missing from the entire research stream are studies associated with *group* level privacy. Future empirical studies - both positivist and interpretive - could profitably be targeted to these under-researched levels of analysis" (p. 1005).

Future work may conduct structural equation modelling (SEM) for large versus small organizations and investigate personal branding and corporate branding. It may examine why some hypotheses were accepted for sample 1 but rejected for sample 2.

Differential results for a group who has experienced breaches versus one that has not are topics for future investigations. Research may be conducted in the future using the model with new data, perhaps with a small sample group to put the privacy-brand model into practice.

Summary and Conclusions

In summary for this dissertation a *Preliminary Privacy Concerns Survey* was created and used for data collection for study 1 (N = 260). A new *Privacy Management Survey* instrument was also created and used to collect data for two samples (N = 315 and N = 205).

New scales were developed and validated for privacy practices, brand protection, experienced harms, and privacy concerns and compared for two data samples.

A new Privacy-Brand Model (see Figure 5.6), and new Expanded Privacy-Brand Model (see Figure 6.17) were developed for studies 2 and 3 respectively. The scientifically

validated privacy-brand model depicted in Figure 7.14 is my contribution at the intersection of the management, MIS, marketing, and risk literatures.

Hypotheses were tested for two data samples (N = 315, N = 205). H1, H2, H3, and H7 have been determined to be statistically significant, $p \leq .001$; H4 and H6 have been determined to be statistically significant, $p \leq .01$; and H5 and H9 have been determined to be statistically significant, $p \leq .05$ in sample 1. H1 and H6, $p \leq .001$; H2, H3 and H9, $p \leq .01$; and H4, $p \leq .05$ have been determined to be statistically significant in sample 2, a holdout sample.

Hypothesis 1. An organization's privacy practices (PP) will be significantly and positively associated with its brand protection (BP). **H1: PP → BP**

Hypothesis 2. An organization's privacy practices (PP) will be significantly and positively associated with its brand value (BV). **H2: PP → BV**

Hypothesis 3. An organization's brand protection (BP) will be significantly and positively associated with its brand value (BV). **H3: BP → BV**

Hypothesis 4. An organizations' privacy practices (PP) will be significantly and negatively associated with experienced harms (EH). **H4: PP → -EH**

Hypothesis 5. An organizations' efforts at brand protection (BP) will be significantly and negatively associated with experienced harms (EH). **H5: BP → -EH**

Hypothesis 6. An organization's experienced harms (EH) will be significantly and negatively associated with brand value (BV). **H6: EH → -BV**

Hypothesis 7. An organization's privacy practices (PP) will be significantly and positively associated with its privacy concerns (PC). **H7: PP → PC**

Hypothesis 8. An organization's brand protection (BP) will be significantly and positively associated with its privacy concerns (PC). **H8: BP → PC**

Hypothesis 9. An organization's privacy concerns (PC) will be significantly and positively associated with its brand value (BV). **H9: PC → BV**

This research provided a *privacy-brand model* for proactive management to protect personal information. Completion of the online survey may have brought awareness to participants to help identify potential privacy problems that may be encountered within their organizations and take appropriate action to address these concerns. The benefit to this approach is to avoid consumer and/or regulatory costs and the negative impact it could have on the brand value of the organization.

Privacy should matter to business beyond the law because "within an organization, privacy is essential to establishing and maintaining trust. If customers, clients or employees believe that their personal information will be handled respectfully, in an open and transparent manner, with strong, reasonable safeguards, and made accessible to them at their request, this fosters trust and a continued positive relationship can be expected" (Office of the Information and Privacy Commissioner of Alberta, n.d.).

The implications of this study include that the privacy management deployed in privacy practices and added to brand protections, which are defined, grouped, and studied in this research, can help organizations to protect their brand value. If organizations use brand protection practices, this may assist organizations from reputational and/or

financial damage to their brand value. If organizations are aware of the privacy concerns of their potential customers, they may be able to address these issues and retain or increase their number of clients or customers.

The implications from this research are that organizations may understand the relationships between privacy practices, brand protection, and brand value better with my model, and that this new understanding may lead to better management practices and brand protection measures as firms seek to protect their brand value. The wonderful side effect is that people's personal information and privacy may become better protected. The harms that organizations may experience without this understanding include: database information changed, destroyed or stolen maliciously; digital brand abuse; brand abused on social media sites; defacement of an organization's website; identity theft; intellectual property abuse; abuse of its domain name; web traffic diversions; online trademark infringements; use of its brand in phishing attacks; hacking; and abuse of the organization's brand by distributing fraudulent emails to clients. These data breaches may cause the organization to experience a loss of time or productivity. Data breaches may result in financial losses because of litigation costs; damaged brand value; loss of customer trust which results in a loss of customers and revenue.

By implementing privacy management through privacy practices and in brand protection measures in organizations, it could provide competitive advantage in terms of building and maintaining brand value. Both academics and practitioners should find the

results of the study to be of interest. Empirical data was collected which tell the story of the current privacy practices and brand protection in place; the type and percent of privacy breaches occurring; the harms experienced by organizations; and the brand value of the organization. Empirical testing of the hypotheses has confirmed that privacy management plays a significant role in brand protection and brand value.

REFERENCES

Acquisti, A. (2013, June). Why privacy matters. [Video file]. Retrieved January 2, 2014 from http://www.ted.com/ talks/alessandro_ acquisti_why_privacy_matters.html

Acquisti, A., Friedman, A. & Telang, R. (2006). Is there a cost to privacy breaches? An event study. The Fifth Workshop on the Economics of Information Security (WEIS 2006). Robinson College, University of Cambridge, England. 26-28 June 2006.

Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. Proceedings of the National Academy of Sciences of the United States of America *106*(27), 10975-10980. Retrieved from http://www.pnas.org/content/106/27/10975.full.pdf

American Marketing Association Dictionary. (2016). Brand. Retrieved October 16, 2016 from https://www.ama.org/resources/Pages/Dictionary.aspx?dLetter=B

Andrade, E. B., Kaltcheva, V. & Weitz, B. (2002). Self-disclosure on the Web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research. 29,* 350-353.

Arellano, N. E. (2012, May). Data encryption seldom used by Canadian businesses. ITBusiness.ca. Retrieved May 21, 2012 from http://www.itbusiness.ca/it/client/en/home/news.asp?id=67458

Associate Press. (2014). Target CEO resigns over privacy breach. *Marketing*. Retrieved August 12, 2014 from

http://www.marketingmag.ca/brands/target-ceo-resigns-over-privacy-breach-109817

Axiology. (2001). Clear Direction Inc. Retrieved March 26, 2016 from http://www.cleardirection.com/docs/axiology.asp

Ball, K., & Wilson, D.C. (2000). Power, control and computer-based performance monitoring: repertoires, resistance and subjectivities. *Organization Studies*, *21*(3), 539-565.

Barnes, S., & Mattsson, J. (2008). Brand value in virtual worlds: An axiological approach. *Journal of Electronic Commerce Research, 9*(3), 195-206.

Bell Media Website Privacy Policy. (2011). *Bell.* Retrieved November 3, 2011 from http://www.bellmedia.ca/about/Media_Privacy.page

Bentler, P. (2007). On tests and indices for evaluating structural models. *Personality and Individual Differences, 42*(5), 825-829.

Bernstein, J. E. (2007). Train employees and officials to be ready for privacy challenges. *Computers in Libraries, 27*(6), 6-56. Retrieved from http://www.infotoday.com/cilmag/jun07/Bernstein.shtml

Berry, L. L., & Seltman, K. D. (2007). Building a strong services brand: Lessons from Mayo Clinic, *Business Horizons*, *50*(3), 199-209. Retrieved from https://clasedemarketing.files.wordpress.com/2012/01/mayo-clinic.pdf

Blue Coat Systems Inc. (2016). Cyberthreat defense report. Retrieved October 1, 2016 from http://dc.bluecoat.com/Cyberthreat_Defense_Report_Download?src=GoogleAdwords_ BC_CyberEdgeReport_Feb16&gclid=CIepivGius8CFQgHaQodLFAFPA

Boisson, A. (2017). Chapter 5 - Tools for data analysis, Implementing ICT projects: Guiding decisions to boost positive outcomes. *DBA Defence*. Arthur Lok Jack Graduate School of Business. Faculty of Social Sciences, University of the West Indies, St. Augustine Campus.

Bradmore, D. (2004). Monash Marketing Dictionary. Retrieved May 23, 2012 from http://dictionary. babylon.com/brand_protection/

Braga, M. (2017). Here's why reports of data breaches will skyrocket this year. *CBC News*. Retrieved February 18, 2017 from http://www.cbc.ca/news/technology/cyber-attacks-data-breaches-reporting-canada-privacy-law-1.3972862

Brand Finance (2014). Brandirectory. Brand Value - Definition. Retrieved August 13, 2014 from http://brandirectory.com/glossary/definition/brand_value

Brand Protection. (2013). Online brand protection. Retrieved October 4, 2013 from http://www.brandprotect.com/online-brand-protection.html

Buchanan, T., Paine, C., Adam N., Joinson, A.N. & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157.

Campbell, A. J. (January 01, 1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Interactive Marketing, 11*(3), 44-57.

Cambridge Business English Dictionary. (2011). Cambridge University Press. Retrieved May 23, 2012 from http://dictionary.cambridge.org/dictionary/business-english/brand-protection

Canadian Identity Theft Statistics. Retrieved November 1, 2010 from http://www.combat-identity-theft.com/canadian-identity-theft-statistics.html

Canadian Marketing Association. (2006). Privacy models that work: A guide for Canadian organizations. Retrieved February 25, 2008 from http://www.the-cma.org/PublicUploads/223589privacymodelsthatwork.pdf

Canadian Tire Centre. (2017). Retrieved February 14, 2017 from http://www.canadiantirecentre.com/privacy-policy/

Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society, 3*(2), 247-251.

Cavoukian, A. (2011). Privacy by Design. The 7 foundational principles. Implementation and mapping of fair information practices. Retrieved September 30, 2013 from https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf

Cavoukian, A., & Hamilton, T. J. (2002a). *The Privacy Payoff: How Successful Businesses Build Customer Trust.* Canada: McGraw-Hill Ryerson Limited.

Cavoukian, A., & Hamilton, T. J. (2002b). *The Privacy Payoff: How Building Privacy Into Your Communications Will Give You A Sustainable Competitive Advantage*. McGraw-Hill Ryerson.

Cline, J. (2010). Privacy training gone awry. Computerworld, *44*(3), 24. Retrieved April 20, 2010 from Academic Search Premier Database.

Cocheo, S. (2000). Making privacy a brand issue at bank one. *American Bankers Association.ABA Banking Journal*, *92*(7), 20-22+. Retrieved January 14, 2016 from http://search.proquest.com /docview/218505996?accountid=13908

Coefficient of Determination (2016, October 21). Retrieved October 30, 2016 from https://en.wikipedia.org/wiki/Coefficient_of_determination

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

Delepine, S. (2011). Taking brand protection to a whole new level. *Adhesives & Sealants Industry*, *18*(5), 39-40.

Department of Justice Canada. (2011-12-01). Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). Retrieved Jan. 8, 2012 from http://laws-lois.justice.gc.ca/ eng/acts/P-8.6/page-2.html

Dillon, T. W., Hamilton, A. J., Thomas, D. S., & Usry, M.L. (2008). The importance of communicating workplace privacy policies. *Employee Responsibility and Rights Journal*, 20, 119–139.

