Ari Peltoniemi

# PERCEIVED EFFECTIVENESS OF PRIVACY POLICY AND ITS ASSOCIATION WITH TRUST AND BEHAVIORAL INTENTION TO PARTICIPATE IN A DIGITAL WORKPLACE WELLNESS PROGRAM

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2020

# ABSTRACT

Peltoniemi, Ari
Perceived Effectiveness of Privacy Policy and its Association with Trust and Behavioral Intention to Participate in a Digital Workplace Wellness Program
Jyväskylä: University of Jyväskylä, 2020, 54 pp.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

The Perceived Effectiveness of Privacy Policy (PEPP) is a topical issue in information privacy research. In this study we developed a research model applying Theory of Reasoned Action and the Privacy–Trust–Behavioral Intention model to measure PEPP and its relationships with Trust and Behavioral Intention to participate in a digital Workplace Wellness Program (WWP). Increased participation in WWPs introduces the potential of increased profits for employers and increased health outcomes for employees. An online survey instrument was developed and used to collect data from the population of Finnish white-collar telecommuters. The Partial Least Squares Path Modeling (PLS-PM) method was used to analyze the data. The results indicate that there are statistically significant positive relationships between the constructs of Security and PEPP, PEPP and Trust, and Trust and Behavioral Intention to Participate in a digital WWP. We identified also statistically significant indirect effects between Security and Trust, Security and Behavioral Intention as well as PEPP and Behavioral Intention to Participate in a digital WWP. The results indicate that efforts to increase PEPP may be justified to increase Trust and Behavioral Intention to participate in a digital WWP among working professionals.

Keywords: Perceived Effectiveness of Privacy Policy, Trust, Behavioral Intention, Participation, Digital Workplace Wellness Program, Theory of Reasoned Action, Partial Least Squares Path Modeling

# TIIVISTELMÄ

Peltoniemi, Ari
Tietosuojapolitiikan koettu vaikuttavuus ja sen yhteys luottamukseen ja käyttäytymisintentioon osallistua digitaaliseen työhyvinvointiohjelmaan
Jyväskylä: Jyväskylä yliopisto, 2020, 54 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tietosuojapolitiikan koettu vaikuttavuus (TPKV) on ajankohtainen aihe tietosuojatutkimuksessa. Tässä tutkimuksessa kehitettiin tutkimusmalli, jossa sovelletaan perustellun toiminnan teoriaa ja yksityisyys-luottamus-käyttäytymisintentio -mallia TPKV:n sekä sen yhteyksien mittaamiseen luottamukseen ja käyttäytymisintentioon osallistua digitaaliseen työhyvinvointiohjelmaan. Työhyvinvointiohjelmiin osallistumisen edistäminen lisää potentiaalisesti työantajien taloudellista tulosta sekä työntekijöiden terveyttä. Aineistonkeruuvälineeksi kehitettiin verkkokysely, jolla aineisto kerättiin populaatiosta, joka koostuu suomalaisista valkokaulusetätyöntekijöistä. Aineiston analysointimenetelmänä käytettiin osittaisen pienimmän neliösumman polun mallinnusta (PLS-PM). Tulokset osoittavat, että seuraavien konstruktioiden välillä vallitsee tilastollisesti merkittävä positiivinen yhteys: tietoturva ja TPKV, TPKV ja luottamus, sekä luottamus ja käyttäytymisintentio osallistua digitaaliseen työhyvinvointiohjelmaan. Myös seuraavat tilastollisesti merkittävät epäsuorat yhteydet tunnistettiin: tietoturva ja luottamus, tietoturva ja käyttäytymisintentio sekä TPKV ja käyttäytymisintentio osallistua digitaaliseen työhyvinvointiohjelmaan. Tulokset viittaavat siihen, että TPKV:n kehittämiseen tähtäävät toimenpiteet voivat olla perusteltuja luottamuksen sekä käyttäytymisintention osallistua digitaaliseen työhyvinvointiohjelmaan lisäämiseksi työntekijöiden keskuudessa.

Asiasanat: tietosuojapolitiikan koettu vaikuttavuus, luottamus, käyttätymisintentio, osallistuminen, digitaalinen työhyvinvointiohjelma, perustellun toiminnan teoria, osittaisen pienimmän neliösumman polun mallinnus

## ACKNOWLEDGEMENTS

The prevalence and severity of recent data breach events from all over the globe indicate that deep understanding and comprehensive management of information privacy may be more important today than ever. Information privacy has been an overarching theme that has influenced my academic and professional endeavors for years. This is partly due to the implementation of GDPR, which in my opinion has been a positive development in the EU legislation.

In today's data-driven business environment, companies must ensure that personally identifiable information will be protected in all their activities. One of the more concrete implications of GDPR for most companies is the obligation to provide privacy policies for their products and services. In addition to academic goals, this rather fast-paced study was conducted in an entrepreneurial spirit to investigate the possibilities of turning a mere legal obligation into more of an evidence-based value creation opportunity.

I would like to express my gratitude towards my colleagues at Fibion Inc., the study participants, my thesis supervisor, and my family for all their support. This thesis concludes my efforts to obtain yet another master's degree within the broad realm of IT. The future will show what additional quests lie ahead for me in the academia.

Jyväskylä
December 2020
Ari Peltoniemi

## FIGURES

FIGURE 1 Integrated Framework for Online Information Privacy Research (Li, 2012, p. 477) ..... 15
FIGURE 2 Model of Perceived Information Privacy Concepts and Correlates (Dinev et al., 2013, p. 298) ..... 17
FIGURE 3 Model of Linking Individuals' Information Privacy Perceptions to Institutional Assurances (Xu et al., 2011, p. 803) ..... 19
FIGURE 4 Privacy Boundary Management Model (Chang et al., 2018, p. 449) . 22
FIGURE 5 The Privacy–Trust–Behavioral Intention model (Liu et al., 2005, p. 292) ..... 27
FIGURE 6 The Research Model of Wu et al. (2012, p. 895) ..... 27
FIGURE 7 Research Model ..... 28
FIGURE 8 The Estimated Model ..... 43

## TABLES

TABLE 1 Privacy Policy Content Taxonomy (Earp et al., 2005, p. 230) ..... 21
TABLE 2 Variables and Measurement Items ..... 29
TABLE 3 Control Variables and Measurement Items ..... 30
TABLE 4 Characteristics of Respondents (n = 101) ..... 36
TABLE 5 Descriptive Statistics of the Items (n = 101) ..... 37
TABLE 6 Steps to Assess Composite Models (Benitez et al., 2020, p. 10) ..... 38
TABLE 7 Overall Saturated Model Fit Evaluation ..... 39
TABLE 8 Indicator Multicollinearity ..... 39
TABLE 9 Indicator Weights T-Values ..... 40
TABLE 10 Indicator Loadings T-Values ..... 40
TABLE 11 Steps to Assess Structural Models (Benitez et al., 2020, p. 12) ..... 41
TABLE 12 Overall Estimated Model Fit Evaluation ..... 42
TABLE 13 Path Coefficient Estimates (***p < .001) ..... 42
TABLE 14 Effect sizes ($f^2$) ..... 42
TABLE 15 $R^2$ values ..... 43
TABLE 16 Significant Path Coefficient Estimates of Control Variables (*p<.05; **p<.01) ..... 44
TABLE 17 Hypotheses and Conclusions ..... 44

**TABLE OF CONTENTS**

ABSTRACT ..... 2

TIIVISTELMÄ ..... 3

ACKNOWLEDGEMENTS ..... 4

FIGURES ..... 5

TABLES ..... 5

TABLE OF CONTENTS ..... 6

1 INTRODUCTION ..... 8
1.1 Background and Motivation ..... 8
1.2 Research Objective and Hypotheses ..... 10
1.3 Structure of the Thesis ..... 10

2 LITERATURE REVIEW ..... 11
2.1 Overview of Information Privacy Research ..... 11
2.2 Key Theories of Information Privacy ..... 12
2.3 An Integrated Framework for Online Information Privacy Research 15
2.4 Perceived Information Privacy ..... 16
2.4.1 Communication Privacy Management Theory ..... 16
2.4.2 Concepts and Correlates of Perceived Information Privacy ..... 17
2.4.3 Linking Perceived Information Privacy to Information Privacy Policy ..... 18
2.5 Information Privacy Policy ..... 20
2.6 Perceived Effectiveness of Privacy Policy ..... 22
2.7 Privacy Issues in Workplace Wellness Programs ..... 23
2.8 Summary ..... 25

3 RESEARCH METHODOLOGY ..... 26
3.1 Research Model Development ..... 26
3.2 Scale Development and Survey Instrument ..... 28
3.3 Data Collection and Research Setting ..... 31
3.3.1 Digital Workplace Wellness Program Under Study ..... 31
3.4 Selection of Data Analysis Method ..... 32
3.5 Summary ..... 34

4 DATA ANALYSIS AND RESULTS ..... 35
4.1 Preparing the Data for Analysis ..... 35

4.2 Data Analysis ..... 37
4.2.1 Assessment of the Composite Model ..... 37
4.2.2 Assessment of the Structural Model ..... 41
4.3 Testing of the Hypotheses ..... 44
4.4 Summary ..... 44

5 DISCUSSION AND CONCLUSIONS ..... 46
5.1 Discussion ..... 46
5.2 Conclusions ..... 47
5.3 Implications of the Study ..... 48
5.4 Limitations ..... 49
5.5 Future Research ..... 50

REFERENCES ..... 51

# 1 INTRODUCTION

In this chapter the background and motivation for the thesis are first discussed. Second, the research questions and objectives for the study are defined. Finally, we describe the structure of the thesis.

## 1.1 Background and Motivation

Over the last decades, an epidemic of "lifestyle diseases" such as type 2 diabetes, obesity and heart disease have been emerging throughout the world (Wu et al. 2014). The higher standard of living, proliferation of digital technologies and increasing number of office jobs have contributed to the epidemic. Sedentary lifestyle is a major factor in the epidemic that increases mortality in the general population and deteriorates one's ability to work over time (Koster et al., 2012). At the workplace, the epidemic manifests itself in the reduction of employees' productivity, increasing occupational health costs, and ultimately, declining profits of employers. Employers are fighting the implications of the epidemic by introducing workplace wellness programs (WWP) that are designed to induce a healthier lifestyle in their employees. (Goetzel et al., 2014)

To facilitate employees' participation in the WWPs, many challenges need to be addressed by employers and service providers of WWPs. Some of the typical barriers to entry are the lack of: time, interest, support by management, resources and funding, and participation of high-risk employees (Pérez-Calhoon, 2017). The barriers to entry discussed within the context of this study are privacy concerns and lack of trust in regard to privacy protection of the health data that is collected in WWPs (Bottles, 2015). The COVID-19 pandemic has increased the number of telecommuters dramatically in 2020. Working from home abruptly became the new normal for which many organizations were not sufficiently prepared. Telecommuting for extended periods of time can lead to a sedentary lifestyle as well as make ergonomics-related problems more prevalent (Charalampous et al., 2019)

As the pandemic has accelerated the digitalization of services in many fields, novel digital WWPs have been introduced to the B2B market as well. Some of them are designed specifically to tackle the health issues telecommuters face. The proliferation of digital WWPs has also made addressing their trust and privacy-related barriers to entry a topical issue. For the service providers of digital WWPs, there is a financial incentive to improve participation rates, as more participants usually translate into more revenue. Similarly, employers' potential for benefitting increases, as a healthier workforce typically takes fewer sick leaves and performs more productively. As the participation rates increase in telecommuters, the potential for tackling the implications of a sedentary lifestyle and ergonomics-related problems increases on the individual level, too. (Baicker et al., 2010; Goetzel et al., 2014)

Previous research has identified online Privacy Policy Statements (PPS) as one of the key mechanisms for lowering privacy concerns and building trust between digital services and users (Bansal et al., 2015; Chang, 2018). Furthermore, some users are more experienced and/or aware of privacy issues than others. The level of disposition to value privacy also depends on the individual (Xu et al., 2011). Nevertheless, it is up to the companies themselves to develop PPSs that users are willing to read, comprehend and trust (Xu et al., 2011). Thus, to better understand privacy and trust-related factors behind the decision making of participating to digital WWPs, it is of relevance to investigate Perceived Effectiveness of Privacy Policy (PEPP) as well as its influence on users' Trust and Behavioral Intention to participate.

Wu et al. (2012) propose a model that was built on the Privacy–Trust–Behavioral Intention model (Liu et al., 2005), suggesting that PEPP has a significant relationship on Privacy Concern, Trust and the Behavioral Intention to provide personal information. Thus, building on Theory of Reasoned Action (Fishbein, 1967; Fishbein & Ajzen, 1975), the Privacy–Trust–Behavioral Intention model and the research of Xu et al. (2011), Wu et al. (2012) and Chang et al. (2018) we build a research model to study the relationship of the perceived effectiveness of a PPS on trust and behavioral intention to participate in a digital WWP for telecommuters.

The model will be empirically tested in a field study as a part of an experimental implementation project of a digital WWP for the telecommuters of the city executive office of a city located in a metropolitan area of Finland. Additional telecommuters of a similar background are recruited from the professional networks of a digital WWP service provider in social media. Our premise is that PEPP of a digital WWP has a significant relationship on telecommuters' Trust and Behavioral Intention to participate in a digital WWP. Using the model, employers and service providers of digital WWPs will be able to measure PEPP and implement informed improvements on the PPSs in efforts to increase participation rates.

## 1.2 Research Objective and Hypotheses

The main objective of the study is to test the correlations between Security, Perceived Effectiveness of Privacy Policy (PEPP), Trust and Behavioral Intention to participate in a digital Workplace Wellness Program (WWP). By testing the correlations, we aim to produce empirical evidence on whether efforts to increase PEPP are justified to potentially improve participation rates in digital WWPs.

Liu et al. (2005) used Notice, Choice, Security and Access to measure Privacy in the Privacy–Trust–Behavioral Intention (PTBI) model. PEPP was first introduced by Xu et al. (2011). Chang et al. (2018) used the Notice, Choice, Access, Security, and Enforcement as antecedents of PEPP. According to the PTBI model, Privacy has a significant effect on Trust, which then affects Behavioral Intention. Wu et al. (2012) found significant effects between Notice and Trust, Access and Trust, Security and Trust. Furthermore, Wu et al. (2012) suggest that Security is the most important concern for online users. In addition, Chang et al. (2018) found positive indirect effects between PEPP and Trust. Based on previous results, the following hypotheses are formed:

H1: Security positively affects PEPP
H2: PEPP positively affects Trust
H3: Trust positively affects Behavioral Intention
H4: Security has a positive indirect effect on Trust though PEPP
H5: Security has a positive indirect effect on Behavioral Intention through PEPP and Trust
H6: PEPP has a positive indirect effect on Behavioral Intention through Trust.

## 1.3 Structure of the Thesis

The thesis is organized into five chapters. In Chapter 2, information privacy theories, the measurement of the perceived effectiveness of privacy policies and common privacy issues in digital workplace wellness programs are discussed. Chapter 3 discusses the research methodology of the study. Chapter 4 discusses the analysis of the data and the results of the study. In Chapter 5, a discussion, conclusions, implications of the study, and limitations of the study are presented as well as future research is outlined.

# 2 LITERATURE REVIEW

In this chapter, the literature that is relevant to the topic of the thesis in the general knowledge area of information privacy is reviewed. First, an overview of information privacy research is given. Second, the key theories of information privacy are presented. Third, an integrated framework for online information privacy research is discussed. Fourth, perceived information privacy is discussed. Fifth, an outlook on information privacy policy is given. Sixth, measuring the perceived effectiveness of an information privacy policy is discussed. Seventh, the common privacy issues of workplace wellness programs are discussed. Finally, a summary is outlined.

## 2.1 Overview of Information Privacy Research

Privacy has been studied in multiple fields of social science for over a century, but still no consensus exists of its definition (Solove, 2006). Westin (1967, p. 7) regards Information Privacy (IP) as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". IP research can be classified according to their level of analysis: individual, group, organizational, and societal (Smith et al., 2011). According to Smith et al. (2011), most IP research has been carried out at the individual level. Bélanger & Crossler (2011) call out for more research out of the individual level, especially multi-level analysis studies.

Bélanger & Crossler (2011) identify the following essential topics of IP research conducted in the field of information systems: IP concerns, e-business impacts of IP, IP attitudes, IP practices, and IP tools and technologies. The research on *IP concerns* "typically seeks to explain differences in levels of privacy concern or to explore the effects of privacy concerns on various dependent variables, such as the willingness to provide personal information or the willingness to transact online" (Bélanger & Crossler, 2011, p. 1020). *E-business impacts of IP* "typically studies how individuals' views of privacy affect their intention to

participate in e-commerce or e-government interactions, or their willingness to share information with e-commerce merchants or e-government agencies" (Bélanger & Crossler, 2011, p. 1020). *IP attitudes* deals with exploring "perceptions of and reactions to information privacy policies, practices, and tools" (Bélanger & Crossler, 2011, p. 1021). *IP practices* "often explores individual and organizational actions regarding privacy protection or infringement, and various factors that affect these practices" (Bélanger & Crossler, 2011, p. 1022). *IP tools and technologies* "typically presents and/or evaluates artifacts or technological solutions for dealing with information privacy protection" (Bélanger & Crossler, 2011, p. 1022).

## 2.2 Key Theories of Information Privacy

Li (2012) identifies 14 key theories of IP: Agency Theory, Social Contract Theory, Theory of Reasoned Action, Theory of Planned Behavior, Privacy Calculus Theory, Utility Maximization Theory, Expectancy Theory of Motivation, Expectancy-Value Theory, Procedural Fairness Theory, Social Presence Theory, Social Response Theory, Protection Motivation Theory, Information Boundary Theory, Social Cognitive Theory, and Personality Theories.

*Agency Theory* "was developed to address the principal-agent problem, i.e., the difficulties that arise under conditions of incomplete and asymmetric information when a principal (such as a customer) hires an agent (such as a website) to pursue the principal's interests. A cause of such problem is the opportunistic behavior of the agent to maximize self-interests. To reduce the agency cost, various mechanisms could be used to align the interests of the agent with those of the principal, such as making efficient contracts." (Li, 2012, p. 473)

*Social Contract Theory,* "in terms of business transactions, suggests that members (i.e., persons and organizations) of a given community or industry behave fairly if their practices are governed by social contracts. A social contract is initiated when social norms (i.e., generally understood obligations) are expected to govern the behavior of those involved, and the social contracts must be grounded in informed consent buttressed by a right of exit." (Li, 2012, p. 473)

*Theory of Reasoned Action* (TRA) was built on Expectancy-Value Theory. "TRA suggests that a person's volitional behavior is determined by the person's behavioral intention to perform that behavior, and behavioral intention is in turn determined by the person's attitude toward the behavior and subjective norm." (Li, 2012, p. 473)

*Theory of Planned Behavior* (TPB) "was developed from TRA, suggesting that in addition to attitude and subjective norm, a person's perceived behavioral control (PBC) also influences behavioral intention. PBC has a direct impact on behavior as well." (Li, 2012, p. 473)

*Privacy Calculus Theory* "suggests that an individual's intention to disclose information is based on a calculus of behavior in which potentially competing factors are weighed in light of possible outcomes. A popular form of the behav-

ioral calculus is the risk-benefit analysis, where the trade-offs between expected risks and expected benefits are considered within a specific information-disclosure context." (Li, 2012, p. 473)

*Utility Maximization Theory* "suggests that consumer behavior is guided toward the maximization of total utility or total satisfaction received from consuming a goods or service. The total utility is a function encompassing aspects of the goods or service that are relevant or important to the consumer, and an optimal level is pursued by the consumer. In terms of privacy, the utility function is normally called privacy calculus" (Li, 2012, p. 473)

*Expectancy Theory of Motivation*" suggests that the motivation for a behavior is determined by the desirability of the outcome. It depicts the cognitive process of how an individual processes different motivational elements in three stages: expectancy that a certain effort will lead to the intended performance, the instrumentality of this performance to achieving a certain result, and the desirability (called valence) of this result for the individual. The three stages together determine the desirability and motivation for a behavior." (Li, 2012, p. 473)

*Expectancy-Value Theory* (EVT), "also known as the expectancy-value model of attitude, this theory was proposed to explain a person's attitude toward an object or action. It suggests that attitude arises spontaneously and inevitably as a person forms beliefs about the object/action. Each belief associates the object/action with a certain attribute (such as the risks associated with an action), and a person's overall attitude toward the object/action is determined by the subjective values of the attributes in interaction with the strength of the associations. Although people can form many different beliefs about an object/action, only beliefs that are readily accessible in memory influence attitude at any given moment." (Li, 2012, p. 473)

*Procedural Fairness Theory,* "Also known as procedural justice theory, it suggests that procedural fairness/justice serves as an intermediary to build trust when agents (e.g., websites) exercise considerable delegated power on behalf of customers who cannot specify or constrain their behavior. To mitigate customer concerns and to achieve justice in such situations, the processes by which decisions are made or actions are taken by the agents should be transparent to the customers." (Li, 2012, p. 473)

*Social Presence Theory,* "developed to study computer-mediated communication, classifies different communication media along a one-dimensional continuum of social presence, defined as the degree of awareness of the other person in a communication interaction. It suggests that communication is effective if the communication medium has the appropriate social presence required for the level of interpersonal involvement (e.g., seeing or hearing each other) required for a task." (Li, 2012, p. 473)

*Social Response Theory* "suggests that a person will engage in self-disclosure of personal information if he or she is the recipient of a similar disclosure from another person, organization, and even computer. During the pro-

cess, a norm of reciprocity is developed between the two that encourages further self-disclosure of intimate information." (Li, 2012, p. 473)

*Protection Motivation Theory* "was developed to explain the effects of fear appeals on health attitudes and behaviors. It suggest that an individual's intention to protect him or herself from potential threats depends on four factors: (1) the perceived severity of a threatening event, (2) the perceived probability of the occurrence of the event, (3) the efficacy of the recommended preventive behavior that an individual expects to carry out, and (4) the individual's perceived ability (such as self-efficacy) to undertake the recommended preventive behavior." (Li, 2012, p. 473)

*Information Boundary Theory* is also known as Communication Boundary Management theory (Petronio, 2002). "It presents a boundary coordination process through which a person manages communications in balancing a need for disclosure with the need for privacy. It suggests that individuals develop rules to form cognitive information spaces with clearly defined boundaries around themselves. These information boundaries are regulated strategically according to decision criteria (such as cost-benefit ratio and context) individuals use to judge expectations for interaction. The boundaries may be loosely or tightly controlled depending on the degree of risk associated with the information privacy." (Li, 2012, p. 473)

*Social Cognitive Theory*, "developed from social learning theory, this theory posits that portions of an individual's knowledge acquisition can be directly related to observing others within the context of social interactions, experiences, and outside media influences. In short, people learn through observing and experiencing. A key component of the learning or cognitive process is self-efficacy, representing a person's belief in his/her own competence in completing a task." (Li, 2012, p. 473)

*Personality Theories* "suggest that various personality traits, such as the Big Five (i.e., openness, conscientiousness, extraversion, agreeableness, and emotional stability) personalities, influence a person's cognitive processes and the corresponding behaviors." (Li, 2012, p. 473)

To summarize, Agency Theory and Social Contract Theory provide a foundation for the understanding of the origin of privacy concerns and help in the recognition of mechanisms of coping with privacy risks. As an empirical study framework, TRA, TPB and the underlying EVT predict a negative effect of privacy concern and a positive effect of the perceived benefit that the disclosure of information induces. Privacy Calculus Theory guides studies on the opposing forces of perceptions on privacy and their joint effect in relation to behavior. Moreover, Privacy Motivation Theory provides two drivers for studying behavioral change in relation to fear appeal: risk appraisal and the mechanisms for coping the with identified risks. The two drivers can be further interpreted by Information Boundary Theory and Personality Theories. Finally, Procedural Fairness Theory, Social Response Theory and Social Presence Theory can be utilized in studying institutional factors that affect privacy concerns. (Li, 2012)

## 2.3 An Integrated Framework for Online Information Privacy Research

Building on the interrelations of the key theories of IP, Li (2012) proposes an integrated framework for online IP research, illustrated in FIGURE 1. The framework emphasizes the two trade-offs that are interrelated, influencing the information disclosure behavior of individuals: privacy calculus (i.e. the trade-off between the perceived privacy risks and benefits) and risk calculus (i.e. the trade-off between perceived privacy risks and coping mechanisms' efficacy). The combination of the two trade-offs is called Dual Calculus Model. (Li, 2012)