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

Eisenhauer, M.P. (2009). The privacy case book: A global survey of privacy and security enforcement actions with recommendations for reducing risks, Chapter 4: Information Security. Retrieved October 30, 2010 from http://www.privacystudio.com/Links posted to web/Casebook Ch 4.pdf

Federal Trade Commission. (2008). *Fair Information Practice Principles*. Retrieved May 20, 2008 from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics*, Fourth Edition. SAGE Publications Ltd.

Field, A. P. (2005). Factor analysis using SPSS. *Discovering statistics using SPSS : (And Sex, Drugs and Rock 'N' Roll).* (2nd Ed.). (ISM introducing statistical methods; ISM (London, England)). London: Sage Publications.

Fienberg, S.E. (2006). Privacy and confidentiality in an e-commerce world: Data mining, data warehousing, matching and disclosure limitation. *Statistical Science 21*(2). A Special Issue on Statistical Challenges and Opportunities in Electronic Commerce

Research (May 2006), 143-154, Institute of Mathematical Statistics. Retrieved from http://www.jstor.org/ stable/27645745

Firouzan, P., & Mckinnon, J. (2004). HIPAA privacy implementation issues in Pennsylvania healthcare facilities. *Perspectives in Health Information Management, 1*, 3.

Freeman, G. (2011). Eye on privacy: Will Facebook's privacy missteps tarnish your brand? *Target Marketing, 34*(7), 8. Retrieved January 14, 2016 from http://search.proquest.com/docview/874621244?accountid=13908

Gaskin, J. (2011, March 25). Model fit during a confirmatory factor analysis (CFA). in AMOS. Retrieved February 9, 2016 from https://www.youtube.com/watch?v=JkZGWUUjdLg

Gaskin, J. (2012, Jan. 27). From measurement model to structural model in AMOS. Retrieved October 29, 2016 from https://www.youtube.com/watch?v=n-ULF6BGVw0

Gaskin, J. (2013a, May 2). SEM series part 3: Exploratory Factor Analysis. Retrieved October 29, 2016 from https://www.youtube.com/watch?v=X-O-OcJPCe8

Gaskin, J. (2013b, Jul 18). SEM BootCamp 2013 Day 4: Moderation and mediation. Retrieved October 5, 2016 from https://www.youtube.com/watch?v=KjByKqdU3aY

Gaskin, J. (2016a, April 23). SEM Series (2016). 8. Mediation. Retrieved October 29, 2016 from https://www.youtube.com/watch?v=ICnh3s2FG14

Gaskin, J. (2016b, August 1). Welcome to Gaskination's StatWiki! Retrieved October 30, 2016 from http://statwiki.kolobkreations.com/index.php?title=Main_Page

Glossary of Canada Council Terms. (February 2005). Retrieved November 9, 2010 from http://www.canadacouncil.ca/help/lj127228791697343750.hhtm

Government of New Brunswick. (2013). Questions and answers for custodians about the Personal Health Information Privacy and Access Act (PHIPAA). Retrieved December 30, 2013 from http://www.gnb.ca /0051/acts/ legislation-e.asp#q2

Gruenwald, J. (November 29, 2011). Facebook settles with FTC over privacy. NationalJournal. Retrieved May 23, 2012 from http://www.nationaljournal.com /tech/facebook-settles-with-ftc-over-privacy-20111129

Hann, I.-H., Hui, K.-L., Lee, S.-Y., & Png, I. (October 01, 2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*, 2, 13-42.

Harris, P. (2008). Right to privacy spurs training, *T+D*, *62*(3), 10-11.

Heffes, E. (2005). Privacy Issuue: Getting noticed. *Financial Executive, 21*(2), 30-32.

Herold, R. (2005). *Managing an Information Security and Privacy Awareness and Training Program*. Florida: Auerbach Publications.

Herold, R. (2007, Jan. 18). Cutter Consortium Identifies Ten Privacy Pitfalls Every Organization Should Avoid Cutter Consortium - January 18, 2007. Retrieved May 20, 2008 from http://security.tekrati.com/ research/8369/

Hermalin, B. E., & Katz, M. L. (2005). Privacy, property rights & efficiency: The economics of privacy as secrecy. Retrieved August 25, 2011 from http://faculty.haas.berkeley.edu /katz/privacy,%20property%20rights %20& %20efficiency%20posted.pdf

Hess, A. (2017, May 9). How privacy became a commodity for the rich and powerful. The New York Times Magazine.

High Tech Crime Investigation Association Atlantic Canada Chapter. (2011). Ninth Annual HTCIA Professional Development Day Privacy and Security Concerns for Modern Organizations, Fredericton Convention Center - October 25, 2011.

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management, 21*(5), 967-988.

Hinkin, T. R., Tracey, J. B., & Enz, C. A. (1997). Scale construction: Developing reliable and valid measurement instruments. *Journal of Hospitality & Tourism Research*, *21*(1), 100-120. doi:10.1177/109634809702100108

Hodson, S., & Playle, S. (2003). Editorial: New developments in the law and what these mean for your brand protection strategy. *Journal of Brand Management, 11*(2), 93-95. Retrieved March 11, 2012 from ABI/INFORM Global. (Document ID: 517462211).

Hoffman, W. M., Hartman, L. P., & Rowe, M. (2003). You've got mail . . . and the boss knows: A survey by the Center for Business Ethics of Companies' Email and Internet Monitoring, *Business and Society Review*, *108*(3), 285-307.

Hutchison, A., Johnston, L., & Breckon, J. (2010). Using QSR-NVivo to facilitate the development of a grounded theory project: An account of a worked example. *International Journal of Social Research Methodology*, *13*(4), 283-302. DOI: 10.1080/13645570902996301.

Iacobucci, D. (2010). Structural equations modeling: Fit indices, sample size, and advanced topics. *Journal of Consumer Psychology*, *20*(1), 90-98.

Interbrand's Brand Valuation Methodology (2013). Retrieved November 1, 2015 from http://www.bestglobalbrands.com

Iverson, R., & Zatzick, C. (2007). High-commitment work practices and downsizing harshness in Australian workplaces. *Industrial Relations, 46*(3), 456-480.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *Int. J. Human-Computer Studies 63,* 203-227.

Jevons, C., Gabbott, M., & de Chernatony, L. (2005), Customer and brand manager perspectives on brand relationships: A conceptual framework, *Journal of Product & Brand Management*, *14*(5), 300- 309. http://dx.doi.org/10.1108/10610420510616331

Joinson, A. N., Reips, U.-D., Buchanan T., & Paine Schofield, C. B. (2010, Jan-Mar). Privacy, trust, and self-disclosure online, *Human-Computer Interaction*, *25*(1), 1-24.

Johnston, L. (2006). Software and method: Reflections on teaching and using QSR NVivo in doctoral research. *International Journal of Social Research Methodology, 9*(5), 379-391.

Jones, R. (2008). Finding sources of brand value: Developing a stakeholder model of brand equity. *International Retail and Marketing Review*. *11*(4), 371-379.

Jutla, D. (2010). Layering privacy on operating systems, social networks, and other platforms by design. *IDIS, 3*, 319–341, DOI 10.1007/s12394-010-0057-8.

Kamakura, W.A., & Russell G.J. (1993). Measuring brand value with scanner data. *Intern. J. of Research in Marketing IO*. 9-22.

Kelly, C. (2005). Compliance focus leads to experiment in cheap films. *Computerworld, 39*(39), 42.

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (Fourth ed., Methodology in the social sciences). New York: The Guilford Press.

Kumaraguru, P., Rhee, Y., Acquisti, A. Cranor, L. F., Hong, J., & Nunge, E. (2006). Protecting people from phishing: The design and evaluation of an embedded training email system. In *CHI 2007: Conference on Human Factors in Computing Systems*, San Jose, California, 28 April-May 3, 2007:905-914. [Originally published as CyLab Technical Report CMU-CyLab-06-017, 2006].

Lawer, C., & Knox, S. (2006), Customer advocacy and brand development, *Journal of Product & Brand Management, 15*(2), 121-129. Retrieved September 23, 2014 from http://dx.doi.org/10.1108/ 10610420610658956

Leading Surveillance Societies in the EU and the World 2007. (2007, December 28). Retrieved November 7, 2010 from http://www.privacyinternational.org/article.shtml?cmd[347]= x-347-559597# method

LimeSurvey Project Team / Carsten Schmitz (2012). / LimeSurvey: An Open Source survey tool /LimeSurvey Project Hamburg, Germany. URL http://www.limesurvey.org

Liu, C, Marchewk, J.T., Lu, J., & Yu, C.-S. (2005). Beyond Concern - A Privacy-Trust-Behavioral Intention Model of Electronic Commerce, *Information & Management*, *42*, 289–304.

Lockton, V., & Rosenberg, R.S. (2006). Office of the Privacy Commissioner of Canada Contributions Program: A preliminary exploration of workplace privacy issues in Canada. Retrieved January 4, 2012 from http://www.cs.ubc.ca/~lockton/workplace.pdf

Lombarte, A. R. (2009). 31st International Conference of Data Protection and Privacy! Retrieved 2009 from http://www.privacyconference2009.org/home/index-iden-idweb.html

Lugaresi, N. (2010). Electronic privacy in the workplace: Transparency and responsibility. *International Review of Law, Computers & Technology, 24*(2), 163-173. doi:10.1080/13600861003748276

Maddox, M. (2015). Data breaches and brand management: How to preserve your brand value. *ClickZ. Marketing News & Expert Advice*. Retrieved November 1, 2015 from http://www.clickz.com/clickz/column/2399488/data-breaches-and-brand-management-how-to-preserve-your-brand-value#

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research. 15*(4), 336-355.

McLeod, E. A. (2004). *E-Business Security and Privacy Practices*. MBA Thesis, Saint Mary's University, Halifax, Nova Scotia, Canada.

McLeod, E. A. (2006). Privacy policy iconography: Symbols and labels to help protect your online safety. Paper presented at the *Seventh World Congress on the Management of E-Business*, Halifax, N.S., July 13-15.

McLeod, E. A., & McLeod, R. (2011). User expectations of privacy of network traffic: Privacy issues and concerns in the information society. Atlantic Schools of Business Conference in Charlottetown, PEI. Published in the *ASB 2011 proceedings*.

Memorial University Information Access and Privacy Protection Office. (2011). The Privacy Rules! Privacy Tools! Training Manual.

Menn, J. (2011, March 30). Google in vow on users' privacy. *FT.com*, London.

Meyers, L., Gamst, G., & Guarino, A. J. (2006 and 2017). *Applied Multivariate Research: Design and Interpretation*. Thousand Oaks: Sage Publications.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57. Retrieved November 8, 2010, from ABI/INFORM Global. (Document ID: 57458013).

Milberg, S. J, Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Association for Computing Machinery. Communications of the ACM, 38*(12), 65. Retrieved November 8, 2010, from ABI/INFORM Global. (Document ID: 8680400).

Mills, A. J. (2015). Reflections on the socio-politics of qualitative research. *Qualitative Research in Organizations and Management, 10*(4), 325-328. Retrieved February 14, 2017 from https://login.library.smu.ca/login?qurl=?url=http://search.proquest.com.library.smu.ca:2048/docview/1732762864?accountid=13908

Milne, G., Rohm, A., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs, 38*(2), 217-232.

Murray, B. H. (2004). *Defending the brand: Aggressive strategies for protecting your brand in the online arena*. New York: American Management Association. Chapter 7: The Costs of Compromised Privacy and Security.