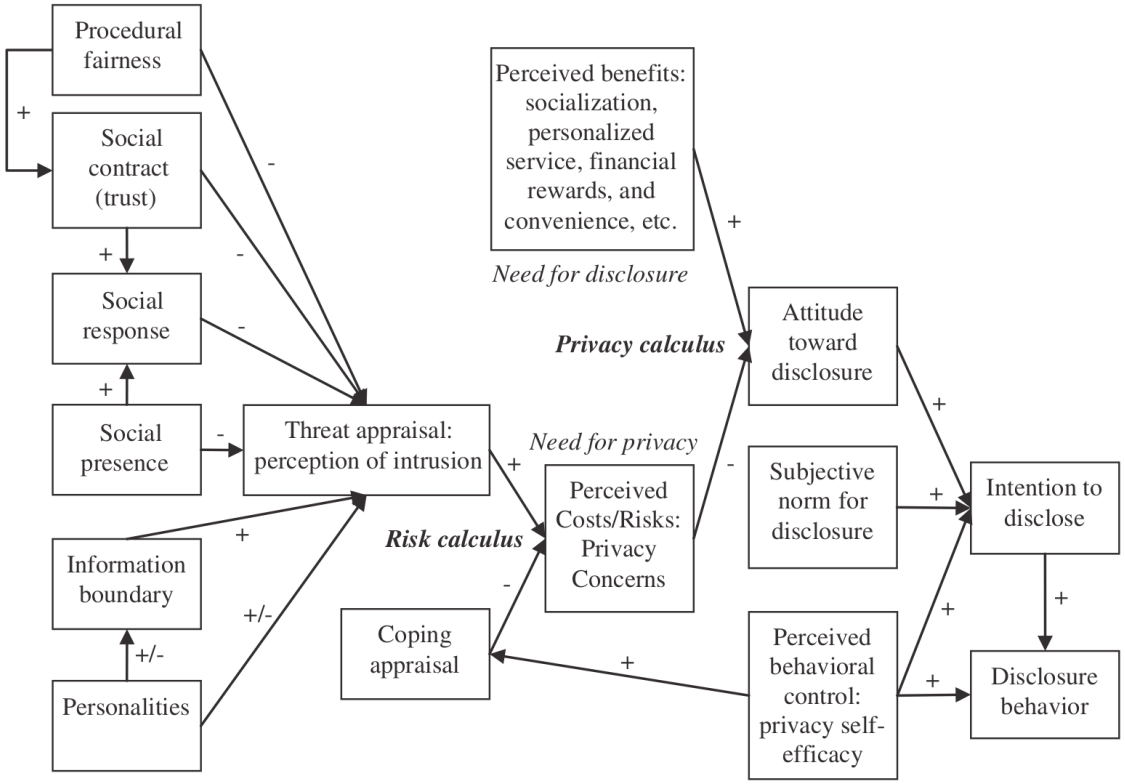


FIGURE 1 Integrated Framework for Online Information Privacy Research (Li, 2012, p. 477)

TPB is adopted as the basis of the framework to outline the relationships between privacy antecedents, privacy belief, privacy-driven behavioral intention and privacy behavior. The framework suggests that information disclosure behavior is positively influenced by intention and ability, and that intention is positively influenced by attitude toward disclosure, subjective norm for disclosure, and PBC, including privacy self-efficacy. Attitude toward disclosure is developed from an overall assessment (i.e. privacy calculus) of behavioral beliefs, including privacy concerns and perceived benefits. Privacy calculus functions as a summation of personal beliefs regarding the expected benefits and negative outcomes of information disclosure. The perceived benefits include

socialization, convenience, personalized service, fun, and financial rewards, etc. The factors that influence privacy concerns include institutional factors (i.e. procedural fairness, social contract, social response, and social presence) and individual factors (i.e. protection motivation, information boundary, self-efficacy, and personalities). The risk calculus measures an individual's perceived net risks (such as net privacy risks) in online transactions based on threat appraisal and coping appraisal. It is calculated as the difference between expected risks and expected coping effectiveness. (Li, 2012)

Thus, if the privacy threat is unmatched by the coping mechanisms, the net risk is high, and, if the coping mechanisms overcome the privacy threat, the net risk is low. Furthermore, if a person is more capable of protecting her online privacy, she would be more willing to perform high-risk transactions if necessary, and a person who has limited privacy protection capabilities would be unwilling to participate in even the least-risky transactions unless the stake is very high. (Li, 2012)

## 2.4 Perceived Information Privacy

Perceived IP falls under the research topic of IP Attitudes (Belanger & Crossler, 2011) and its concepts are used in the integrated framework for online information privacy research (Li, 2012). There is a plethora of research available on individuals' perceptions on IP. Typically, the research models of the studies have been derived from the Communication Boundary Management theory.

### 2.4.1 Communication Privacy Management Theory

Communication Privacy Management (CPM) theory is a well-established theoretical framework for the investigation of perceived information privacy issues (Petronio, 2002). CPM "offers a privacy management system that identifies ways privacy boundaries are coordinated between and among individuals" (Petronio, 2002, p. 3). For instance, CPM has been utilized to study privacy issues of co-worker Facebook friend requests (Frampton & Child, 2013), and personal fitness data sharing (Zimmer et al., 2018). According to CPM, individuals have an intrinsic need for privacy, which is defined as "the feelings that one has the right to own private information, either personally or collectively" (Petronio, 2002, p. 6).

An individual's ability to manage the boundary between private and publicly shared information can become problematic, if stakeholders that do not "co-own" the private information attempt to access it. CPM delineates that because individuals and groups inherently need some privacy, they will seek to regulate the dialectical tension between privacy and disclosure by setting boundaries around their information based on decision criteria used to generate privacy rules. The privacy rules are then open to negotiation, coordination,

transmission, and modification. Privacy boundary turbulence can occur when problems exist with privacy boundary management. (Petronio, 2002)

At a work environment, individuals manage personal, dyadic, group, and organizational privacy boundaries and seek to coordinate the permeability, linkages, and ownership of private information (Petronio, 2002). For instance, individuals can perceive electronic surveillance at work as an invasion of privacy that can harm one's personal identity, one's estimation of oneself, the image one wants to portray, and one's social identity in the group, as well as, the quality of one's work life. Organizations often serve as sites of contested privacy boundary ownership even though power is unevenly distributed between employers and employees. (Allen et al. 2007)

### 2.4.2 Concepts and Correlates of Perceived Information Privacy

Dinev et al. (2013) present an integrative model for perceived information privacy concepts and correlates, presented in FIGURE 2. They define perceived information privacy as: "an individual's self-assessed state in which external agents have limited access to information about him or her". Their proposed model depicts that individuals' perceived information privacy is dependent on perceived information control and perceived risk. The relevant correlates to information privacy are anonymity, secrecy, confidentiality, and control. Anonymity, secrecy, and confidentiality are tactics of information control. Furthermore, perceived risk is a function of perceived benefits of information disclosure, information sensitivity, importance of information transparency, and regulatory expectations. The model was empirically validated by surveying Web 2.0 applications' users. (Dinev et al., 2013)

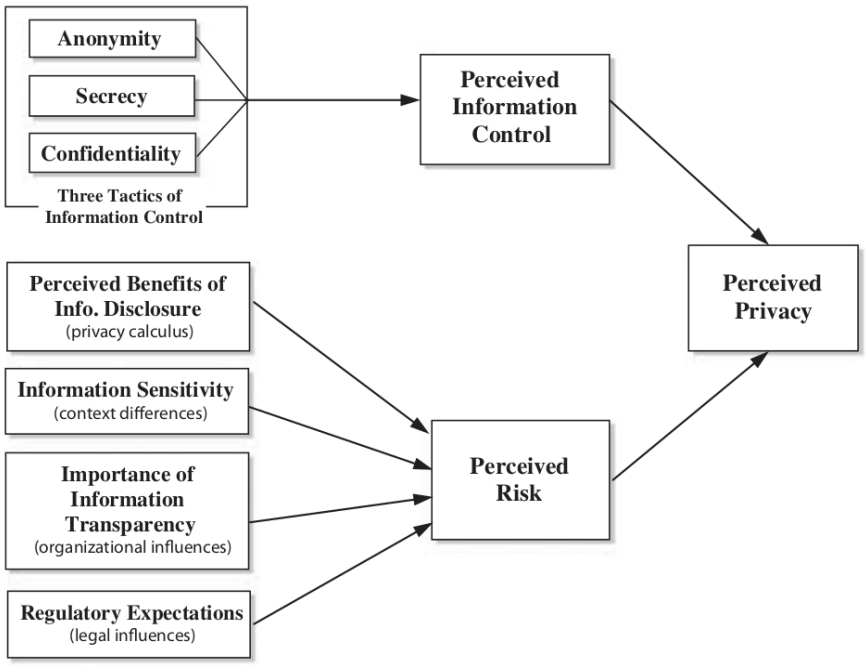


FIGURE 2 Model of Perceived Information Privacy Concepts and Correlates (Dinev et al., 2013, p. 298)

Dinev et al. (2013) define perceived information control as "an individual's beliefs in one's ability to determine to what extent information about the self will be released onto the Web 2.0-related sites". The three tactics of information control, anonymity, secrecy, and confidentiality are adopted from a theoretical framework on identity management proposed by Zwick & Dholakia (2004). The three tactics are applied by consumers to manage the externalization of their personal information. *Anonymity* is the tactic to conceal a person's identity. *Secrecy* is the tactic of the intentional concealment of information. *Confidentiality* is the tactic that restricts the information flow in terms of what is externalized as well as who gets to see it. (Dinev et al., 2013)

Dinev et al. (2013) define perceived information risk as "user's perceived expectation of suffering a negative outcome as a consequence of online disclosure of personal information". They also suggest that perceived information risk is a function of perceived benefits of information disclosure, information sensitivity, importance of information transparency, and regulatory expectations. *Perceived benefits of information disclosure* is adopted from privacy calculus which means the concept is directly compliant with its counterpart in the integrated framework for online information privacy research (Li, 2002). *Information sensitivity* is "a personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent". *Importance of information transparency* is "the consumer-rated importance of notifying the consumers what types of information a firm has collected about them, and how that information is going to be used". Finally, *regulatory expectations* refers to individuals' assumptions about the existence of effective legislative approaches that can regulate the type of personal information external agents are allowed to collect from individuals, as well as the ways with which the stored personal information should be protected against misuse. (Dinev et al., 2013)

### 2.4.3 Linking Perceived Information Privacy to Information Privacy Policy

Xu et al. (2011) suggest that individuals' perceived IP in relation to an organization is linked to institutional assurances. Their research model is illustrated in FIGURE 3. They propose that an individual's privacy concerns form through a cognitive process involving perceived privacy risk, privacy control, and the individual's disposition to value privacy. Moreover, individuals' perceptions on institutional privacy assurances, i.e. perceived effectiveness of privacy policies and perceived effectiveness of industry self-regulation are suggested to affect the risk-control assessment of information disclosure. The model was tested by surveying the users of various types of websites and analyzing the collected data with statistical methods. (Xu et al., 2011)

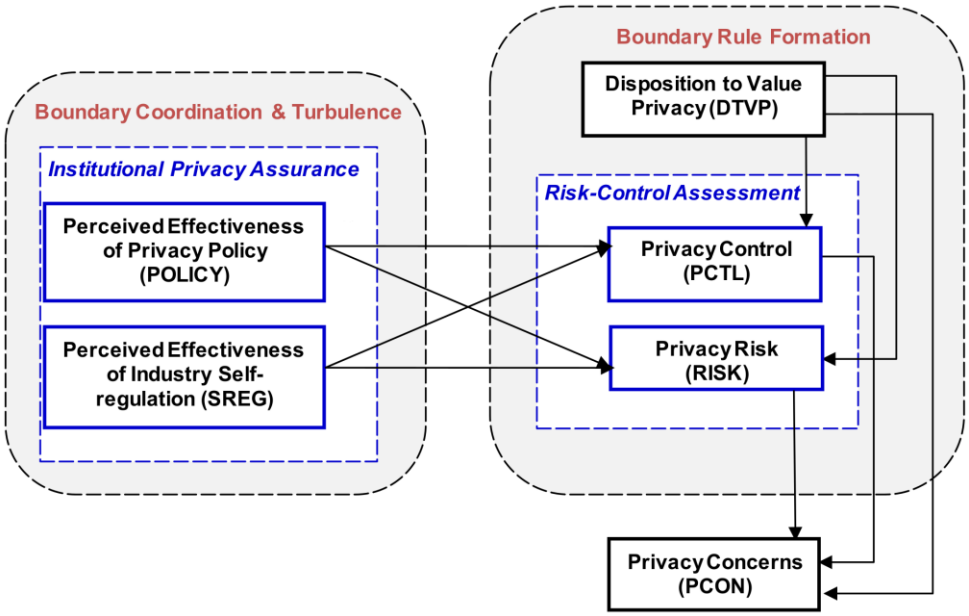


FIGURE 3 Model of Linking Individuals' Information Privacy Perceptions to Institutional Assurances (Xu et al., 2011, p. 803)

Xu et al. (2011) use the concept of a privacy concern as a synonym for IP related beliefs, attitudes and perceptions. The model is based on CPM theory from which the concepts of boundary rule formation and boundary coordination and boundary turbulence are drawn. According to the model, privacy concerns are formed "by an individual's perceived boundary of the information space that depends on a contextual risk-control assessment, as well as on the individual's personal dispositions", and "by institutional privacy assurances that enable a person to assess the consequences of information disclosure and coordinate boundary management". Moreover, they define the concept of a disposition to value privacy as "a personality attribute reflecting an individual's inherent need to maintain certain boundaries that frame personal information space". They also state that the privacy boundary management rules are situational and dependent on individuals' personality, which adds to the complex and dynamic nature of IP and IP concerns. (Xu et al., 2011, p. 803)

As situational and environmental factors influence information boundary management rules, Xu et al. (2011) regard institutional assurances as essential environmental factors that influence individuals' decisions on opening and closing the information boundary. In the model, the institutional assurance components are institutional dimensions of IP interventions that represent the environmental factors influencing IP decisions. They define institutional IP assurance as "the interventions that a particular company makes to ensure consumers that efforts have been devoted to protect personal information" (Xu et al., 2011, p. 805). The interventions are made also to assure individuals that the company's information practices are reasonable and fair. Two typical interventions that companies can implement and control in their information practices are information privacy policy and industry self-regulation. The implementa-

tion of institutional IP assurances is predicated on the assumption that companies have an incentive to address IP concerns because if they fail to do so, they will suffer reputational losses. (Xu et al., 2011)

Xu et al. (2011) define a privacy policy as "a mechanism through which consumers can be informed about the choices available to them regarding how the collected information is used; the safeguards in place to protect the information from loss, misuse, or alteration; and how consumers can update or correct any inaccurate information". The implementation of privacy policies is typically based on fair information practices. Furthermore, they define perceived effectiveness of privacy policy as "the extent to which a consumer believes that the privacy notice posted online is able to provide accurate and reliable information about the firm's information privacy practices". In addition, they define the perceived effectiveness of industry self-regulation as "the extent to which consumers believe that self-policing industry groups and certifying agencies are able to assist them in protecting their online privacy". (Xu et al., 2011, p. 804)

In the empirical testing of the model, Xu et al. (2011) found that the perceived effectiveness of privacy policy increases individuals' perceived privacy control. Moreover, it was validated that the perceived effectiveness of privacy policy reduces consumers' perceived privacy risk. Similar claims on industry self-regulation could not be validated in the study. Therefore, it was indicated that the perceived effectiveness of privacy policy is linked to perceived privacy control and perceived privacy risk, which are then again linked to privacy concerns. (Xu et al., 2011)

## 2.5 Information Privacy Policy

Schwaig et al. (2013) suggest that, in a business context, customers hold the companies, not the digital services, responsible for any inappropriate use of their personal information. Therefore, companies ought to be proactive in developing and enforcing privacy policies in order to address customers' privacy concerns (Schwaig et al., 2013). Companies publish their privacy policies online to build trust towards the customers (Chang et al., 2018).

Xu et al. (2011) suggest that, to a large extent, it is up to the companies themselves to impact the customer's perceptions on IP. This can be achieved by making the privacy policies easily accessible and by emphasizing in their wording and presentation the implemented IP management practices that reduce the privacy risks and empower the customers with control over their personal information (Xu et al., 2011).

However, according to Tsai et al. (2011) customers rarely make the effort to properly read and understand privacy policies. Nevertheless, their findings show that when the user interface of an online service clearly and compactly displays privacy policy information, customers prefer to purchase from such services, suggesting that companies may be able to leverage privacy protection as a selling point (Tsai et al., 2011).

Furthermore, Earp et al. (2005) studied the Internet users' expectations about website IP and compared them to the privacy policy statements of 50 websites of the most stringently regulated organizations such as healthcare institutions. They found a notable discrepancy between what privacy policies are stating and what users deem most significant on IP. (Earp et al., 2005)

Earp et al. (2005 used a content analysis method to formulate a privacy policy content taxonomy presented in TABLE 1. Twelve categories were identified by analyzing the privacy policy statements: notice/awareness, choice/consent, access/participation, integrity/security, enforcement/redress, information monitoring, information aggregation, information storage, information transfer, information collection, information personalization, and contact (see TABLE 1 for the definitions). The categories were further classified under privacy protection goals that aim to protect user privacy rights, and privacy vulnerability goals that potentially invade users' privacy. (Earp et al., 2005)

TABLE 1 Privacy Policy Content Taxonomy (Earp et al., 2005, p. 230)

| Privacy Protection Goal Classifications | Privacy Vulnerability Goal Classifications |
|---|---|
| *Notice/Awareness*<br>*Assert that users should be notified and/or made aware of an organization's information practices (e.g., via an organization's privacy policy) before any information is actually collected from them.* | *Information Monitoring*<br>*Organizations' tracking practices (e.g. what users do on their site through means such as cookies). Could be for the user's benefit (e.g. when an e-commerce application maintains a shopping cart for a user), or for the organization's benefit, be it for purely statistical use or for profit (e.g. via selling of aggregated information to 3rd parties).* |
| *Choice/Consent*<br>*Ensure that users are given the option to decide what personal information collected about them is to be used and whether it may be used for secondary purposes.* | *Information Aggregation*<br>*Aggregation practices as when organizations combine previously gathered data in such a way that they create non-identifying statistical data often used for marketing and promotional purposes.* |
| *Access/Participation*<br>*Allow or restrict access to a particular site or functionality based upon whether or not the user provides their PII (Personally Identifiable Information). Address the ability for users to access or correct their PII.* | *Information Storage*<br>*What and how records are stored in an organization's database.* |
| *Integrity/Security*<br>*Ensure that data are both accurate and secure. Security and accuracy come from both the user and the organization collecting the personal information. Goals in this category range from vague ones stating only that personal information is securely kept to specific technical descriptions of what security protocols will be used to transfer personal information over the Internet.* | *Information Transfer*<br>*Any transfer of information. Privacy by its very definition means insurance that others cannot find something out, that information must not be transferred. Addresses the transfer of information, as well as to whom what information is transferred.* |
| *Enforcement/Redress*<br>*Address the mechanisms in place to enforce privacy. Prescribe general guidelines that companies and their employees should follow. These include both self-imposed and government imposed work restrictions. Redress includes possible actions for consumers harmed by a violation of the policy.* | *Information Collection*<br>*How and what information is being collected. Collection occurs when an organization collects information from a user either by directly requesting that they enter the information, or by collecting information without user consent, such as browser information.* |
| | *Information Personalization*<br>*Actions that reflect the customization of a website to a specific visitor, thus affecting the functionality/content offered to individuals. This may be as simple as greeting the website visitor by name (e.g. "Welcome, George.")* |
| | *Contact*<br>*How and for what purpose organizations contact users using their personal information. This could be helpful, such as contacting customers to validate an email address, or annoying, such as sending out unwanted promotions based on past patterns.* |

The privacy policy content taxonomy provides a useful framework for comparing and analyzing information privacy policy statements. It can be used by researchers, managers in organizations, and website developers to ensure that their stated and actual privacy policies are consistent with each other and that they reflect what online users value. (Earp et al., 2005)

## 2.6 Perceived Effectiveness of Privacy Policy

Drawing on the CPM theory, Chang et al. (2018) propose a Privacy Boundary Management Model (PBMM) to explain how customers formulate and manage their privacy boundaries. Building on the work of Wu et al. (2012), PBMM examines privacy policies through the five dimensions of Fair Information Practice Principles (FIPPs), provided by United States Federal Trade Commission (FTC): notice, choice, access, security, and enforcement. PBMM analyzes the effect of FIPPs on the privacy boundary formation to assess how customers associate these dimensions to the effectiveness of a privacy policy. (Chang et al., 2018)

The empirical validation of PBMM indicated that four (access, notice, security, and enforcement) out of the five dimensions have significant impact on the perceived effectiveness of a privacy policy. The study also found that the perceived effectiveness of a privacy policy significantly influences perceived privacy control and perceived privacy risk. Furthermore, perceived privacy control significantly influences trust and perceived IP. Perceived privacy concern and trust also significantly influence perceived IP. (Chang et al., 2018)

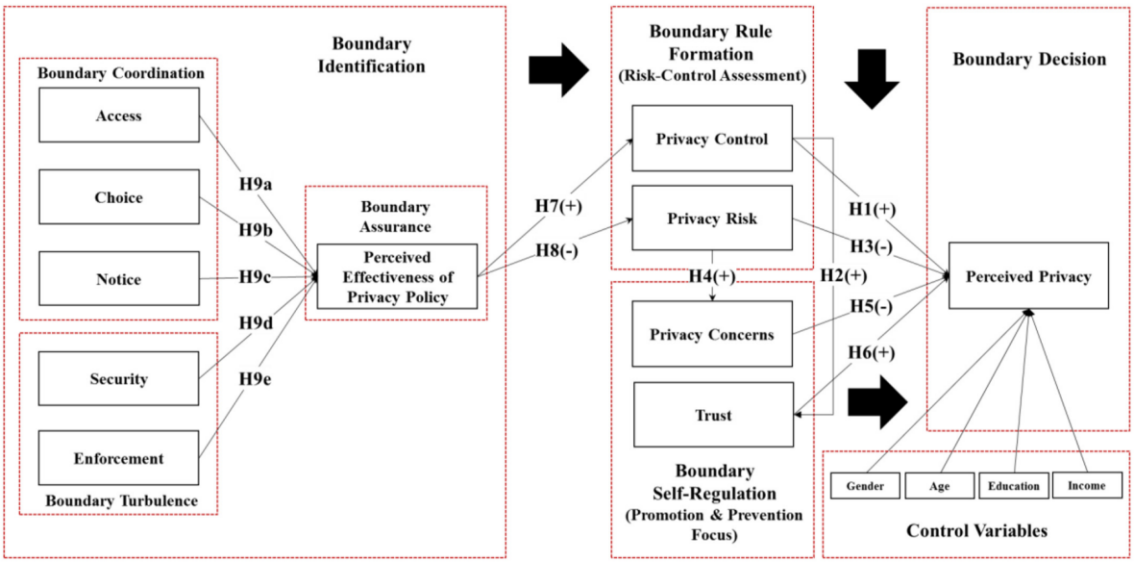


FIGURE 4 Privacy Boundary Management Model (Chang et al., 2018, p. 449)

PBMM follows a four-phase process, that depicts an individual's privacy boundary management process. The phases of the process are 1) institutional

boundary identification, including coordination, turbulence, and assurance, 2) boundary rule formation, 3) boundary self-regulation, and 4) individual boundary decision. According to the process, individuals constantly, recursively and iteratively adjust their privacy boundary based on their latest experiences and information gathered. (Chang et al., 2018)

Apart from trust, the key concepts of PBMM are defined in the previous sections. Chang et al. (2018, p. 448) define *trust* as "the willingness to take risks". The relationships between the concepts are denoted as H1-9, followed by (+) as an indication of a positive influence as well as (-) for negative influence. The black arrows represent the transitions of the PBMM process. Chang et al. (2018) used gender, age, education and income as control variables for the model testing (Chang et al., 2018)

In PBMM, The FIPPs of access, choice and notice are categorized as boundary coordination concepts, whereas security and enforcement are boundary turbulence concepts. The FIPPs influence the concept of perceived effectiveness of privacy policy, which is categorized as a boundary assurance concept. These concepts belong to the institutional boundary identification phase, which then affects the boundary rule formation phase, i.e. the risk-control assessment of individuals. The concepts of privacy control and privacy risks belong to the boundary rule formation phase, which then affects the boundary self-regulation phase, in which the concepts of privacy concerns and trust belong. Finally, the concepts of boundary rule formation and boundary self-regulation phases influence the perceived IP concept that belongs to the individual boundary decision phase. (Chang et al., 2018)

## 2.7 Privacy Issues in Workplace Wellness Programs

Along with the potential health and financial benefits of Workplace Wellness Programs (WWPs), many challenges have to be addressed as well when implementing WWPs. Some of the common barriers to entry into WWPs are the lack of: time, interest, support by management, resources and funding, and participation by high-risk employees (Pérez-Calhoon, 2017). Another key barrier to entry is the perceived privacy risks related to the personal health data (PHD) that is produced, processed and stored in WWPs (Bottles, 2015). Some of the other privacy-related concerns are: unequal treatment, selling of PHD to third parties, and limitless surveillance (Tu & Mayrell, 2010; Ajunwa et al., 2017; Lupton, 2016b). Additionally, employees are not always provided with the opportunity to choose whether to share their data (Lupton, 2016b). A common issue is also that employees perceive that WWPs are something that are done to them, not for them. Thus, it's important that participation in WWPs is voluntary.

The data privacy legislation is also lagging behind in many countries, as the stakeholders of WWPs aren't usually subjected to the stricter regulations that, for example, healthcare organizations must adhere to in PHD processing. This often predisposes the PHD of WWPs under a state of implicit regulation,

creating potential privacy risks such as breach of confidential information, lack of access control and identity theft for the stakeholders involved. The enforcement of GDPR has benefited the citizens of EU in that regard, as nowadays it is explicit that PHD of WWPs are owned and controlled by the individuals themselves. Recent technological advancements in fields such as big data analytics, communications capture, mobile device design, DNA testing, and biometrics have dramatically increased the exploitation potential of PHD (Ajunwa et al., 2017). Thus, up-to-date legislation is needed to promote the entry of employees to WWPs, too.

In the recent years, the adoption of wearable technologies such as physical activity trackers has been steadily increasing in WWPs. In 2016, nearly one out of three large employers surveyed in the UK provided wearable devices to track employees' physical activity, with the aim to save money and improve their health and happiness (Willis Towers Watson, 2016). The evidence from a recent study indicates that the mere participation in WWPs that use activity trackers effectively increases the daily step count as well as physical and psychological well-being of employees (Giddens et al., 2017). Yet, another study that investigated employees' attitudes towards step count sharing at the workplace, found evidence of employees having growing concerns on: data privacy, general obsession to track, the amount of extra time required, and, the potential blurring of the lines between work and private life (Gorm & Shklovski, 2016).