Narayanan, A., & Shmatikov, V. (2010, June). 2010. Myths and fallacies of personally identifiable information. *Communications of the ACM*, 53(6), 24-26. DOI=10.1145/1743546.1743558. Retrieved October 1, 2013 from http://doi.acm.org/10.1145/1743546.1743558

New York Times. (2016, September 23). How to protect yourself after the Yahoo attack. Retrieved October 2, 2016 from http://www.nytimes.com/interactive/2016/technology/personaltech/what-to-do-if-hacked.html?_r=0

Nirupama, D. S., Chei, S. L., & Dion Hoe-Lian Goh. (2012). Tweeting the friendly skies. *Program*, *46*(1), 21-42. doi:http://dx.doi.org/10.1108/00330331211204548

Nymity. (2012, June 13). An update on taking steps to protect our members - Vicente Silveira, LinkedIn. Retrieved June 18, 2012 from http://www.nymity.com/Free_Privacy_Resources/Previews/ReferencePreview.aspx?guid=8cb0a208-13f8-4adb-a770-474607c3f345

Oehlert, P., (2014, September). Reputation and brand protection. Risk Managers' Forum. Rough Notes. Retrieved from http://browndigital.bpc.com/article/Risk_Managers%E2%80%99_Forum/1798956/222976/article.html

Office of the Information and Privacy Commissioner of Alberta. Office of the Privacy Commissioner of Canada. Office of the Information & Privacy Commissioner for British Columbia. (n.d.). Getting accountability right with a privacy management program. Retrieved August 4, 2014 from

http://www.priv.gc.ca/information/guide/ 2012/gl_acc_ 201204_e.pdf

Office of the Privacy Commissioner of Canada. (2007). Privacy breach checklist. Retrieved January 6, 2012 from http://www.priv.gc.ca/information/guide/2007/gl_070801_ checklist_e.pdf

Office of the Privacy Commissioner of Canada. (2008a). Privacy and your business, Privacy Breach Handbook. Retrieved January 2, 2014 from https://www.priv.gc.ca/media/2006/pb_hb_e.pdf

Office of the Privacy Commissioner of Canada. (2008b). Privacy breaches. Retrieved January 2, 2014 from https://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_e.asp

Office of the Privacy Commissioner of Canada. (2009). Legal information related to PIPEDA. Retrieved May 20, 2011 from http://www.priv.gc.ca/leg_c/p_ principle_e.cfm

Office of the Privacy Commissioner of Canada. (2012, January 4). Privacy Commissioners sign new MOU on private sector privacy. Ottawa. Retrieved January 5, 2012 from http://www.priv.gc.ca/media/nr-c/2012/an_120104_e.cfm#content top

Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner of Alberta. (2007, September 25). Report of an investigation into the security, collection and retention of personal information, TJX Companies Inc. /Winners Merchant International L.P. Retrieved May 21, 2008 from http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp

Ores, P. (2001). Whom do you trust? Collaboration, privacy, and brand management. Design Management Journal (Former Series), *12*(2), 36-42.

Pachner, J. (2008, Apr. 9). Canadian firms putting a lock on data privacy. The Globe and Mail, Toronto, Ont.: pg. B.8. Retrieved April 10, 2008 from http://www.Theglobeandmail.com/archives/article678773.ece

Palm, E. (2009). Privacy expectations at work -What is reasonable and why? *Ethical Theory and Moral Practice, 12*:201–215.

Perlroth, N. (2016, September 22). Yahoo says hackers stole data on 500 million users in 2014. The New York Times. Retrieved October 1, 2016 from http://www.nytimes.com/ 2016/09/23/technology/yahoo-hackers.html?_r=0

Personal Health Information Act. (2010). Bill No. 89, Chapter 41 of The Acts of 2010. Reporting of a Privacy Breach. Retrieved January 29, 2015 from http://nslegislature.ca/ legc/bills/61st2nd/3rd_read/b089.htm

Personal Information Protection and Electronic Documents Act. (S.C. 2000, c. 5). Retrieved Nov. 6, 2015 from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-2.html

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review, 2*: 175–196. doi: 10.1111/j.1756-2589.2010.00052.x

Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality grasping the complexities through communication privacy management theory. Published in:

Afifi, T. A., & Afifi, W. A. (Eds.). (2009). Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications (pp. 365-383). NY: Routledge.

PIPEDA compliance improving slowly. (2007). *Information Management Journal. 41*, 14.

PIPEDA.INFO, Personal Information Protection and Electronic Documents Act statutory provisions and some relevant abstracts of decision summaries. Retrieved March 11, 2012 from http://www.pipeda.info/a/s4-1.html

PIPEDA Report of Findings #2010-005. (2011, Dec.). Laurier optical improperly discloses client's personal information. Retrieved January 5, 2012 from http://www.priv.gc.ca/cf-dc/2010/2010_005_0331_e.cfm

Ponemon Institute. (2011). Best practices in data protection survey of U.S. IT & IT security practitioners. Retrieved from https://paylablog.files.wordpress.com/2013/05/rp-ponemon-data-protection-full.pdf

Ponemon Institute. (2012, Jan. 25). Ponemon study shows the cost of a data breach continues to increase. PRNewswire. Retrieved March 11, 2012 from https://www.ponemon.org/news-2/23

Ponemon Institute, (2014a, May). 2014 Cost of data breach study: Global analysis. Retrieved July 28, 2014 from https://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_ Cost_of_Data_Breach_Study.pdf

Ponemon Institute, (2014b, May). 2014 Cost of data breach study: United States. Retrieved June 18, 2014 from https://www.ponemon.org/blog/2014-cost-of-data-breach-united-states

Ponemon Institute, (2015, May). 2015 Cost of data breach study: Global analysis. Retrieved from https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

Ponemon Institute, (2016). 2016 Cost of data breach study: Global study. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Ponemon Institute. (2017, June). 2017 Cost of data breach study: Global overview. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Price Waterhouse Coopers. (1997). Price Waterhouse Privacy Survey 1997. Privacy Law and Policy Reporter 22, 4(2). Retrieved from http://www.austlii.edu.au/au/journals/PrivLawPRpr/1997/28.html

Privacy Breaches: Tools and Resources. (2012, March). Privacy breach checklist. Retrieved May 23, 2012. New link retrieved August 11, 2016 from https://www.oipc.bc.ca/media/15062/oipc_privacy_breach_checklist.pdf

Privacy Legislation in Canada Fact Sheets. (2014). Office of the Privacy Commissioner of Canada. Retrieved July 21, 2016 from https://www.priv.gc.ca/resource/fs-fi/02_05_d_ 15_e.asp

PwC US. (2012, Dec. 21). Protecting your brand from risk. [Video file]. Retrieved April 21, 2016 from https://youtu.be/CXA41eRRHFw

Ragan, S. (2016, March 8). Rosen hotels & resorts discloses data breach. Retrieved March 13, 2016 from http://www.csoonline.com/article/3041986/security/rosen-hotels-and-resorts-discloses-data-breach.html

Reifman, A. (2007, January 12). Dr. Alan Reifman's SEM Course. HDFS 6365, Quantitative Methods IV Texas Tech University. Retrieved October 5, 2016 from http://reifman-sem. blogspot.ca/2007/01/today-well-go-over-left-side-of-sem.html

Rosen Hotels and Resorts Inc., (2016, March 4). Protecting our guests. Rosen Hotels & Resorts Inc. completes investigation of payment card incident. Retrieved March 11, 2016 from http://www.rosenhotels.com/protectingourguests/

Ruparelia, N., White, L., & Hughes, K. (2010). Drivers of brand trust in internet retailing, *Journal of Product & Brand Management*, *19*(4), 250 - 260.

Sabo, J., Willett, M., Brown, P. F., Jutla, D. N., Janssen, G., Magnuson, G., McNabb, J., & Shapiro, S. (2012, March 18). Privacy management reference model and methodology (PMRM). Version 1.0, Working Draft 04. OASIS Open 2012.

Samson, M. (2008). Bill No. 234. Privacy Review Officer Act. Chapter 42 of the Acts of 2008. Retrieved May 21, 2012 from http://nslegislature.ca/legc/bills/ 60th_2nd/3rd_read/ b234.htm

Schick, S. (2007, June 1). Many Canadian firms still not compliant with privacy laws, report shows. Retrieved February 21, 2008 from http://www.itworldcanada.com/a/daily-news/c7640bb6-cbda-4c60-8ff3-fa95133d8baf.html

Seounmi, Y. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs 43(3), 389-418. doi:10.1111/j.1745-6606.2009.01146.x

Shergill, G. S. (2006). Internet banking-An empirical investigation of a trust and loyalty model for New Zealand banks. *Journal of Internet Commerce.* 1533-2861.*4*(4), 101-118.

Sheridan, N. (2010). Writing a methodology chapter.m4v. Retrieved April 17, 2016 from https://www.youtube.com/watch?v=zQFSNB-0sfQ

Smit, E., Bronner, F., & Tolboom, M. (2007). Brand relationship quality and its value for personal contact. *Journal of Business Research*, *60*(6), 627-633. doi:10.1016/j.jbusres. 2006.06.012.

Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-A27.

Smith, H. J., Milberg, S. J., & Burke. S. J, (1996). Information privacy: Measuring individual's concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Smith, T., Koohang, A., & Behling, R. (2010). Understanding and prioritizing technology management challenges. *Journal of Computer Information Systems. 51*(1), 91-98.

Spamlaws.com (2009). What is identity theft and how can it affect me? Retrieved November 1, 2010 from http://www.spamlaws.com/what-is-id-theft.html

St. Davčik, N. (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.

Stoddart, J., & Denham, E. (2008). Leading by example: Key developments in the first seven years of the personal information protection and electronic documents act (PIPEDA). Retrieved October 30, 2010 from http://www.priv. gc.ca/information/pub/lbe_080523_e.cfm#conclusion

Suhr, D. D. (n.d.). Paper 203-30, Principal component analysis vs. exploratory factor analysis. SUGI 30. Statistics and data analysis. Retrieved April 29, 2016 from http://www2.sas.com/proceedings/sugi30/203-30.pdf

Symantec. (2011). Symantec finds enterprises that are not preserving social networking business content risk increased litigation costs and company reputation. Retrieved October 4, 2013 from http://www.symantec.com/about/news/release/article.jsp?prid= 20110721_01&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011July_worldwide_socialmediaflashpoll

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics* (6th ed.). Boston, MA: Pearson/Allyn and Bacon.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*. *2*, 53-55. doi: 10.5116/ijme.4dfb.8dfd PMCID: PMC 4205511.

Techterms.com. (2012). Flaming. Retrieved May 31, 2012 from http://www.techterms.com/definition/Flaming

Techterms.com. (2012). Netiquette. Retrieved May 31, 2012 from http://www. techterms.com/ definition/Netiquette

TED. (2013). Speakers Alessandro Acquisti: Privacy economist. Retrieved January 2, 2014 from http://www.ted.com/speakers/alessandro_acquisti.html

Teufel III, H. (2008, December 29). Department of homeland security privacy policy guidance memorandum number: 2008-01. Retrieved October 16, 2016 from https:// www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf

Tharenou, P., Saks, A. M., & Moore, C. (2007). A review and critique of research on training and organizational-level outcomes. *Human Resource Management Review, 17*, 251–273.

The Canadian Press. (Feb. 14, 2012). Retrieved June 18, 2012 from http://www.ctv.ca/ CTVNews/Health/20120214/nova-scotia-health-board-privacy-breach-120214/#ixzz1yACppmAS

Thornton, M. (2001). Building a security, privacy 'brand'. *Computerworld*, *35*(30), 24. Retrieved January 14, 2016 from

http://search.proquest.com/docview/216077685?accountid=13908

UCDHSC Center for Nursing Research. (2006). Structural equation modeling with AMOS 5.0. Retrieved April 11, 2016 from http://www.ucdenver.edu/academics/colleges/nursing/Documents/PDF/HowToUseAMOS5.pdf

USA.gov (n.d.). Retrieved October 2, 2016 from https://www.usa.gov/identity-theft

van Lieshout, M., Kool, L., van Schoonhoven, B., & de Jonge, M. (2011). Privacy by design: An alternative to existing practice in safeguarding privacy. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 13*(6), 55-68. doi:http://dx.doi.org/0.1108/ 14636691111174261

Vijayan, J. (2007). TJX data breach: At 45.6M card numbers, it's the biggest ever. ComputerWorld. Retrieved April 21, 2016 from http://www.computerworld.com/ article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html

Wallace, E., & De Chernatony, L. (2009). Service employee performance: Its components and antecedents. *Journal of Relationship Marketing, 8*(2), 82-102.

Wang, Y., & Kobsa, A. (2007). Respecting users' individual privacy constraints. User modeling 2007 lecture notes in computer science, *4511*, 157-166.

Wang, P., & Petrison, L.A. (1993). Direct marketing activities and personal privacy: A consumer survey, *Journal of Direct Marketing, 7*(1), 7-19, doi:10.1002/dir.4000070104

Way, S. (2002). High performance work systems and intermediate indicators of firm performance within the US small business sector. *Journal of Management, 28*(6), 765-785.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 1-37.

Wright, T. A., Quick, J. C., Hannah, S. T., & Hargrove, M. B. (2017). Best practice recommendations for scale construction in organizational research: The development and initial validation of the Character Strength Inventory (CSI). *Journal of Organizational Behavior*, DOI: http://dx.doi.org/10.1002/job.2180

Xu, H., Smith H.J., Dinev, T., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view, Proceedings of the 2008 International Conference on Information Systems (ICIS).

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

Yue, A.R. (2009). "Validity" in Mills, A.J., Durepos, G., & Wiebe, E. (Eds). The Sage Encyclopedia of Case Studies. Thousand Oaks, CA: Sage Publications. p. 959-960.

Zalud, B. (2010). Privacy 3.0: Leave me alone goes away. *Security, 47*(12), 58. Retrieved September 28, 2013 from

http://search.proquest.com/docview/ 846781947?accountid=13908

APPENDICES

Appendix A: Privacy Management Survey Information Letter

Privacy Management Survey Information Letter

REB File # 09-218

INTRODUCTION

This survey is being conducted by Elizabeth McLeod, Ph.D. Candidate affiliated with the Department of Management at Saint Mary's University in Halifax, Nova Scotia, Canada as part of her Doctoral Dissertation. This research is being supervised by Dr. Dawn Jutla, Saint Mary's University. If you have any questions contact: Elizabeth McLeod at elizabeth.mcleod@smu.ca or (902) 420-5182 or Dr. Dawn Jutla at dawn.jutla@gmail.com or (902) 491-6441.

PURPOSE OF THIS RESEARCH

The purpose of this research is to explore the state-of- the-art in privacy programs across sectors. It investigates privacy programs for use in brand protection and their impact on an organization's brand value.

WHO IS ELIGIBLE TO TAKE PART? (OR WHO IS BEING INVITED TO PARTICIPATE)

I would like to invite you to take part in my study if you are or were employed and are at least 18 years old.

WHAT DOES PARTICIPATING MEAN? (OR WHAT WILL I HAVE TO DO)

Participation in the study is voluntary and entails completing an **anonymous** survey. This survey is expected to take fifteen minutes or less to complete. Demographic information will be collected for aggregate descriptive analysis.

WHAT ARE THE POTENTIAL BENEFITS AND RISKS OF THIS RESEARCH?

The potential benefits to participants include becoming aware of the highest level of general development of tactical and regulatory aspects of privacy management. Some organizations may become more aware around privacy accountability to stakeholders and responsibility for protecting their clients, customers and/or employees' personal information. Analysis of survey results are intended to test a simple privacy-brand model which could effectively guide management and other stakeholders in creating a business case and appropriate policies and procedures as part of their future privacy management program. Potential indirect benefits to the participant's community may include fewer data breaches and cost savings in the future. Potential benefits to the scientific/scholarly community and/or society are new contributions to management literature in the form of peer-reviewed articles and conference presentations. There are no potential risks that may emerge from this study.

HOW CAN I WITHDRAW FROM THIS STUDY?

Participants can withdraw from this study at any time by not completing or submitting the survey. Since participation is anonymous it is not possible to withdraw after data has been submitted.

WHAT WILL BE DONE WITH MY INFORMATION? WHO WILL HAVE ACCESS TO IT?

Information will be collected and reported in aggregate form. Access to the raw data will be restricted to the researchers. Results will be published in Elizabeth McLeod's publically available dissertation.

CERTIFICATION

This research has been reviewed and approved by the Saint Mary's University Research Ethics Board. If you have any questions or concerns about ethical matters, you may contact the Chair of the Saint Mary's University Research Ethics Board at ethics@smu.ca or 420-5728.

Click the Start Survey button to volunteer to participate in the study. Thank you for participating!

Appendix B: Network Traffic Privacy Survey

Note. Survey was renamed *Preliminary Privacy Concerns Survey* for clarity within the body of the thesis.

NETWORK TRAFFIC PRIVACY SURVEY

Instructions: Please check the appropriate box in each row for each location.	**Question: With respect to your network traffic, what is your Expectation of Privacy in the following locations?** *(Note: Your expectation is what you believe to be true, not what you wish were true.)*		
Location	**Do not expect any privacy.**	**Expect privacy of data sent and received (packet payload) but no privacy for the address information of the two computers that are communicating (packet header).**	**Very private, no one should be looking at any part of the communication (not even your employer).**
Home			
Work			
Public Hotspot			

What concerns do you have about network traffic privacy? *(Use the back if you require more space.)*_____

<u>Demographic Information</u> *Please circle appropriate answers:*

Gender: ♀ Female ♂ Male

Born Before: *(circle the earliest applicable date*

1950 1970 1990

1960 1980 2000

Education:

No College or University

Some College or University

Undergraduate Degree(s)

Graduate Degree(s)

Country of origin: _____ **Country of residence:** _____

Profession/Occupation: _____

If you have any questions related to the survey contact: Elizabeth McLeod at elizabeth.mcleod@smu.ca (902) 420-5182 or Ron McLeod at rmcleod13215@gmail.com (902) 456-9520 or Faculty Advisor Dr. Dawn Jutla at dawn.jutla@smu.ca (902) 420-5157.

This research has been reviewed and approved by the Saint Mary's University Research Ethics Board. If you have any questions or concerns about ethical matters, you may contact Dr. Jim Cameron, Chair of the Saint Mary's University Research Ethics Board at ethics@smu.ca or 420-5728.

Please submit completed survey in envelope at Registration Desk. *By submitting this anonymous survey, you agree to voluntarily participate in this study. Thank you.*

Appendix C: Privacy Management Survey

Elizabeth McLeod
Saint Mary's University
923 Robie Street
Halifax, Nova Scotia, Canada
B3H 3C3

Privacy Management Survey

Hello my name is Elizabeth McLeod. I am conducting a survey for my Ph.D. research at Saint Mary's University in Halifax, Nova Scotia, Canada to explore the state-of-the-art in privacy programs across sectors. It investigates privacy programs for use in brand protection and their impact on an organization's brand value. If you have any questions contact: Elizabeth McLeod at elizabeth.mcleod@smu.ca or (902) 420-5182 or Faculty supervisor, Dr. Dawn Jutla, at dawn.jutla@gmail.com or (902) 491-6441.

I would like to invite you to take part in my study if you are or were employed and are at least 18 years old. Participation is voluntary and entails completing an anonymous survey by selecting the best answer on the seven-point scales anchored with strongly disagree to strongly agree or don't know regarding questions about policies and procedures for the protection of personal information and brand protection; fair information practices (FIPs); privacy and security programs and privacy breaches. Refer to your department to answer the questions or to your organization as a whole if there is no difference between departments. Demographic information will be collected for aggregate descriptive analysis. It should only take about 30-45 minutes of your time to answer the survey. You can withdraw from the study by not submitting your survey. Your answers will remain anonymous. Since participation is anonymous, it is not possible to withdraw after data has been submitted. Please complete and submit the survey within one week.

The potential benefits to participants include becoming aware of the highest level of general development of tactical and regulatory aspects of privacy management. Some organizations may become more aware of privacy accountability to stakeholders and responsibility for protecting their clients, customers and/or employees' personal information. Analysis of survey results is intended to test a simple privacy-brand model, which could effectively guide management and other stakeholders in creating a business case and appropriate policies and procedures as part of their future privacy management

program. Potential indirect benefits to the participant's community may include fewer data breaches and cost savings in the future. Potential benefits to the scientific/scholarly community and/or society are new contributions to management literature in the form of peer-reviewed articles and conference presentations. Survey results will be available in Elizabeth McLeod's publicly available dissertation. There are no potential risks that may emerge from this study.

Information will be collected and reported in aggregate form. Access to the raw data will be restricted to the researchers. Electronic data will be collected using Saint Mary's University approved LimeSurvey and Qualtrics software. LimeSurvey and Qualtrics are "Secure and web-based - Input data from anywhere in the world with secure web authentication and Secure Sockets Layer (SSL) encryption." Data will be stored on a secure server at Qualtrics, Saint Mary's University and on a secure encrypted portable drive.

This research has been reviewed and approved by the Saint Mary's University Research Ethics Board. If you have any questions or concerns about ethical matters, you may contact the Chair of the Saint Mary's University Research Ethics Board at ethics@smu.ca or (902) 420-5728 and refer to REB File # 14-340.

Please select the best answer on the seven-point scales anchored with "strongly disagree" and "strongly agree."

To complete the survey online follow this link:
https://survey.qualtrics.com/SE/?SID=SV_5c1NN6nLRJvC6e9

Thank you for participating!

"Personal information" means "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Personal information that the organization "collects, uses or discloses in the course of commercial activities" or "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business" (Office of The Privacy Commissioner of Canada, 2013). "Organization" in this survey refers to private sector entities, public bodies (government departments, agencies, boards and commissions, municipal bodies) and health custodians.