Lupton (2016a) identifies five modes of self-tracking that relate to the different conditions of data sharing: private, pushed, communal, imposed and exploited. The conditions vary based on how tracking platforms provide notice and obtain consent regarding how data is being collected, what data is collected, and how it is being used (Lupton, 2016, p. 143). The pushed self-tracking mode is the most relevant in the context of this study as it is being manifested, for example, when employers expect the employees to sign up to WWPs, in which activity tracking is required. It's also a fine line between pushed and imposed self-tracking, for instance, in a situation where an employee is given a penalty such as a higher health insurance premium for not participating in self-tracking (Lupton, 2016b). Furthermore, the data generated from many of these modes of activities are exploited by many different actors and agencies for commercial, managerial, governmental or research purposes (Lupton, 2016a). Lupton and Michael (2017) further suggest that the particular context of the collection and use of the data strongly determines users' concerns about tracking and surveillance.

The common privacy concerns in regard to wearable technologies are related to the potentially large amount of data collected, as well as, sharing, access, and control of the data (De Mooy & Yuen, 2017). Currently, there is no comprehensive set of privacy and security regulations, guidance, standards, or best practices for companies that provide wearable technology products and services (De Mooy & Yuen, 2017). Similarly, there is no overarching guidance for the employers that run WWPs or companies that provide added-value services for the WWPs, using wearable technologies. In other words, the ecosystem of

WWPs, in which wearable technologies are utilized in various capacities, is often implicitly regulated. Nevertheless, GDPR has recently given a solid foundation for the data privacy management of such ecosystems on a general level, as well as, more specific regulations for the controllers and processors of PHD, applicable in product and service design.

## 2.8 Summary

In this chapter, the literature that is relevant to the topic of the thesis in the general knowledge area of information privacy was reviewed. First, a brief overview of information privacy research was given. Second, the key theories of information privacy were presented. Third, an integrated framework for online information privacy research was discussed. Fourth, perceived information privacy was discussed. Fifth, an outlook on information privacy policy was given. Sixth, measuring the perceived effectiveness of an information privacy policy is discussed. Finally, the common privacy issues of workplace wellness programs were discussed.

# 3 RESEARCH METHODOLOGY

In this chapter the research methodology for the study is discussed. First, research model development is discussed. Second, scale development and the survey instrument development are discussed. Third, data collection and the research setting are described. Fourth, the selection of the data analysis method is discussed. Finally, a summary of the chapter is outlined.

## 3.1 Research Model Development

Theory of Reasoned Action (TRA; Fishbein, 1967; Fishbein & Ajzen, 1975) is one of the most influential theories in social and psychological literature (Staats, 2004). Throughout the past decades it has been extensively used in predicting behavioral intentions and/or behaviors (Liu et al., 2005). According to TRA, the attitudes and perceptions of an individual influence his/her actions when he/she believes that a behavior is linked to a specific outcome. Furthermore, subjective norms and social pressures of performing a behavior will influence the behavioral intentions, determined by his/her positive or negative evaluation of it. (Liu et al., 2005)

Liu et al. (2005) adapted TRA for information privacy research and developed the Privacy–Trust–Behavioral Intention (PTBI) model. PTBI was originally considered in the context of ecommerce. They apply the logic of TRA in the following way: "a customer's perception and attitudes regarding privacy and trust should influence his or her attitudes toward online transactions and in turn, shape his or her behavioral intentions to participate in an online business activity" (Liu et al., 2005, p. 291). For the measurement of Privacy, they apply the FIPS, of which there were four at that time. Trust is measured by degree of trust a person has towards an online business activity. Behavioral Intention considers dimensions related to economic activity in the ecommerce. BTBI was tested with university students and strong support for the model was found. Since

then it has been applied in multiple studies in privacy research. The BTBI model is presented in FIGURE 5. (Liu et al., 2005)

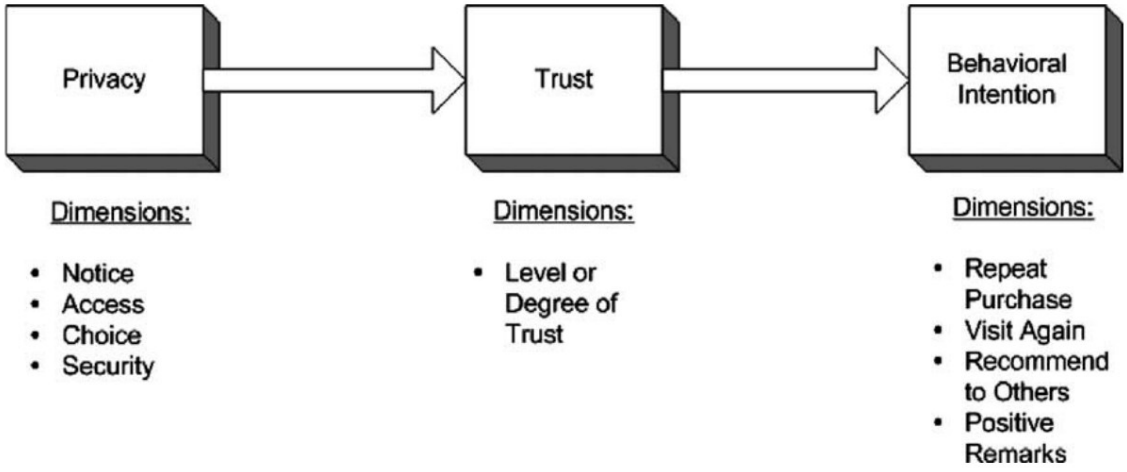


FIGURE 5 The Privacy–Trust–Behavioral Intention model (Liu et al., 2005, p. 292)

Wu et al. (2012) then applied BTBI in their research model, augmenting it with Privacy Concern and cross-cultural effects (power distance). Whereas BTBI considered privacy on a more general level, Wu et al. (2012) focused on privacy policy. They also used the FIPS to measure the user perceptions on privacy policy. The model was tested with a total of 500 participants from Russia and Taiwan. The findings indicate that there are significant relationships between Privacy Policy and Privacy Concern and Trust as well as Privacy Concern and Trust and willingness to provide personal information (Behavioral Intention). Privacy Concern also influences Trust. They also found that from Privacy Policy, Security had the largest impact on Privacy Concern and Trust. The model is presented in FIGURE 6. (Wu et al., 2012)

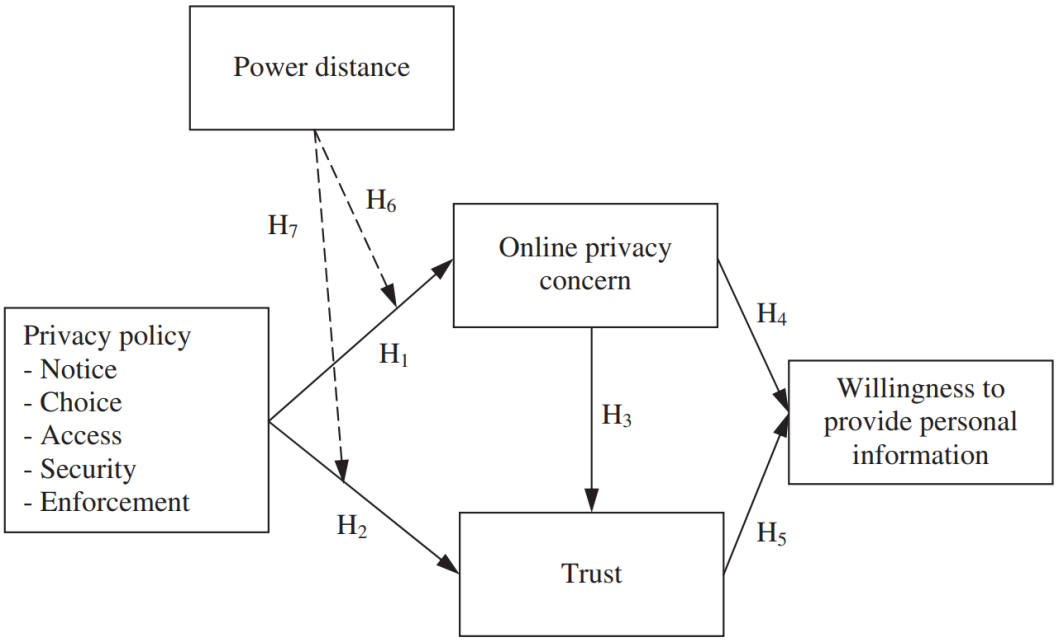


FIGURE 6 The Research Model of Wu et al. (2012, p. 895)

The model of Xu et al. (2011) introduced the construct Perceived Effectiveness of Privacy Policy. Chang et al. (2018) used the FIPs as constructs that affect PEPP. Furthermore, Wu et al. (2012) found that Security is the most important dimension of the FIPs for online users. This indicates that in the efforts of developing privacy policies and online services, the focus should be on providing security information for users to maximize Trust.

We adapt the core constructs of previous studies to our research model to ensure close alignment with TRA and BTBI: Security, PEPP, Trust and Behavioral Intention. Security is an in independent construct and PEPP, Trust and BI are dependent constructs. The BI in our study is willingness to participate in a digital WWP. The research model is presented in FIGURE 7, annotated with the IDs of our hypotheses to be tested. The direct effects under study are denotated as arrow-ended lines. The indirect effects under study are denotated as dashed arrow-ended lines. As control variables, age, gender, education, employment sector, telecommuting and sample group are utilized.

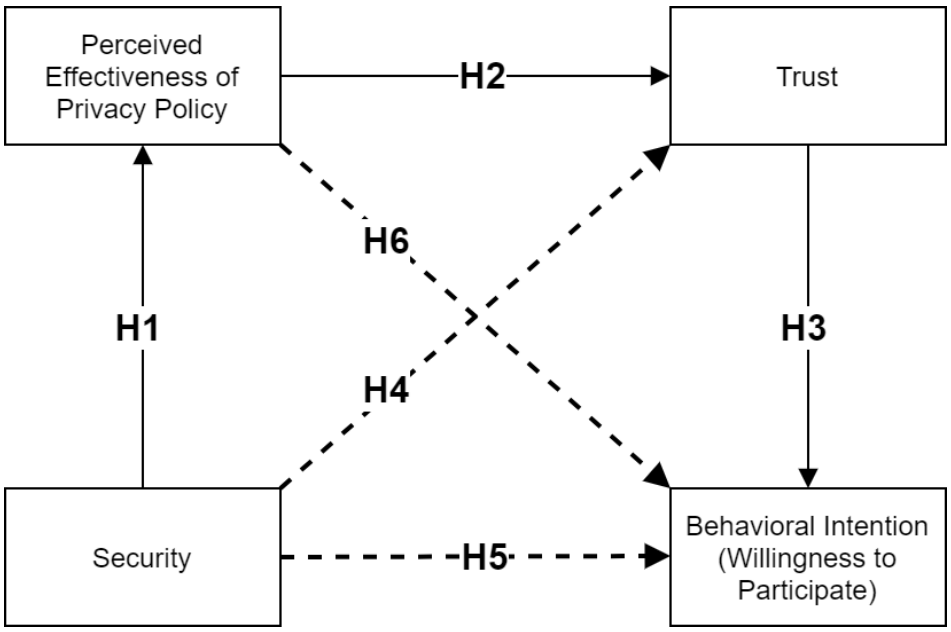


FIGURE 7 Research Model

## 3.2 Scale Development and Survey Instrument

As we are investigating behavioral concepts that cannot be observed directly, we use the survey method to measure the variables of our research model (Groves et al., 2004). The previous studies also used surveys to collect the data for testing their research models. Wu et al. (2012) developed three measurement items for Security, which are adapted as a scale for our survey instrument. From the model of Xu et al. (2011) we adapt three items for PEPP. Furthermore, we adapt three items for Trust from Wu et al. (2012). For BI we develop three items of our own as we found no applicable existing items for our research set-

ting. A 7-point Likert scale is used to measure the items. However, it is required that the items are contextualized in order to be useful in a real-world situation. TABLE 2 describes the variables, items and respective questions to be used in the survey. For the questions, the original questions from previous studies as well as our contextualized adaptations are presented.