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

1	My organization is responsible for personal information under its control.	1	2	3	4	5	6	7
2	My organization has designated an individual or individuals who are accountable for the organization's compliance with the Privacy principles (Fair information principles).	1	2	3	4	5	6	7
3	My organization identifies the purposes for which personal information is collected at or before the time the information is collected.	1	2	3	4	5	6	7
4	My organization requires the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except when required by law.	1	2	3	4	5	6	7
5	My organization limits the collection of personal information to that which is necessary for the purposes identified by the organization.	1	2	3	4	5	6	7
6	My organization collects information by fair and lawful means.	1	2	3	4	5	6	7
7	My organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.	1	2	3	4	5	6	7
8	My organization retains personal information only as long as necessary for the fulfillment of the purposes, which it was collected, except with the consent of the individual or as required by law.	1	2	3	4	5	6	7
9	My organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

10	My organization protects personal information by security safeguards appropriate to the sensitivity of the information.	1	2	3	4	5	6	7
11	My organization makes specific information about its policies and practices relating to the management of personal information readily available to individuals.	1	2	3	4	5	6	7
12	My organization informs an individual of the existence, use, and disclosure of his or her personal information.	1	2	3	4	5	6	7
13	My organization gives an individual access to his or her personal information upon request.	1	2	3	4	5	6	7
14	An individual is able to challenge the accuracy and completeness of the information and have it amended as appropriate in my organization.	1	2	3	4	5	6	7
15	My organization allows an individual to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization's compliance.	1	2	3	4	5	6	7
16	My organization requires all employees who access personal information to take privacy training.	1	2	3	4	5	6	7
17	My organization provides mandatory training on personal privacy protection at least every two years.	1	2	3	4	5	6	7
18	My organization trains employees about the federal *Privacy Act (PA).*	1	2	3	4	5	6	7
19	My organization trains employees about the *Health Insurance Portability and Accountability Act (HIPAA).*	1	2	3	4	5	6	7
20	My organization's privacy training covers the policies and practices established by the organization.	1	2	3	4	5	6	7
21	My organization educates clients to help manage the risk of client loss resulting from corporate identity theft.	1	2	3	4	5	6	7
22	My organization extends training on personal privacy protection to partners.	1	2	3	4	5	6	7
23	My organization extends privacy training to all stakeholders (i.e. employees, clients).	1	2	3	4	5	6	7
24	Contracts with 3rd party service providers include protection of personal information.	1	2	3	4	5	6	7
25	My organization provides communication to stakeholders and users regarding data privacy awareness.	1	2	3	4	5	6	7
26	My organization has a privacy policy.	1	2	3	4	5	6	7
27	My organization has a policy in place so employees know what to do if there is a data breach.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

28	Management provides alignment of privacy policies with privacy practices.	1	2	3	4	5	6	7
29	My organization has best practices use for privacy.	1	2	3	4	5	6	7
30	My organization has a privacy program.	1	2	3	4	5	6	7
31	My organization uses privacy management models.	1	2	3	4	5	6	7
32	My organization has a privacy program to prevent credit card fraud.	1	2	3	4	5	6	7
33	My organization has a privacy program to prevent digital brand abuse.	1	2	3	4	5	6	7
34	My organization uses privacy methodologies.	1	2	3	4	5	6	7
35	My organization conducts privacy impact assessments (PIAs).	1	2	3	4	5	6	7
36	My organization conducts privacy audits.	1	2	3	4	5	6	7
37	My organization stores personal information on mobile devices such as laptops, tablets and jump drives *with* encryption.	1	2	3	4	5	6	7
38	My organization stores personal information on mobile devices such as laptops, tablets and jump drives *without* encryption.	1	2	3	4	5	6	7
39	My organization uses encryption when storing data.	1	2	3	4	5	6	7
40	My organization conducts e-business.	1	2	3	4	5	6	7
41	My organization uses Secure Socket Layer (SSL) to encrypt sensitive information that is transmitted over the Internet during e-commerce transactions.	1	2	3	4	5	6	7
42	My organization uses software to detect intruders.	1	2	3	4	5	6	7
43	My organization stores personal information in the cloud.	1	2	3	4	5	6	7
44	My organization stores personal information in other countries.	1	2	3	4	5	6	7
45	My organization has the security necessary to ensure the ongoing protection of personal information.	1	2	3	4	5	6	7
46	My organization has policies in place to protect personal information.	1	2	3	4	5	6	7
47	My organization ensures that policies to protect personal information are put into practice each and every day.	1	2	3	4	5	6	7
48	My organization periodically examines portable storage devices to ensure they are being used solely for legitimate reasons.	1	2	3	4	5	6	7
49	My organization reviews holdings, disposes of transitory records and classifies remaining records at the appropriate security level.	1	2	3	4	5	6	7
	A **privacy breach** occurs when information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification *(N.S. Personal Health Information Act - PHIA).*							

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

50	My organization has experienced a data privacy breach.	1	2	3	4	5	6	7
51	My organization had a data breach because of malicious or criminal attacks.	1	2	3	4	5	6	7
52	My organization had a data breach because of employee negligence.	1	2	3	4	5	6	7
53	My organization had a data breach because of system glitches.	1	2	3	4	5	6	7
54	My organization has a formal incident response plan in place to address data breaches.	1	2	3	4	5	6	7
55	My organization has appointed an individual to lead the data breach incident response team.	1	2	3	4	5	6	7
56	My organization does not report instances of a data privacy breach to authorities.	1	2	3	4	5	6	7
57	My organization has reported instances of a data privacy breach to authorities.	1	2	3	4	5	6	7
58	My organization had customers terminate their relationship with the company because of a data breach.	1	2	3	4	5	6	7
59	A data privacy breach has caused my organization's brand to lose value.	1	2	3	4	5	6	7
60	My organization has had clients' credit card information compromised.	1	2	3	4	5	6	7
61	My organization has had clients' debit card information compromised.	1	2	3	4	5	6	7
62	Clients of my organization have faced the inconvenience of cancelling cards.	1	2	3	4	5	6	7
63	My organization requires staff and/or clients to regularly change their passwords.	1	2	3	4	5	6	7
64	Clients of my organization have expressed inconvenience related to changing passwords as a result of a data privacy breach.	1	2	3	4	5	6	7
65	My organization has had unauthorized attempts to access personal information.	1	2	3	4	5	6	7
66	My organization has had a mobile device (i.e. laptop) lost or stolen that contained unencrypted personal information.	1	2	3	4	5	6	7
67	My organization has had a mobile device (i.e. laptop) lost or stolen that contained encrypted personal information.	1	2	3	4	5	6	7
68	My organization restricts the use of portable storage devices.	1	2	3	4	5	6	7
69	My organization uses system software, which blocks unauthorized use of portable storage devices on desktop computers.	1	2	3	4	5	6	7
70	My organization's database of personal information has been changed maliciously.	1	2	3	4	5	6	7
71	Personal information held by my organization has been maliciously destroyed.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

72	My organization has experienced digital brand abuse.	1	2	3	4	5	6	7
73	My organization has had its brand abused on social media sites.	1	2	3	4	5	6	7
74	My organization has experienced defacement of its site's website.	1	2	3	4	5	6	7
75	My organization has experienced identity theft.	1	2	3	4	5	6	7
76	My organization has experienced intellectual property abuse.	1	2	3	4	5	6	7
77	My organization has experienced abuse of its domain name.	1	2	3	4	5	6	7
78	My organization has experienced web traffic diversions.	1	2	3	4	5	6	7
79	My organization has experienced online trademark infringements.	1	2	3	4	5	6	7
80	My organization has experienced the use of its brand in phishing attacks.	1	2	3	4	5	6	7
81	My organization is a service-oriented business that depends on information (e.g. airline schedules or stock quotes).	1	2	3	4	5	6	7
82	My organization has experienced instances of hacking.	1	2	3	4	5	6	7
83	A data breach has caused my organization to experience a loss of time.	1	2	3	4	5	6	7
84	A data breach has caused my organization to experience a loss of productivity.	1	2	3	4	5	6	7
85	My organization has experienced litigation costs because of a data breach.	1	2	3	4	5	6	7
86	My organization has experienced direct financial costs because of a data breach.	1	2	3	4	5	6	7
87	My organization has experienced damaged brand value because of a data breach.	1	2	3	4	5	6	7
88	My organization has experienced loss of customer trust because of a data breach.	1	2	3	4	5	6	7
89	A data breach has caused my organization to affect public safety.	1	2	3	4	5	6	7
90	My organization has experienced lost revenue because of a data breach.	1	2	3	4	5	6	7
91	A data breach has caused my organization to experience a loss of intellectual property.	1	2	3	4	5	6	7
92	Spammers have abused my organization's brand by distributing fraudulent emails to clients.	1	2	3	4	5	6	7
93	A breach of client privacy may have a severe impact on an organization's financial position.	1	2	3	4	5	6	7
94	A breach of client privacy may result in a decreased market valuation.	1	2	3	4	5	6	7
95	A breach of client privacy may result in lost brand value.	1	2	3	4	5	6	7
96	A breach of client privacy may result in costs for litigation.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

97	Protecting privacy and security may lead to a competitive advantage for my organization.	1	2	3	4	5	6	7
98	I am sensitive to online information privacy concerns.	1	2	3	4	5	6	7
99	I am willing to provide my personal information in exchange for money.	1	2	3	4	5	6	7
100	I am willing to provide my personal information in exchange for convenience.	1	2	3	4	5	6	7
101	I feel there are gaps between privacy practices and privacy training in my organization.	1	2	3	4	5	6	7
102	I feel that privacy policies and privacy practices in my organization are not aligned.	1	2	3	4	5	6	7
103	I believe that privacy training helps to protect my organization's brand.	1	2	3	4	5	6	7
104	I believe that a privacy breach would damage my organization's brand.	1	2	3	4	5	6	7
105	I believe that privacy breaches may result in substantial loss of consumer confidence.	1	2	3	4	5	6	7
106	I believe that privacy breaches may result in loss of value of my organization's brand.	1	2	3	4	5	6	7
107	I read license agreements fully before I agree to them.	1	2	3	4	5	6	7
108	I read a website's privacy policy before I register my information.	1	2	3	4	5	6	7
109	I am engaged in social networking over the Internet.	1	2	3	4	5	6	7
110	I use the privacy settings in social networking over the Internet.	1	2	3	4	5	6	7
111	I am aware that Employment and Social Development Canada has a hard drive missing that contained the Social Insurance number, name, date of birth, home address, telephone number, loan amounts and balances for more than half a million student loan recipients from 2000 to 2006.	1	2	3	4	5	6	7
112	I am aware of the privacy breach in 2007 at the parent company of TJ Maxx that affected 90 million records.	1	2	3	4	5	6	7
113	I am aware that my organization experienced hackers' theft of information on many customers.	1	2	3	4	5	6	7
114	I believe that we need a system that requires people to be notified when their personal data has been breached.	1	2	3	4	5	6	7
115	I am generally distrustful of organizations that ask for my personal information.	1	2	3	4	5	6	7
116	I worry about the accuracy of computerized information about me.	1	2	3	4	5	6	7
117	I worry about additional uses made of computerized information about me.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

118	I am in favor of new laws and regulatory actions to protect privacy rights and provide enforceable remedies.	1	2	3	4	5	6	7
119	I am generally trustful of organizations collecting my personal information.	1	2	3	4	5	6	7
120	I am comfortable with my organization's existing privacy practices.	1	2	3	4	5	6	7
121	I am not in favor of the enactment of new privacy laws or regulations.	1	2	3	4	5	6	7
122	I weigh the benefits of various consumer opportunities and services before providing my personal information.	1	2	3	4	5	6	7
123	I look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved.	1	2	3	4	5	6	7
124	I believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it.	1	2	3	4	5	6	7
125	Where consumer matters are involved, I want the opportunity to decide whether to opt out of even non-evaluative uses of my personal information as in compilations of mailing lists.	1	2	3	4	5	6	7
126	What concerns do you have about the privacy of your personal information?							
127	What concerns do you have about network traffic privacy?							
128	If I have concerns for online privacy, I use protection behaviors such as falsifying information.	1	2	3	4	5	6	7
129	If I have concerns for online privacy, I use protection behaviors such as refusing information disclosure or transactions.	1	2	3	4	5	6	7
130	If I have concerns for online privacy, I use protection behaviors such as removing personal information from lists.	1	2	3	4	5	6	7
131	If I do not have concerns for online privacy, I use my personal information.	1	2	3	4	5	6	7
132	If I have concerns for online privacy, I adopt privacy-enhancing technologies.	1	2	3	4	5	6	7
133	If I have concerns for online privacy, I refrain from interacting with a Web site.	1	2	3	4	5	6	7
134	I engage in m-commerce (mobile commerce).	1	2	3	4	5	6	7
135	I have concerns for mobile privacy.	1	2	3	4	5	6	7
136	I am concerned about the increase number of mobile devices.	1	2	3	4	5	6	7
137	I have personally been the victim of what I felt was an improper invasion of privacy of my personal information.	1	2	3	4	5	6	7
138	My organization has been the victim of an improper invasion of privacy of personal information.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