TABLE 2 Variables and Measurement Items

| **Variable** | **Item** | **Questions** |
|---|---|---|
| Security (Wu et al., 2012) | SECURITY1<br>SECURITY2<br>SECURITY3 | Original Questions:<br>1. The website explains that the domain takes some steps to provide security for personal information has been collected<br>2. The website informs that any personal information will not be disclosed to third party<br>3. The website has the advanced technology to protect your personal information<br>Contextualized Questions:<br>1. The privacy policy informs you about the fact that appropriate measures have been taken to secure the personal information collected<br>2. The privacy policy informs you about the fact that personal information collected can only be disclosed to a third party by an agreement<br>3. The privacy policy informs you about the fact that advanced technology has been implemented to protect the personal information collected |
| Perceived Effectiveness of Privacy Policy (Xu et al., 2011) | PEPP1<br>PEPP2<br>PEPP3 | Original Questions:<br>1. I feel confident that these websites' privacy statements reflect their commitments to protect my personal information<br>2. With their privacy statements, I believe that my personal information will be kept private and confidential by these websites<br>3. I believe that these websites' privacy statements are an effective way to demonstrate their commitments to privacy<br>Contextualized Questions:<br>1. Based on reading this privacy policy, I am confident that it represents this company's commitments to protect my personal information in a realistic way<br>2. Based on reading this privacy policy, I am confident that this company keeps my personal information private<br>3. Based on reading this privacy policy, I am confident that it is an effective way for this company to demonstrate their commitments to protect my privacy |
| Trust (Wu et al., 2012) | TRUST1<br>TRUST2<br>TRUST3 | Original Questions:<br>1. Even if not monitored, I would trust them to do the job right<br>2. I trust those who protect personal information<br>3. I believe that they are trustworthy<br>Contextualized Questions:<br>1. I trust that this company operates according to the privacy policy<br>2. I trust companies that have implemented high-level privacy practices<br>3. I believe that this company is trustworthy in protecting my personal information |
| Behavioral Intention (Willingness to Participate) | BI1<br>BI2<br>BI3 | 1. I would be willing to participate in a digital WWP that implements the privacy practices described in the privacy policy<br>2. For me, the privacy practices described in the privacy policy would not constitute a barrier of entry to the digital WWP<br>3. The privacy practices described in the privacy policy encourage me to participate in the digital WWP |

It has been suggested by prior research that employees' personal characteristics may affect how they evaluate privacy issues (Bartel Sheehan, 1999; Petronio, 2002; Xu et al., 2012). Thus, we include age, gender and education as control variables for Security, PEPP and Trust. As our focus is on a digital WWP that is targeted to working professionals who telecommute regularly, we also add employment sector and telecommuting as control variables for BI. As our data sample was formed by combining a convenience sample and a random sample, sample group is also included as a control variable to investigate the potential effect of the sampling method on Security, PEPP, Trust and BI. The control variables are used to control for effects of extraneous variables on dependent variables. The control variables are presented in TABLE 3.

TABLE 3 Control Variables and Measurement Items

| Variable | Item | Range / Question |
|---|---|---|
| Gender | GENDER | Male<br>Female |
| Age | AGE | 18-24<br>25-29<br>30-34<br>35-39<br>40-49<br>50-59<br>60-69<br>70+ |
| Education Level | EL | Basic education<br>Matriculation examination / Vocational qualification<br>Post-Secondary / Higher Vocational Level Diploma<br>Bachelor's degree<br>Master's degree<br>Doctoral degree / Licenciate |
| Primary Employment Sector | ES | Public Sector<br>Private Sector<br>Third Sector |
| Telecommuting | TELE | I telecommute regularly (yes/no) |
| Group | GROUP | The sample group (convenience/random) |

A localized online instantiation of the survey instrument was developed using modern web development technologies. The instrument is structured as follows: a) introduction, b) control variables, c) privacy policy of a WWP, d) survey variables, e) a voluntary feedback form, f) (lottery) participation form, and g) end notes. As the survey library and a managed database for the responses, a software developer-friendly solution called SurveyJS was utilized. A considerable amount of development effort went into optimizing the user experience of the instrument for both desktop and mobile users. We ended up developing our own survey solution as none of the tested SaaS solutions provided the flexibility nor the usability that was required by us for the purpose of maximizing the respondent participation rate. Responding to the survey, including reading the privacy policy statement takes about 5 minutes

on average. The online survey instrument was hosted in a high-availability public cloud infrastructure.

## 3.3 Data Collection and Research Setting

The study is conducted under the quantitative research paradigm, in which an online survey is the data collection method. The data collection was conducted in a customer project of a wellness technology company that offers a digital Workplace Wellness Program (WWP). The selected population is Finnish white-collar telecommuters within the fields of HR, business development and IT. As the sampling method, a convenience sample is first used. The data was collected in a pilot project in which a novel type of a digital WWP was rolled out to the employees of a city executive office of a Finnish metropolitan city. The employees were encouraged to take the survey as a part of the enrollment process to the digital WWP. The privacy policy that governs the data management practices of the digital WWP is under investigation in this study. As the data collection that was conducted during the pilot project yielded only 30 responses, a supplementary random sampling method was then used to collect more responses. In the second phase of data collection, the company's social media marketing automation solutions were used to disseminate the survey link programmatically via LinkedIn to random Finnish professionals in the fields of HR, business development and IT. The respondents were incentivized by an opportunity to participate in a lottery of the company's wellness technology products. The data was collected anonymously. The data collection was started 8.10.2020 and stopped 13.11.2020. Finally, the 30 responses from the convenience sample and the 73 responses from the random sample were combined. Thus, a total of 103 responses were collected.

### 3.3.1 Digital Workplace Wellness Program Under Study

Recently, a research-based wellness technology startup company developed a novel digital WWP in which their scientifically validated physical activity trackers are utilized. The digital WWP is optimized for telecommuters, which is beneficial at the time of the pandemic as telecommuting is encouraged by the officials. The WWP utilizes the measurement of the everyday physical activity levels of employees and/or groups of employees at the workplace in a very accurate detail. The WWP provides analytical information and recommendations for the employees, for example, in regard to their habits of taking microbreaks and carrying out everyday activities as an individual and/or a group. The employees then participate in an online intervention program that interactively and systematically guides them in e.g. breaking long sitting bouts, optimizing remote work ergonomics and reducing sitting time. Decision makers such as HR managers can further utilize the anonymized group data in the manage-

ment and optimization of their investments on WWPs. The WWP demands little extra time and effort from the employees as the tracker requires no interaction and the tracking lasts only up to a week per employee per measurement, which also brings attrition rates down. The participation in the online intervention program only takes about 5 minutes daily and is designed to engage the employee in the behavior change. As the end results of a delivered digital WWP, detailed reports and certificates are provided for the use of the employees and/or customer organization. Furthermore, webinars are organized in which the results of the different phases of the digital WWP are discussed.

According to the company, the digital WWP has been designed from the ground up with GDPR compliance in mind, and, for example, the principles of anonymization, minimization, and privacy by design and default have been utilized. Regardless, the digital WWP may introduce privacy concerns and trust issues in the employees of their customer organizations, due to the sensitivity of physical activity data. In order to minimize the privacy-related risks, the measurement process is designed to only handle the minimum amount of personal data and, for example, the group reports only contain averaged and anonymized information in which no individuals can be identified. Additionally, as the information provided in the group reports potentially affects managerial decisions, employees may experience privacy-related concerns, such as unequal treatment and invasive surveillance. After all, there are known tensions between the stakeholders of WWPs that are probably in effect in this context, too. The WWP was designed to induce a positive change for all the stakeholders involved but the concept has not been thoroughly tested in regard to privacy-related risks, yet. In order to create new knowledge on the perceptions of working professionals on this type of wearable technology use, as well as, to mitigate the potential privacy-related risks in the designs of eHealth services similar to the WWP, it is of relevance to study the perceived effectiveness of the digital WWP's privacy policy and its effects on trust and behavioral intention to participate in the program.

## 3.4 Selection of Data Analysis Method

As we translated the survey items derived from the literature into Finnish and slightly adjusted the focus of the questions from surveying the participants' overall perceptions about an online service into an informed evaluation of the presented privacy policy of a WWP, we may have impacted the nature of some of the items and constructs into what may not be consistent with prior research.

The adjustment was made so that the questions would fit better in the context of our study in which only the privacy policy statement of a digital WWP was under examination and not the service itself. The goal was to gain insights about the privacy policy statement specifically as opposed to how it manifests itself in the characteristic of an online service, which has been the setting in most of the previous studies. This will be taken into account in the selection of

the data analysis method so that it will be suitable for the nature of the data, which may not be commensurate to the data of previous research.

Some of the previous studies have used reflective measurement models in which the main research model constructs are latent variables (Liu et al., 2005;Wu et al., 2012). This is typical when behavioral concepts are measured (Benitez et al., 2020). Reflective measurement models assume a causal relationship between the indicators (items) and the constructs (Benitez et al., 2020).

In our preliminary data analyses, including parallel analysis, factor analysis and principal component analysis, the main constructs of interest in our research model were not consistently identified as factors or principal components. This may have to do with the combined nature of the sample, smaller sample size and/or the adjusted focus of the items discussed above. This ultimately means that considering our model reflective leaves the model underidentified.

It has been stated that "research resources devoted to estimating and testing an underidentified model may ultimately be wasted" (Rigdon, 1995, p. 359). However, for the purposes of this study, we will use a composite modeling approach in which the model constructs are considered as emergent variables, i.e. the indicators form the constructs completely. This way we will be able to carry out our study efforts using our intended research model and test out the most recent developments in composite modeling. We will be using the Confimatory Composite Analysis approach, which comprises 1) model specification, 2) model identification, 3) model estimation, and 4) model assessment (Henseler & Schuberth, 2020; Benitez et al., 2020).

In the past few years, variance-based Structural Equation Modeling (SEM) has been gaining attention in the research community (Benitez et al., 2020). In variance-based SEM, different types of measurement models can be used: composites, common factors, and causal–formative (Henseler, 2017). SEM Partial Least Squares Path Modeling (PLS-PM) can be used to estimate all types of measurement models (Benitez et al., 2020). There has also been critique towards various aspects of PLS-PM as a research method (e.g. Rönkkö et al., 2016; Guide & Ketokivi, 2015). However, some of the identified issues have already been addressed by recent research (e.g. Benitez et al., 2020; Henseler & Schuberth, 2020; Rigdon et al., 2017).

Henseler (2017) suggests that when investigating relationships between design constructs and behavioral constructs, analytical tools that can cope with the requirements of both are needed. Design constructs are artifacts that are designed by humans, e.g. marketing instruments. Behavioral constructs such as attributes and attitudes of consumers are often considered as latent variables (Henseler, 2017). It has also been suggested that, depending on which view on the philosophy of science is taken, composite constructs may be used as reasonable proxies for behavioral concepts (Rigdon et al., 2017).

Thus, for the purposes of this study, we take a realist perspective and use composite constructs as proxies to measure the behavioral concepts of our research model.

## 3.5 Summary

In this chapter the research methodology for the study was discussed. First, research model development was discussed. Second, scale development and the survey instrument were discussed. Third, data collection and the research setting were described. Finally, the selection of the data analysis method was discussed.

# 4 DATA ANALYSIS AND RESULTS

This chapter discusses the analysis of the data and presents the results. First, the preparing of the data for the analysis is discussed. Second, data analysis and the assessment of the composite and structural models are discussed. Third, our hypotheses are tested based on the results. Finally, the chapter is summarized.

## 4.1 Preparing the Data for Analysis

First, the received 103 cases were screened for missing data, unengaged responses and outliers (Gaskin, 2016). The data was also rescaled from -3 to 3 to 1 to 7 for clarity reasons. As the survey instrument required that all the items had to be answered, there were no missing data on rows or columns. An unengaged response is when the respondent is not really paying attention, which can manifest in data that e.g. contains repetitive values (Gaskin, 2016). An "attention trap" that measures the engagement of the respondent was planted as one of the items of the survey in which the question was reverse coded. First, the data was visually inspected. Then, the standard deviation of the items was checked in Excel to eliminate the cases of very low standard deviation (SD). SD is a measure of how widely the response values are dispersed from the average response value. For a minimum SD value 0.7 was used. Two cases were eliminated (SD 0.368 and SD 0.666) and the rest were accepted within the SD range of 0.795 to 1.977. As the all the responses were ordinal, there were no outliers among responses. The final size of the sample to be analyzed is 101, which is adequate for our purposes. A commonly agreed minimum sample size for getting any kind of meaningful result is 100, so we have reached the threshold.

Next, R and the Psych library were used to calculate basic descriptive statistics for the data. The following characteristics of the respondents are presented in TABLE 4: gender, age group, education level, employment sector and telecommuting habits.

TABLE 4 Characteristics of Respondents (n = 101)

| | Number | Percentage |
|---|---|---|
| **Gender** | | |
| Male | 42 | 41.58 |
| Female | 59 | 58.42 |
| Total | 101 | 100 |
| **Age Group** | | |
| 18-24 | 2 | 1.98 |
| 25-29 | 6 | 5.94 |
| 30-34 | 13 | 12.87 |
| 35-39 | 15 | 14.85 |
| 40-49 | 22 | 21.78 |
| 50-59 | 39 | 38.62 |
| 60-69 | 4 | 3.96 |
| 70+ | 0 | 0 |
| Total | 101 | 100 |
| **Education Level** | | |
| Basic education | 0 | 0 |
| Matriculation examination / Vocational qualification | 3 | 2.97 |
| Post-Secondary / Higher Vocational Level Diploma | 6 | 5.94 |
| Bachelor's degree | 26 | 25.74 |
| Master's degree | 55 | 54.46 |
| Doctoral degree / Licenciate | 11 | 10.89 |
| Total | 101 | 100 |
| **Employment Sector** | | |
| Public Sector | 47 | 46.53 |
| Private Sector | 51 | 50.5 |
| Third Sector | 3 | 2.97 |
| Total | 101 | 100 |
| **Telecommuter** | | |
| Yes | 89 | 88.12 |
| No | 12 | 11.88 |
| Total | 101 | 100 |
| **Sample Group** | | |
| Convenience Sample | 30 | 29.7 |
| Random Sample | 71 | 70.3 |
| Total | 101 | 100 |

Thus, the typical respondent in the sample is a 50 to 59-year-old woman who has a master's degree, works in the private sector and telecommutes regularly.

The following descriptive statistics were calculated for the Likert scale items: mean, SD, median, trimmed mean, median absolute deviation, min, max, range, skewness, kurtosis and standard error. According to Brown (2006), acceptable values of skewness are between −3 and +3, and kurtosis is appropriate in a range of −10 to +10 in SEM analyzes. The descriptive statistics are presented in TABLE 5. All items were within the acceptable range of skewness and kurtosis.

TABLE 5 Descriptive Statistics of the Items (n = 101)

| | Mean | SD | Median | Trimmed | MAD | Min | Max | Range | Skew | Kurtosis | SE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **pepp1** | 6.26 | 0.77 | 6 | 6.36 | 1.48 | 4 | 7 | 3 | -0.86 | 0.34 | 0.08 |
| **pepp2** | 6.27 | 0.79 | 6 | 6.38 | 1.48 | 4 | 7 | 3 | -0.99 | 0.68 | 0.08 |
| **pepp3** | 6.25 | 0.84 | 6 | 6.38 | 1.48 | 4 | 7 | 3 | -1.08 | 0.69 | 0.08 |
| **security1** | 6.04 | 1.10 | 6 | 6.22 | 1.48 | 2 | 7 | 5 | -1.40 | 2.17 | 0.11 |
| **security2** | 6.12 | 1.05 | 6 | 6.30 | 1.48 | 3 | 7 | 4 | -1.10 | 0.37 | 0.10 |
| **security3** | 5.63 | 1.33 | 6 | 5.81 | 1.48 | 1 | 7 | 6 | -1.28 | 1.85 | 0.13 |
| **trust1** | 6.43 | 0.71 | 7 | 6.54 | 0.00 | 4 | 7 | 3 | -1.14 | 1.06 | 0.07 |
| **trust2** | 6.42 | 0.90 | 7 | 6.60 | 0.00 | 2 | 7 | 5 | -2.05 | 5.37 | 0.09 |
| **trust3** | 6.41 | 0.78 | 7 | 6.53 | 0.00 | 3 | 7 | 4 | -1.72 | 3.92 | 0.08 |
| **bi1** | 6.26 | 0.97 | 7 | 6.42 | 0.00 | 4 | 7 | 3 | -1.05 | -0.08 | 0.10 |
| **bi2** | 6.47 | 0.83 | 7 | 6.64 | 0.00 | 4 | 7 | 3 | -1.54 | 1.63 | 0.08 |
| **bi3** | 5.50 | 1.44 | 6 | 5.65 | 1.48 | 1 | 7 | 6 | -0.88 | 0.40 | 0.14 |

## 4.2 Data Analysis

For the purposes of this study, we consider our research model a composite model. We use the Confimatory Composite Analysis (CCA) process and a composite modeling tool called Adanco 2.2 (Henseler & Dijkstra, 2020) to specify the composite model and the structural model and to estimate the models using PLS-PM. A composite model comprises the constructs and their indicators. A structural model also includes the relationships between the constructs that are to be analyzed.

Our applied CCA process is structured as follows: first, we create a new project in Adanco and import our data to the workspace. Second, we model the composite constructs and their indicators. Mode B (regression weights) is used as the weighting scheme of the indicators and dominant indicators are selected. Third, we specify the relationships between the constructs. Fourth, we run a complete PLS-PM analysis for the model. We use bootstrapping with 4999 runs and assess overall model fit. Before estimation, we ensure that the estimation is technically valid, i.e. the estimation is admissible and no Heywood case has occurred (Benitez et al., 2020). Finally, we assess the models.

We then apply the process to specify, identify and estimate the models. In the following sections, the assessment of the estimated models is presented.

### 4.2.1 Assessment of the Composite Model

For the systematic assessment of the reliability and validity of composite models, Benitez et al. (2020) suggest the following steps: testing the adequacy of the composite models, evaluating content validity, multicollinearity, weights, and loadings. In TABLE 6, the steps are given descriptions, assessment criterions, decision criterions as well as interpretations.

TABLE 6 Steps to Assess Composite Models (Benitez et al., 2020, p. 10)

| Step | Description | Assessment Criterion | Decision Criterion | Interpretation |
|---|---|---|---|---|
| **Testing the adequacy of composite models** | Evaluate the overall fit of the model with a saturated structural model by investigating discrepancy between empirical and model-implied indicator variance–covariance matrix | SRMR | SRMR < 0.080<br>SRMR < $HI_{95}$ | A SRMR value smaller than 0.080 indicates an acceptable model fit; however, these thresholds are preliminary and need to be investigated in more detail |
| | | $d_{ULS}$<br>$d_G$ | $d_{ULS} < HI_{95}$<br>$d_G < HI_{95}$ | The null hypothesis that the population indicator variance–covariance matrix equals the model-implied counterpart is not rejected. Hence, empirical evidence for the model is given when the value of the discrepancy measure is below the 95% quantile of its corresponding reference distribution |
| **Evaluating content validity** | How the corresponding theoretical concepts have been operationalized (measured or built) in prior research | Flexibility in the case of artifacts represented by an emergent variable | | |
| **Multicollinearity** | Evaluating how the standard errors of the weight estimates are affected by the correlations of the indicators | Variance Inflation Factor (VIF) | VIF < 5 | If the estimates suffer from multicollinearity, weights obtained by Mode A or predetermined weights can be used |
| **Weights** | Evaluating relative contribution of an indicator to its construct | Weights' value and significance | Significant at 5% significance level | Each indicator contributes significantly to the emergent variable |
| **Loadings** | Evaluating absolute contribution of an indicator to its construct | Loading significance | Significant at 5% significance level | Each indicator contributes to the emergent variable in a statistically significant way |

As the first step, the overall fit of the saturated model is evaluated. A saturated model is a variant of the estimated model in which all the constructs are allowed to be freely correlated (Benitez et al., 2020). The overall model fit of the saturated model can be used to assess the validity of the measurement and the composite models and to rule out misspecifications in the composite models. Thus, empirical support can be obtained for the composite constructs, i.e. do the indicators form an emergent variable (Benitez et al., 2020). According to our evaluation, the SRMR value was under .08 and all of the values were smaller than $HI_{95}$. Thus, evaluation for the overall fit of the saturated model was fully supported. The results of the evaluation are presented in TABLE 7.

TABLE 7 Overall Saturated Model Fit Evaluation

| Discrepancy | Value | $HI_{95}$ | Conclusion |
|---|---|---|---|
| **SRMR** | 0.0455 | 0.0520 | Supported |
| $\mathbf{d_{ULS}}$ | 0.1612 | 0.2112 | Supported |
| $\mathbf{d_G}$ | 0.2041 | 0.2147 | Supported |

As the second step, content validity is assessed. All the model constructs and most of their respective items were adapted from prior research, in which they were used to measure latent variables. As we have localized them, adjusted their focus, and adapted them in our composite model to measure emergent variables, we cannot make explicit claims on the content validity of the composite constructs nor their indicators, based on prior research. However, based on the overall model fit, the content of the emergent variables seems to be coherent and valid.

As the third step, multicollinearity is assessed. The indicator multicollinearity matrix is presented in TABLE 8. There is one indicator that suffers from multicollinearity: pepp2, which slightly exceeds the VIF value of 5, which makes it a potential candidate for elimination.

TABLE 8 Indicator Multicollinearity

| Indicator | PEPP | Security | BI | Trust |
|---|---|---|---|---|
| **pepp1** | 4.0291 | | | |
| **pepp2** | 5.2440 | | | |
| **pepp3** | 3.4937 | | | |
| **security1** | | 2.4768 | | |
| **security2** | | 1.4906 | | |
| **security3** | | 1.9459 | | |
| **trust1** | | | | 3.4517 |
| **trust2** | | | | 2.1923 |
| **trust3** | | | | 3.4130 |
| **bi1** | | | 2.0025 | |
| **bi2** | | | 1.5679 | |
| **bi3** | | | 1.5664 | |

As the fourth and fifth steps, indicator weights and loadings are assessed. In TABLE 9 the t-values for the indicator weights are presented. Furthermore, in TABLE 10 the t-values for indicator loadings are presented. We set the alpha level at .05 as the cutoff point for statistical significance, which translates to the absolute value of 1.96 in t-values. Before we eliminate indicators we have to keep in mind content validity to avoid changing the semantic nature of the composite constructs.

In TABLE 9 the statistically insignificant indicators based on the t-values of the weights are denotated in red color. All t-values of indicator loadings were

statistically significant. As a working rule, we require at least two indicators per construct. Eliminated indicators are denotated with strikethroughs.

TABLE 9 Indicator Weights T-Values

| Indicator | PEPP | Security | BI | Trust |
|---|---|---|---|---|
| **pepp1** | 2.2291 | | | |
| ~~pepp2~~ | 1.8521 | | | |
| **pepp3** | 2.3364 | | | |
| **security1** | | 4.2312 | | |
| **security2** | | 2.7669 | | |
| ~~security3~~ | | 1.8981 | | |
| **trust1** | | | | 2.9593 |
| ~~trust2~~ | | | | 1.7877 |
| **trust3** | | | | 2.2479 |
| ~~bi1~~ | | | -0.7146 | |
| **bi2** | | | 8.6944 | |
| **bi3** | | | 3.0688 | |

In PEPP, the indicator pepp2 is eliminated at this stage. In Security, the indicator security3 is near of statistical significance, but it is eliminated to promote overall model fit. In BI, the indicator bi1 is eliminated. In Trust, the indicator trust2 is eliminated.

TABLE 10 Indicator Loadings T-Values

| Indicator | PEPP | Security | BI | Trust |
|---|---|---|---|---|
| **pepp1** | 3.9154 | | | |
| **pepp2** | 3.9415 | | | |
| **pepp3** | 4.1301 | | | |
| **security1** | | 26.6251 | | |
| **security2** | | 9.8376 | | |
| **security3** | | 10.1932 | | |
| **trust1** | | | | 13.7740 |
| **trust2** | | | | 10.6768 |
| **trust3** | | | | 12.5626 |
| **bi1** | | | 4.4627 | |
| **bi2** | | | 27.6683 | |
| **bi3** | | | 7.7172 | |

As the assessment of the composite model is finished, next we will assess the structural model in which the relationships between the constructs are examined.

### 4.2.2 Assessment of the Structural Model

For the systematic assessment of the reliability and validity of structural models, Benitez et al. (2020) suggest the following steps: testing the overall fit of the estimated model, consider path coefficient estimates and their significance levels, consider effect sizes ($f^2$), and evaluate $R^2$. In TABLE 11, the steps are given descriptions, assessment criterions, decision criterions as well as interpretations.

TABLE 11 Steps to Assess Structural Models (Benitez et al., 2020, p. 12)

| Step | Description | Assessment Criterion | Decision Criterion | Interpretation |
|---|---|---|---|---|
| **Overall fit of estimated model** | Evaluating overall fit of the estimated model by evaluating discrepancy between the empirical indicator variance–covariance matrix and its model-implied counterpart | SRMR | SRMR < 0.080<br>SRMR < $HI_{95}$ | Value of discrepancy measure below the 95% quantile of the corresponding reference distribution provides empirical evidence for the postulated model. In other words, it is possible that the empirical data stem from a world that functions as theorized by the model |
| | | $d_{ULS}$ | $d_{ULS} < HI_{95}$ | |
| | | $d_G$ | $d_G < HI_{95}$ | |
| **Consider path coefficient estimates and their significance levels** | Standardized regression coefficients are interpreted as change in standard deviations of the dependent variable if an independent variable is increased by one standard deviation while all other independent variables in the equation remain constant | Path coefficient estimates and their significance level | Significant at 5% significance level, i.e., p-value < 5% | Effect of independent variables on dependent variables is statistically significant |
| **Consider effect sizes ($f^2$)** | Measure of the magnitude of an effect that is independent of sample size. Give an indication about the practical relevance of an effect | $f^2$ value | $f^2 < 0.020$: no substantial effect $0.020 \leq f^2 < 0.150$: weak effect size $0.150 \leq f^2 < 0.350$: medium effect size $f^2 \geq 0.350$: large effect size | Degree of strength of an effect |
| **Evaluate $R^2$** | Explained variance of an dependent construct | $R^2$ | When the phenomena are already quite well understood, one would expect a high $R^2$. When the phenomena are not yet well understood, a lower $R^2$ is acceptable | Degree of variance explained for phenomenon under investigation |

As the first step, the overall fit of the estimated model is evaluated. The overall fit of the estimated model is used as a measure of the approximate fit to obtain empirical evidence for the proposed model (Benitez et al., 2020). According to our evaluation, the SRMR value was under .08 and all of the values were smaller than $HI_{95}$. Thus, the evaluation of the overall fit of the estimated model was fully supported. The results of the evaluation are presented in TABLE 12.