139	I am concerned that my personal information is accessed without permission.	1	2	3	4	5	6	7
140	I am concerned that my personal information is used without permission.	1	2	3	4	5	6	7
141	I am concerned about online banking.	1	2	3	4	5	6	7
142	I am concerned about online credit card transactions.	1	2	3	4	5	6	7
143	I am concerned about online shopping.	1	2	3	4	5	6	7
144	I am concerned about information seen or intercepted by a third party.	1	2	3	4	5	6	7
145	I am concerned that someone may hijack my system and perform illegal activities where my system is the only traceable element.	1	2	3	4	5	6	7
146	I am concerned about identity theft.	1	2	3	4	5	6	7
147	I am concerned that privacy online is an illusion; it does not exist.	1	2	3	4	5	6	7
148	I am concerned about the lack of privacy control online.	1	2	3	4	5	6	7
149	I am concerned about the privacy of my email messages.	1	2	3	4	5	6	7
150	I am concerned about the privacy of my photographs online.	1	2	3	4	5	6	7
151	I am concerned about viruses / spyware / malware / EXE files / multimedia files.	1	2	3	4	5	6	7
152	I am concerned about Facebook so I deleted my account.	1	2	3	4	5	6	7
153	If I want my personal information protected, I would not put it online.	1	2	3	4	5	6	7
154	I am concerned about people who have personal data do not care about its security.	1	2	3	4	5	6	7
155	I am concerned that there is no way to tell if personal data being stored is secure.	1	2	3	4	5	6	7
156	I am concerned that personal data obtained is shared with others.	1	2	3	4	5	6	7
157	I am concerned about tracking purchase habits.	1	2	3	4	5	6	7
158	I am concerned about privacy of passwords.	1	2	3	4	5	6	7
159	I am concerned about the privacy of wireless access at home.	1	2	3	4	5	6	7
160	I am concerned about the privacy of wireless access at work.	1	2	3	4	5	6	7
161	I am concerned about the privacy of wireless access at public hot spots.	1	2	3	4	5	6	7
162	I am concerned about protecting client's data.	1	2	3	4	5	6	7
163	I am concerned about export of data to jurisdictions with lax privacy laws.	1	2	3	4	5	6	7
164	I am concerned that personal information is readily available and that risks are not communicated to the public.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

165	I am concerned about the lack of privacy rights.	1	2	3	4	5	6	7
166	I am concerned about location tracking.	1	2	3	4	5	6	7
167	I am concerned about the government having my personal information.	1	2	3	4	5	6	7
168	I am concerned that network traffic is leaking private data.	1	2	3	4	5	6	7
169	I am concerned that online registration is easily compromised.	1	2	3	4	5	6	7
170	I am concerned that someone may hijack my account and ruin my reputation.	1	2	3	4	5	6	7
171	I feel great pride identifying with my organization.	1	2	3	4	5	6	7
172	What my organization delivers feels right for me.	1	2	3	4	5	6	7
173	I feel I am able to trust my organization completely.	1	2	3	4	5	6	7
174	My organization does me good.	1	2	3	4	5	6	7
175	My organization is a satisfying buy.	1	2	3	4	5	6	7
176	What I get from my organization is worth the cost.	1	2	3	4	5	6	7
177	The uniqueness of my organization stands out.	1	2	3	4	5	6	7
178	My organization is a symbol of quality.	1	2	3	4	5	6	7
179	Information about my organization is always correct.	1	2	3	4	5	6	7
180	My organization is a good brand.	1	2	3	4	5	6	7
181	I feel great pride identifying with my government.	1	2	3	4	5	6	7
182	What my government delivers feels right for me.	1	2	3	4	5	6	7
183	I feel I am able to trust my government completely.	1	2	3	4	5	6	7
184	My government does me good.	1	2	3	4	5	6	7
185	My government is a satisfying experience.	1	2	3	4	5	6	7
186	What I get from my government is worth the cost.	1	2	3	4	5	6	7
187	The uniqueness of my government stands out.	1	2	3	4	5	6	7
188	My government is a symbol of quality.	1	2	3	4	5	6	7
189	Information about my government is always correct.	1	2	3	4	5	6	7
190	My government is a good brand.	1	2	3	4	5	6	7
191	I feel great pride identifying with my government.	1	2	3	4	5	6	7
192	What TJX Companies Inc. (Winners and Home Sense) delivers feels right for me.	1	2	3	4	5	6	7
193	I feel I am able to trust TJX Companies Inc. (Winners and Home Sense) completely.	1	2	3	4	5	6	7

1. Strongly Disagree	2. Disagree	3. Moderately Disagree	4. Neither Agree nor Disagree / Neutral	5. Moderately Agree	6. Agree	7. Strongly Agree

194	TJX Companies Inc. (Winners and Home Sense) does me good.	1	2	3	4	5	6	7
195	TJX Companies Inc. (Winners and Home Sense) is a satisfying buy.	1	2	3	4	5	6	7
196	What I get from TJX Companies Inc. (Winners and Home Sense) is worth the cost.	1	2	3	4	5	6	7
197	The uniqueness of TJX Companies Inc. (Winners and Home Sense) stands out.	1	2	3	4	5	6	7
198	TJX Companies Inc. (Winners and Home Sense) is a symbol of quality.	1	2	3	4	5	6	7
199	Information about TJX Companies Inc. (Winners and Home Sense) is always correct.	1	2	3	4	5	6	7
200	TJX Companies Inc. (Winners and Home Sense) is a good brand.	1	2	3	4	5	6	7
201	I feel great pride identifying with Bank of America.	1	2	3	4	5	6	7
202	What Bank of America delivers feels right for me.	1	2	3	4	5	6	7
203	I feel I am able to trust Bank of America completely.	1	2	3	4	5	6	7
204	Bank of America does me good.	1	2	3	4	5	6	7
205	Bank of America is a satisfying buy.	1	2	3	4	5	6	7
206	What I get from Bank of America is worth the cost.	1	2	3	4	5	6	7
207	The uniqueness of Bank of America stands out.	1	2	3	4	5	6	7
208	Bank of America is a symbol of quality.	1	2	3	4	5	6	7
209	Information about Bank of America is always correct.	1	2	3	4	5	6	7
210	Bank of America is a good brand.	1	2	3	4	5	6	7

Appendix D: Privacy Management Survey Demographics

Privacy Management Survey Demographic Information

Elizabeth A. McLeod, Ph.D. Candidate Research

Demographic Information *Please choose appropriate answers:*

Gender:

○ Male ○ Female

Education: What is the highest degree or level of school you have completed?

If currently enrolled, highest degree received.

○ Some high school, no diploma

○ High school graduate, diploma or the equivalent (i.e. GED)

○ Some college or university, no degree

○ Trade/technical/vocational training

○ Associate degree

○ Bachelor's degree

○ Master's degree

○ Professional degree

○ Doctorate degree

○ Other: _____

Age: What is your age?

- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- 65-74 years old
- 75 years or older

What is your country of residence?

- Canada
- United States
- Australia
- China
- Finland
- France
- Germany
- Sweden
- Switzerland
- United Kingdom
- Other

What is your Profession or Occupation?

- ○ Administrative Support
- ○ Arts and Entertainment
- ○ Engineer
- ○ Financial
- ○ Human Resources
- ○ Information Technology
- ○ Law Enforcement
- ○ Legal
- ○ Medical
- ○ Privacy Officer
- ○ Professor / Teacher
- ○ Sales and Marketing
- ○ Science
- ○ Security
- ○ Student
- ○ Transport
- ○ Other: [ ]

What level is your position?

- ○ Senior Management
- ○ Middle Management
- ○ Technical
- ○ Clerical/Labour/Other Support
- ○ Other: [ ]

What size is your organization (number of employees)?

- ○ Very small (1-50 employees)
- ○ Small (51-100)
- ○ Medium (101- 500)
- ○ Large (>500)
- ○ Do not know

Describe your organization.

My organization has an online presence.	○ Yes	○ No
My organization has a mobile presence.	○ Yes	○ No
My organization provides products or services online.	○ Yes	○ No
My organization purchases online.	○ Yes	○ No
My organization provides products or services directly to the general public.	○ Yes	○ No

My organization provides products or services both to the public and to other businesses/organizations. ○ Yes ○ No

My organization provides products or services only to other businesses/organizations. ○ Yes ○ No

My organization provides products or services that do not fall into any of the above categories. ○ Yes ○ No

What information does your organization use?

Credit card information ○ Yes ○ No

Financial information ○ Yes ○ No

Medical information ○ Yes ○ No

Personal information ○ Yes ○ No

Proprietary information ○ Yes ○ No

Other

What sector is your organization?

○ Public

○ Private

○ Not-for-Profit

○ Other: [ ]

What sector is your organization involved with?

- Accommodation and Food Services
- Administrative and Support, Waste Management and Remediation Services
- Agriculture, Forestry, Fishing and Hunting
- Airline
- Arts, Entertainment and Recreation
- Construction
- Educational Services
- Finance and Insurance
- Food and Beverage
- Government
- Health Care and Social Assistance
- Information and Cultural Industries
- Legal
- Management of Companies and Enterprises
- Manufacturing
- Mining, Quarrying, and Oil and Gas Extraction
- Other Services (except Public Administration)
- Professional, Scientific and Technical Services
- Public Administration
- Real Estate and Rental and Leasing

- ○ Retail Trade
- ○ Telecommunications Industry
- ○ Transportation and Warehousing
- ○ Utilities
- ○ Wholesale Trade
- ○ Other: [ ]

If you have any questions related to the survey please contact:
Elizabeth McLeod at elizabeth.mcleod@smu.ca (902) 420-5182 or
Faculty Advisor: Dr. Dawn Jutla at dawn.jutla@gmail.com (902) 491-6441.
Saint Mary's University, 923 Robie Street, Halifax, Nova Scotia, Canada B3H 3C3

This research has been reviewed and approved by the Saint Mary's University Research Ethics Board. If you have any questions or concerns about ethical matters, you may contact the Chair of the Saint Mary's University Research Ethics Board at ethics@smu.ca or (902) 420-5728.

Please submit your completed survey. Thank you!

Appendix E: Privacy Management Survey Results

Headings for Survey

SD: Strongly Disagree

D: Disagree

MD: Moderately Disagree

N: Neither Agree Nor Disagree / Neutral

MA: Moderately Agree

A: Agree

SA: Strongly Agree

Combined Agree: (Summed MD: Moderately Agree + A: Agree + SD: Strongly Agree)

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
1	My organization is responsible for personal information under its control.	3%	1%	1%	6%	11%	23%	55%	89%
2	My organization has designated an individual or individuals who are accountable for the organization's compliance with the Privacy principles (Fair information principles).	2%	1%	3%	13%	10%	28%	42%	80%
3	My organization identifies the purposes for which personal information is collected at or before the time the information is collected.	2%	1%	1%	8%	11%	28%	49%	88%
4	My organization requires the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except when required by law.	2%	2%	1%	9%	10%	24%	51%	85%
5	My organization limits the collection of personal information to that which is necessary for the purposes identified by the organization.	3%	1%	3%	9%	11%	28%	45%	84%
6	My organization collects information by fair and lawful means.	3%	0%	1%	5%	5%	25%	62%	91%
7	My organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.	3%	0%	1%	6%	5%	21%	64%	90%
8	My organization retains personal information only as long as necessary for the fulfillment of the purposes, which it was collected, except with the consent of the individual or as required by law.	3%	1%	2%	7%	8%	25%	54%	88%
9	My organization ensures that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.	2%	1%	2%	4%	11%	29%	51%	91%
10	My organization protects personal information by security safeguards appropriate to the sensitivity of the information.	2%	0%	2%	6%	9%	27%	53%	89%
11	My organization makes specific information about its policies and practices relating to the management of personal information readily available to individuals.	1%	1%	3%	10%	12%	27%	46%	84%
12	My organization informs an individual of the existence, use, and disclosure of his or her personal information.	1%	2%	3%	10%	12%	31%	42%	85%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
13	My organization gives an individual access to his or her personal information upon request.	2%	3%	3%	10%	9%	26%	48%	83%
14	An individual is able to challenge the accuracy and completeness of the information and have it amended as appropriate in my organization.	2%	2%	2%	11%	13%	30%	41%	83%
15	My organization allows an individual to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization's compliance.	3%	1%	2%	14%	13%	29%	39%	81%
16	My organization requires all employees who access personal information to take privacy training.	6%	3%	5%	12%	9%	18%	47%	73%
17	My organization provides mandatory training on personal privacy protection at least every two years.	7%	6%	7%	16%	8%	14%	42%	63%
18	My organization trains employees about the Privacy Act (PA).	7%	5%	5%	16%	9%	16%	42%	67%
19	My organization trains employees about the Health Insurance Portability and Accountability Act (HIPAA).	9%	5%	5%	16%	10%	16%	39%	65%
20	My organization's privacy training covers the policies and practices established by the organization.	3%	2%	2%	13%	11%	19%	49%	79%
21	My organization educates clients to help manage the risk of client loss resulting from corporate identity theft.	6%	7%	4%	22%	14%	19%	27%	60%
22	My organization extends training on personal privacy protection to partners.	7%	10%	5%	23%	10%	17%	27%	54%
23	My organization extends privacy training to all stakeholders (i.e. employees, clients).	9%	7%	7%	25%	10%	17%	25%	52%
24	Contracts with 3rd party service providers include protection of personal information.	7%	3%	6%	22%	11%	19%	32%	62%
25	My organization provides communication to stakeholders and users regarding data privacy awareness.	5%	6%	5%	23%	14%	19%	28%	61%
26	My organization has a privacy policy.	2%	1%	2%	7%	10%	22%	57%	89%
27	My organization has a policy in place so employees know what to do if there is a data breach.	4%	3%	5%	17%	11%	22%	38%	71%
28	Management provides alignment of privacy policies with privacy practices.	3%	2%	2%	17%	13%	23%	39%	76%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
29	My organization has best practices use for privacy.	3%	2%	2%	16%	13%	25%	40%	78%
30	My organization has a privacy program.	3%	3%	3%	16%	14%	21%	41%	76%
31	My organization uses privacy management models.	4%	4%	6%	28%	11%	18%	29%	57%
32	My organization has a privacy program to prevent credit card fraud.	5%	6%	3%	25%	9%	22%	30%	60%
33	My organization has a privacy program to prevent digital brand abuse.	6%	5%	5%	28%	10%	16%	30%	56%
34	My organization uses privacy methodologies.	3%	3%	4%	28%	10%	19%	34%	63%
35	My organization conducts privacy impact assessments (PIAs).	6%	6%	6%	33%	11%	13%	24%	49%
36	My organization conducts privacy audits.	4%	7%	5%	27%	13%	16%	27%	56%
37	My organization stores personal information on mobile devices such as laptops, tablets and jump drives with encryption.	10%	5%	3%	19%	13%	20%	29%	62%
38	My organization stores personal information on mobile devices such as laptops, tablets and jump drives without encryption.	26%	12%	8%	19%	9%	14%	13%	36%
39	My organization uses encryption when storing data.	3%	3%	3%	19%	16%	20%	37%	72%
40	My organization conducts e-business.	6%	5%	5%	17%	16%	21%	30%	66%
41	My organization uses Secure Socket Layer (SSL) to encrypt sensitive information that is transmitted over the Internet during e-commerce transactions.	6%	5%	3%	31%	11%	16%	29%	55%
42	My organization uses software to detect intruders.	4%	2%	3%	22%	14%	23%	32%	70%
43	My organization stores personal information in the cloud.	18%	12%	8%	26%	11%	12%	12%	35%
44	My organization stores personal information in other countries.	31%	17%	6%	19%	7%	9%	10%	26%
45	My organization has the security necessary to ensure the ongoing protection of personal information.	3%	2%	4%	17%	17%	25%	32%	75%
46	My organization has policies in place to protect personal information.	1%	1%	2%	12%	19%	23%	43%	84%
47	My organization ensures that policies to protect personal information are put into practice each and every day.	2%	2%	3%	14%	16%	23%	41%	79%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
48	My organization periodically examines portable storage devices to ensure they are being used solely for legitimate reasons.	7%	5%	5%	29%	12%	14%	29%	55%
49	My organization reviews holdings, disposes of transitory records and classifies remaining records at the appropriate security level.	3%	3%	2%	27%	14%	17%	33%	64%
50	My organization has experienced a data privacy breach.	33%	23%	7%	17%	6%	5%	8%	19%
51	My organization had a data breach because of malicious or criminal attacks.	38%	24%	9%	15%	3%	3%	7%	13%
52	My organization had a data breach because of employee negligence.	38%	24%	7%	17%	5%	4%	5%	14%
53	My organization had a data breach because of system glitches.	37%	23%	6%	20%	5%	3%	5%	13%
54	My organization has a formal incident response plan in place to address data breaches.	14%	10%	5%	22%	14%	13%	22%	48%
55	My organization has appointed an individual to lead the data breach incident response team.	13%	9%	6%	27%	13%	14%	18%	45%
56	My organization does not report instances of a data privacy breach to authorities.	38%	17%	10%	27%	1%	4%	4%	9%
57	My organization has reported instances of a data privacy breach to authorities.	21%	13%	6%	37%	3%	7%	11%	22%
58	My organization had customers terminate their relationship with the company because of a data breach.	44%	15%	6%	22%	4%	3%	5%	12%
59	A data privacy breach has caused my organization's brand to lose value.	45%	19%	8%	18%	3%	3%	3%	9%
60	My organization has had clients' credit card information compromised.	53%	22%	3%	12%	4%	3%	3%	10%
61	My organization has had clients' debit card information compromised.	53%	22%	3%	12%	3%	4%	3%	9%
62	Clients of my organization have faced the inconvenience of cancelling cards.	50%	23%	3%	12%	6%	4%	3%	13%
63	My organization requires staff and/or clients to regularly change their passwords.	13%	8%	3%	12%	10%	17%	38%	64%
64	Clients of my organization have expressed inconvenience related to changing passwords as a result of a data privacy breach.	37%	19%	10%	19%	7%	5%	3%	15%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
65	My organization has had unauthorized attempts to access personal information.	36%	17%	6%	21%	9%	6%	5%	20%
66	My organization has had a mobile device (i.e. laptop) lost or stolen that contained unencrypted personal information.	46%	19%	6%	17%	3%	5%	3%	11%
67	My organization has had a mobile device (i.e. laptop) lost or stolen that contained encrypted personal information.	44%	17%	7%	18%	3%	5%	5%	14%
68	My organization restricts the use of portable storage devices.	18%	10%	7%	22%	13%	11%	19%	42%
69	My organization uses system software, which blocks unauthorized use of portable storage devices on desktop computers.	13%	9%	5%	24%	12%	13%	24%	49%
70	My organization's database of personal information has been changed maliciously.	50%	23%	5%	15%	3%	2%	2%	7%
71	Personal information held by my organization has been maliciously destroyed.	52%	24%	4%	15%	1%	3%	1%	5%
72	My organization has experienced digital brand abuse.	50%	23%	4%	16%	3%	1%	2%	6%
73	My organization has had its brand abused on social media sites.	47%	24%	4%	15%	4%	3%	2%	10%
74	My organization has experienced defacement of its site's website.	52%	24%	4%	14%	3%	1%	2%	6%
75	My organization has experienced identity theft.	51%	22%	5%	13%	5%	2%	3%	9%
76	My organization has experienced intellectual property abuse.	50%	22%	5%	17%	2%	2%	3%	7%
77	My organization has experienced abuse of its domain name.	52%	23%	3%	16%	1%	2%	3%	5%
78	My organization has experienced web traffic diversions.	51%	20%	4%	17%	3%	3%	3%	8%
79	My organization has experienced online trademark infringements.	53%	21%	4%	16%	3%	1%	3%	7%
80	My organization has experienced the use of its brand in phishing attacks.	43%	19%	5%	17%	7%	5%	4%	16%
81	My organization is a service-oriented business that depends on information (e.g. airline schedules or stock quotes).	32%	18%	7%	16%	10%	9%	8%	27%
82	My organization has experienced instances of hacking.	43%	20%	5%	17%	8%	5%	4%	17%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
83	A data breach has caused my organization to experience a loss of time.	48%	20%	5%	15%	4%	4%	4%	12%
84	A data breach has caused my organization to experience a loss of productivity.	48%	20%	4%	14%	6%	4%	4%	14%
85	My organization has experienced litigation costs because of a data breach.	52%	21%	3%	15%	2%	2%	4%	9%
86	My organization has experienced direct financial costs because of a data breach.	50%	19%	4%	16%	5%	3%	3%	11%
87	My organization has experienced damaged brand value because of a data breach.	52%	21%	5%	16%	2%	2%	2%	5%
88	My organization has experienced loss of customer trust because of a data breach.	52%	21%	3%	14%	6%	3%	2%	10%
89	A data breach has caused my organization to affect public safety.	56%	23%	3%	13%	2%	2%	2%	5%
90	My organization has experienced lost revenue because of a data breach.	50%	23%	4%	15%	4%	2%	2%	8%
91	A data breach has caused my organization to experience a loss of intellectual property.	53%	22%	4%	16%	1%	2%	2%	5%
92	Spammers have abused my organization's brand by distributing fraudulent emails to clients.	50%	21%	3%	15%	4%	4%	3%	12%
93	A breach of client privacy may have a severe impact on an organization's financial position.	26%	10%	3%	14%	12%	15%	20%	47%
94	A breach of client privacy may result in a decreased market valuation.	22%	10%	2%	17%	13%	16%	21%	50%
95	A breach of client privacy may result in lost brand value.	20%	9%	3%	15%	13%	17%	24%	54%
96	A breach of client privacy may result in costs for litigation.	17%	8%	2%	13%	16%	18%	26%	60%
97	Protecting privacy and security may lead to a competitive advantage for my organization.	13%	9%	3%	17%	16%	17%	25%	58%
98	I am sensitive to online information privacy concerns.	7%	3%	2%	10%	19%	25%	34%	78%
99	I am willing to provide my personal information in exchange for money.	46%	14%	7%	19%	6%	3%	4%	14%
100	I am willing to provide my personal information in exchange for convenience.	37%	14%	8%	24%	8%	5%	4%	17%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
101	I feel there are gaps between privacy practices and privacy training in my organization.	27%	16%	13%	20%	12%	7%	4%	23%
102	I feel that privacy policies and privacy practices in my organization are not aligned.	32%	17%	13%	18%	11%	5%	3%	19%
103	I believe that privacy training helps to protect my organization's brand.	4%	3%	3%	17%	22%	19%	31%	72%
104	I believe that a privacy breach would damage my organization's brand.	5%	3%	4%	18%	23%	17%	30%	70%
105	I believe that privacy breaches may result in substantial loss of consumer confidence.	5%	3%	4%	13%	23%	21%	31%	75%
106	I believe that privacy breaches may result in loss of value of my organization's brand.	6%	2%	5%	18%	20%	20%	29%	69%
107	I read license agreements fully before I agree to them.	8%	12%	12%	18%	20%	14%	16%	50%
108	I read a website's privacy policy before I register my information.	9%	11%	13%	21%	18%	11%	17%	46%
109	I am engaged in social networking over the Internet.	6%	3%	3%	8%	17%	24%	39%	81%
110	I use the privacy settings in social networking over the Internet.	3%	2%	3%	10%	15%	26%	41%	82%
111	I am aware that Employment and Social Development Canada has a hard drive missing that contained the Social Insurance number, name, date of birth, home address, telephone number, loan amounts and balances for more than half a million student loan recipients from 2000 to 2006.	40%	24%	7%	14%	4%	5%	6%	15%
112	I am aware of the privacy breach in 2007 at the parent company of TJ Maxx that affected 90 million records.	24%	14%	7%	9%	12%	17%	17%	46%
113	I am aware that my organization experienced hackers' theft of information on many customers.	47%	20%	6%	10%	6%	6%	5%	17%
114	I believe that we need a system that requires people to be notified when their personal data has been breached.	2%	2%	2%	8%	11%	25%	50%	86%
115	I am generally distrustful of organizations that ask for my personal information.	3%	5%	12%	27%	23%	15%	16%	54%
116	I worry about the accuracy of computerized information about me.	3%	4%	7%	20%	29%	20%	17%	66%
117	I worry about additional uses made of computerized information about me.	2%	4%	6%	17%	27%	23%	23%	72%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
118	I am in favor of new laws and regulatory actions to protect privacy rights and provide enforceable remedies.	1%	2%	3%	12%	22%	27%	34%	83%
119	I am generally trustful of organizations collecting my personal information.	11%	12%	17%	30%	17%	6%	7%	30%
120	I am comfortable with my organization's existing privacy practices.	1%	3%	4%	19%	19%	29%	26%	73%
121	I am not in favor of the enactment of new privacy laws or regulations.	21%	23%	20%	23%	5%	5%	3%	13%
122	I weigh the benefits of various consumer opportunities and services before providing my personal information.	2%	1%	4%	17%	29%	29%	18%	76%
123	I look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved.	2%	5%	7%	32%	19%	18%	17%	54%
124	I believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it.	1%	1%	2%	14%	22%	25%	35%	82%
125	Where consumer matters are involved, I want the opportunity to decide whether to opt out of even non-evaluative uses of my personal information as in compilations of mailing lists.	0%	2%	1%	12%	18%	29%	38%	85%
	To show your commitment to providing thoughtful answers please select disagree.	0%	100%	0%	0%	0%	0%	0%	0%
	Privacy concerns								
	Network privacy concerns								
128	If I have concerns for online privacy I use protection behaviors such as falsifying information.	8%	18%	13%	17%	18%	15%	10%	43%
129	If I have concerns for online privacy I use protection behaviors such as refusing information disclosure or transactions.	1%	3%	2%	14%	24%	30%	25%	79%
130	If I have concerns for online privacy I use protection behaviors such as removing personal information from lists.	2%	3%	3%	12%	26%	29%	26%	81%
131	If I do not have concerns for online privacy I use my personal information.	6%	7%	7%	13%	22%	29%	15%	66%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
132	If I have concerns for online privacy I adopt privacy-enhancing technologies.	2%	4%	8%	23%	25%	24%	13%	63%
133	If I have concerns for online privacy I refrain from interacting with a Web site.	2%	2%	3%	10%	22%	32%	30%	83%
134	I engage in m-commerce (mobile commerce).	15%	7%	7%	22%	18%	17%	15%	50%
135	I have concerns for mobile privacy.	3%	2%	3%	16%	28%	24%	25%	77%
136	I am concerned about the increase number of mobile devices.	10%	11%	11%	19%	17%	18%	13%	49%
137	I have personally been the victim of what I felt was an improper invasion of privacy of my personal information.	24%	21%	11%	11%	15%	10%	9%	34%
138	My organization has been the victim of an improper invasion of privacy of personal information.	36%	23%	5%	18%	8%	7%	3%	18%
139	I am concerned that my personal information is accessed without permission.	6%	7%	5%	15%	26%	22%	20%	68%
140	I am concerned that my personal information is used without permission.	6%	7%	6%	14%	25%	19%	23%	67%
141	I am concerned about online banking.	8%	11%	11%	17%	25%	13%	15%	53%
142	I am concerned about online credit card transactions.	8%	9%	10%	16%	23%	17%	17%	57%
143	I am concerned about online shopping.	7%	9%	12%	17%	24%	16%	15%	55%
144	I am concerned about information seen or intercepted by a third party.	4%	3%	5%	13%	24%	25%	26%	75%
145	I am concerned that someone may hijack my system and perform illegal activities where my system is the only traceable element.	6%	7%	8%	18%	20%	20%	21%	61%
146	I am concerned about identity theft.	1%	3%	5%	7%	27%	27%	30%	84%
147	I am concerned that privacy online is an illusion; it does not exist.	7%	5%	4%	18%	26%	18%	21%	65%
148	I am concerned about the lack of privacy control online.	3%	3%	6%	11%	31%	22%	24%	77%
149	I am concerned about the privacy of my email messages.	4%	6%	11%	18%	23%	19%	18%	61%
150	I am concerned about the privacy of my photographs online.	4%	6%	11%	16%	20%	20%	23%	64%
151	I am concerned about viruses / spyware / malware / EXE files / multimedia files.	1%	2%	3%	9%	24%	28%	33%	85%
152	I am concerned about Facebook so I deleted my account.	32%	28%	12%	14%	5%	4%	5%	14%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
153	If I want my personal information protected I would not put it online.	4%	6%	10%	23%	23%	19%	15%	57%
154	I am concerned about people who have personal data do not care about its security.	4%	2%	5%	23%	27%	20%	19%	65%
155	I am concerned that there is no way to tell if personal data being stored is secure.	2%	3%	3%	15%	25%	31%	22%	78%
156	I am concerned that personal data obtained is shared with others.	3%	2%	3%	10%	27%	34%	21%	82%
157	I am concerned about tracking purchase habits.	5%	7%	8%	13%	22%	26%	19%	68%
158	I am concerned about privacy of passwords.	4%	4%	6%	11%	22%	29%	25%	75%
159	I am concerned about the privacy of wireless access at home.	6%	5%	11%	16%	20%	25%	17%	62%
160	I am concerned about the privacy of wireless access at work.	9%	11%	13%	17%	16%	19%	16%	50%
161	I am concerned about the privacy of wireless access at public hot spots.	4%	3%	5%	12%	18%	27%	32%	76%
162	I am concerned about protecting client's data.	4%	3%	3%	11%	19%	29%	30%	79%
163	I am concerned about export of data to jurisdictions with lax privacy laws.	4%	4%	5%	22%	21%	24%	20%	65%
164	I am concerned that personal information is readily available and that risks are not communicated to the public.	3%	3%	3%	13%	27%	28%	23%	77%
165	I am concerned about the lack of privacy rights.	3%	3%	5%	18%	21%	24%	26%	70%
166	I am concerned about location tracking.	4%	4%	8%	13%	23%	22%	26%	70%
167	I am concerned about the government having my personal information.	6%	6%	8%	14%	19%	23%	25%	66%
168	I am concerned that network traffic is leaking private data.	4%	5%	5%	19%	24%	26%	17%	67%
169	I am concerned that online registration is easily compromised.	5%	3%	5%	17%	26%	25%	19%	71%
170	I am concerned that someone may hijack my account and ruin my reputation.	5%	4%	10%	17%	21%	23%	20%	64%
171	I feel great pride identifying with my organization.	2%	3%	5%	17%	17%	27%	29%	73%
172	What my organization delivers feels right for me.	1%	2%	2%	18%	21%	27%	29%	77%
173	I feel I am able to trust my organization completely.	2%	3%	5%	17%	18%	27%	28%	73%
174	My organization does me good.	2%	2%	3%	15%	19%	30%	30%	79%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
175	My organization is a satisfying buy.	1%	2%	3%	19%	18%	30%	27%	75%
176	What I get from my organization is worth the cost.	1%	3%	5%	19%	20%	28%	24%	72%
177	The uniqueness of my organization stands out.	1%	3%	4%	21%	20%	27%	24%	70%
178	My organization is a symbol of quality.	1%	3%	3%	15%	21%	27%	29%	77%
179	Information about my organization is always correct.	1%	5%	10%	23%	22%	18%	20%	60%
180	My organization is a good brand.	0%	1%	3%	14%	20%	30%	32%	82%
181	I feel great pride identifying with my government.	10%	8%	16%	26%	17%	13%	10%	40%
182	What my government delivers feels right for me.	14%	11%	17%	28%	14%	10%	6%	30%
183	I feel I am able to trust my government completely.	23%	16%	15%	22%	11%	8%	5%	24%
184	My government does me good.	15%	13%	14%	30%	15%	9%	4%	28%
185	My government is a satisfying experience.	18%	15%	13%	29%	11%	10%	4%	26%
186	What I get from my government is worth the cost.	18%	16%	12%	27%	11%	9%	6%	26%
187	The uniqueness of my government stands out.	12%	12%	9%	25%	21%	13%	8%	42%
188	My government is a symbol of quality.	16%	14%	9%	25%	18%	10%	8%	36%
189	Information about my government is always correct.	26%	20%	17%	20%	5%	8%	4%	17%
190	My government is a good brand.	20%	10%	10%	30%	13%	11%	5%	30%
191	I feel great pride identifying with my government.	19%	11%	15%	24%	14%	10%	6%	30%
192	What TJX Companies Inc. (Winners and Home Sense) delivers feels right for me.	6%	4%	5%	60%	12%	6%	7%	25%
193	I feel I am able to trust TJX Companies Inc. (Winners and Home Sense) completely.	6%	5%	8%	57%	11%	6%	6%	24%
194	TJX Companies Inc. (Winners and Home Sense) does me good.	6%	6%	6%	59%	11%	8%	4%	23%
195	TJX Companies Inc. (Winners and Home Sense) is a satisfying buy.	6%	5%	5%	59%	10%	8%	7%	25%
196	What I get from TJX Companies Inc. (Winners and Home Sense) is worth the cost.	4%	4%	4%	60%	12%	8%	7%	27%
197	The uniqueness of TJX Companies Inc. (Winners and Home Sense) stands out.	4%	4%	5%	59%	13%	8%	6%	27%
198	TJX Companies Inc. (Winners and Home Sense) is a symbol of quality.	4%	5%	6%	60%	12%	6%	7%	25%

#	Survey Statement	SD	D	MD	N	MA	A	SA	Combined Agree
199	Information about TJX Companies Inc. (Winners and Home Sense) is always correct.	4%	6%	8%	63%	9%	6%	5%	19%
200	TJX Companies Inc. (Winners and Home Sense) is a good brand.	4%	4%	4%	59%	13%	8%	7%	29%
201	I feel great pride identifying with Bank of America.	13%	14%	11%	34%	10%	11%	7%	28%
202	What Bank of America delivers feels right for me.	14%	12%	11%	31%	14%	11%	7%	32%
203	I feel I am able to trust Bank of America completely.	14%	13%	11%	30%	14%	10%	8%	32%
204	Bank of America does me good.	13%	13%	10%	34%	9%	14%	7%	30%
205	Bank of America is a satisfying buy.	13%	12%	10%	33%	11%	13%	7%	32%
206	What I get from Bank of America is worth the cost.	13%	10%	9%	38%	12%	12%	6%	31%
207	The uniqueness of Bank of America stands out.	13%	11%	11%	33%	11%	13%	6%	31%
208	Bank of America is a symbol of quality.	13%	11%	7%	32%	17%	12%	8%	38%
209	Information about Bank of America is always correct.	11%	13%	12%	38%	10%	8%	8%	26%
210	Bank of America is a good brand.	12%	9%	8%	28%	17%	18%	9%	44%