TABLE 12 Overall Estimated Model Fit Evaluation

| Discrepancy | Value | $HI_{95}$ | Conclusion |
|---|---|---|---|
| **SRMR** | 0.0617 | 0.0653 | Supported |
| $\mathbf{d_{ULS}}$ | 0.1369 | 0.1536 | Supported |
| $\mathbf{d_G}$ | 0.0845 | 0.0972 | Supported |

As the second step, path coefficients and their significance levels are evaluated. Path coefficients can be interpreted as "the change in the dependent construct measured by standard deviations, if an independent construct is increased by one standard deviation while keeping all other explanatory constructs constant" (Benitez et al., 2020, p. 11). For example, according to the estimation, as Security increases by one standard deviation PEPP will increase by 0.7359 standard deviations, if other variables are kept constant. The path coefficient estimates are presented in TABLE 13 (indirect effects in brackets). All path coefficients were statistically significant as their p-values were smaller than .001.

TABLE 13 Path Coefficient Estimates (***p < .001)

| Independent Variable | PEPP | Behavioral Intention | Trust |
|---|---|---|---|
| **PEPP** | | (0.5922***) | 0.7633*** |
| **Trust** | | 0.7758*** | |
| **Security** | 0.7359*** | (0.4358***) | (0.5617***) |

As the third step, the effects sizes, i.e. Cohen's $f^2$ values are evaluated. The effect size can be described as the measure of the magnitude of an effect independent of sample size (Benitez et al., 2020). Our values are presented in TABLE 14. The values seem to be larger than usual as values larger than .350 are already considered as indicators of large effect. However, we double checked the effect sizes using R with the cSEM library with matching results. For the purposes of this study, we consider the effect sizes to be large in the scale of Benitez et al. (2020).

TABLE 14 Effect sizes ($f^2$)

| Independent Variable | PEPP | Behavioral Intention | Trust |
|---|---|---|---|
| **PEPP** | | | 1.3959 |
| **Trust** | | 1.5117 | |
| **Security** | 1.1812 | | |

As the fourth step, the $R^2$ values of the dependent constructs are evaluated. An $R^2$ value indicates the share of variance explained in a dependent construct (Benitez et al., 2020). Our values are presented in TABLE 15. Thus, 1) Security explains 54.15% of the variance in PEPP, 2) PEPP explains 58.26% of the variance in Trust, and 3) Trust explains 60.19% of the variance in Behavioral Intention.

TABLE 15 $R^2$ values

| Construct | $R^2$ value |
|---|---|
| **PEPP** | 0.5415 |
| **Behavioral Intention** | 0.6019 |
| **Trust** | 0.5826 |

FIGURE 8 illustrates the estimated model. In the figure, the composite constructs are depicted as hexagons, indicators as rectangles and paths between constructs as arrow-ended lines. Security is an independent construct. Perceived Effectiveness of Privacy Policy (PEPP), Privacy Concern, Trust, and Behavioral Intention are dependent constructs. Indicator weights are presented above the lines that connect them to their composite constructs. $R^2$ values for the dependent constructs are presented inside the construct hexagons. Estimated path coefficients are presented on top of the path lines. Indirect effects are presented as dashed arrow-ended lines. Statistically significant path coefficients are postfixed by ampersands as follows: *** $p < .001$.

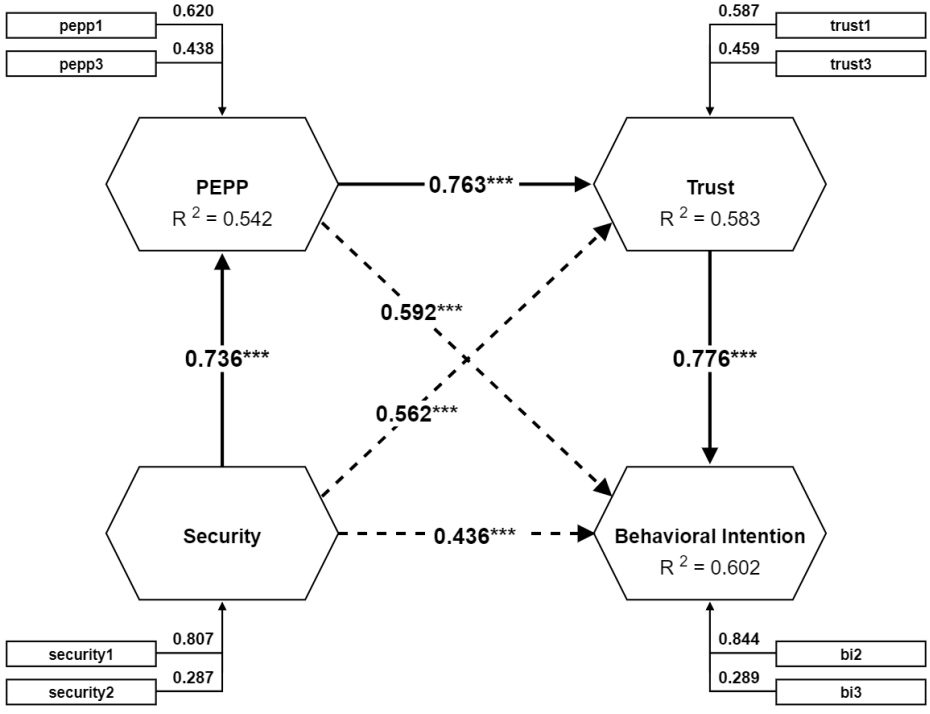


FIGURE 8 The Estimated Model

Finally, we analyze the effects of the control variables on the composite constructs. We control Security, PEPP and Trust with age, gender and education. Significant effects are found between gender and Trust. BI is controlled with employment and telecommuting. No significant effects were found. Security, PEPP, Trust and BI are controlled with sample group. Significant effects were found between sample group and PEPP as well as sample group and BI. The identified significant effects are presented in TABLE 16.

TABLE 16 Significant Path Coefficient Estimates of Control Variables (*p<.05; **p<.01)

| Control Variable | PEPP | Behavioral Intention | Trust |
|---|---|---|---|
| **Gender** | | | -0.1702* |
| **Sample Group** | -0.2075** | -0.2025** | |

As the assessment of the structural model is completed, we have finished our data analysis. We have utilized the recent CCA approach and reported the metrics that the recent guidelines for impactful PLS-PM research suggest (Benitez et al., 2020).

## 4.3 Testing of the Hypotheses

In this section our hypotheses are tested, based on the results of the analysis. We found empirical support for H1, H2, H3, H4, H5 and H6. Thus, empirical support was found that could be used to justify efforts to increase PEPP to potentially improve participation rates in digital WWPs. The hypotheses and conclusions are presented in TABLE 17.

TABLE 17 Hypotheses and Conclusions

| ID | Hypothesis | Conclusion |
|---|---|---|
| **H1** | Security positively affects PEPP | Supported |
| **H2** | PEPP positively affects Trust | Supported |
| **H3** | Trust positively affects Behavioral Intention | Supported |
| **H4** | Security has a positive indirect effect on Trust though PEPP | Supported |
| **H5** | Security has a positive indirect effect on Behavioral Intention through PEPP and Trust | Supported |
| **H6** | PEPP has a positive indirect effect on Behavioral Intention through Trust | Supported |

## 4.4 Summary

This chapter discussed the analysis of the data and presented the results. First, the preparing of the data for the analysis was discussed. Second, data analysis

and the assessment of the composite and structural models were discussed. Finally, our hypotheses were tested based on the results.

# 5 Discussion and Conclusions

This chapter presents the discussion, conclusions, and the implications of the study. First, the summary of the thesis is presented. Second, the implications of the study to research and practice are discussed. Third, the limitations of the study are discussed. Finally, directions for future research are outlined.

## 5.1 Discussion

The Perceived Effectiveness of Privacy Policy (PEPP) is a topical issue in information privacy research. It has been correlated before with the five dimensions of fair information practice principles: Notice, Choice, Access, Security, and Enforcement. Security has been found to be the most important concern for online users. In the context of Theory of Reasoned Action and the Privacy–Trust–Behavioral Intention model, PEPP has been shown before to have a positive effect on Trust, that, in turn has been shown to positively affect the Behavioral Intention to share information on online platforms.

In this study, we developed a research model based on prior research to test the correlations between Security, Perceived Effectiveness of Privacy Policy (PEPP), Trust and Behavioral Intention to participate in a digital Workplace Wellness Program (WWP). As control variables, age, gender, education, employment sector, telecommuting and sample group were utilized. By testing the correlations, we aimed to produce empirical evidence on whether efforts to increase PEPP are justified to potentially improve participation rates in digital WWPs. This would have economic implications for employers and service provider of digital WWPs as well as health implications for working professionals.

An online survey instrument was developed and used to collect data from the population of Finnish white-collar telecommuters, working in the fields of HR, business development and IT. The data was collected in two phases. First, a convenience sample was collected from pilot project, in which a novel digital WWP was implemented in a public sector organization. Second, a random

sample of the same population was collected via social media networks. The respondents were instructed to study the Privacy Policy Statement (PPS) of a novel digital WWP and to respond to survey according to their perceptions of the PPS. At the end of data collection the samples were combined, yielding a total of 103 responses from working professionals.

For the purposes of this study, our research model was considered as a composite model. The Partial Least Squares Path Modeling (PLS-PM) method was used to analyze the data. This involved applying a recent Confirmatory Composite Analysis process to specify, identify, estimate and assess composite and structural models that depict our research model. Recent guidelines that address some of the methodological issues previously identified with PLS-PM were applied in the process. The guidelines encourage researchers to assess the overall fit of the models in future PLS-PM research as such capability was introduced only recently. This was largely missing in prior research, which means researchers were not able to obtain any signal of an incorrectly omitted important effect in their models. Thus, we reported the overall fit of both the composite and structural models in this study. The overall fit of the models was supported. Thus, our model fit the data that was collected.

In Chapter 4, we assessed the models for the reliability and validity measures that are available to composite models at this time. After the estimation of the composite model, one unreliable indicator was eliminated from each of the model constructs to promote the overall fit of the model. In the assessment of the reliability and validity measures, the composite model was deemed to be of sufficient quality. The estimation of the structural model indicates that there are statistically significant positive correlations between the constructs of Security and PEPP, PEPP and Trust, and Trust and Behavioral Intention to Participate in a digital WWP. We identified also statistically significant indirect effects between Security and Trust through PEPP, Security and Behavioral Intention through PEPP and Trust as well as PEPP and Behavioral Intention to Participate in a digital WWP through Trust. Furthermore, we found that some of our control variables influenced some of our constructs. Significant negative correlations were found between gender and Trust, sample group and PEPP and sample group and Behavioral Intention. Based on the assessment of the reliability and validity measures, the structural model was deemed to be of sufficient quality.

## 5.2 Conclusions

Our findings provide empirical evidence for the following conclusions in the context of digital WWPs: 1) PEPP can be increased be improving the Security dimension of a PPS, 2) Trust can be increased by improving PEPP and/or Security, and 3) Behavioral Intention to participate can be increased by improving Trust and/or PEPP and/or Security. The findings are in line with Theory of

Reasoned Action and the Privacy–Trust–Behavioral Intention model as well as the previous findings of Wu et al. (2012) and Chang et al. (2018).

We also found that males perceived Trust lower than females. Riquelme & Román (2014) provide one explanation for this: the influence of perceived online security and privacy is stronger for males in relation to online trust formation. This is plausible in our study since we found that gender had a similar near significant correlation to Behavioral Intention.

Furthermore, we found that the group of respondents acquired by random sampling perceived PEPP and Behavioral Intention lower than the convenience sample. The difference in the correlations may be due to fact that the random sample probably represents the population better. The convenience sample has 83% of females, 83% are over 40 years of age and 100% work in the public sector, whereas the random sample has 48% of females, 56% are over 40 years old and 72% work in the private sector. In addition, the respondents of the convenience sample had the digital WWP readily available to them via the pilot project whereas the respondents of the random sample did not. This may have affected Behavioral Intention positively in the convenience sample.

Finally, based on our results, a concluding remark can be drawn that efforts to increase PEPP may be justified to increase Trust and Behavioral Intention to participate in a digital WWP among working professionals.

## 5.3 Implications of the Study

The implications of this study for research are described in the following. Our findings are consistent with prior research and can be considered as further evidence for prior results. We used a recent composite modeling approach to analyze our research model. This approach may not have been used before to study these constructs and their interrelations. As the composite model was identified and the overall fit of the model was supported, our study provides support on the viability of the composite modeling approach to study such behavioral concepts. PLS-PM is still a developing approach to structural equation modeling and this study contributes to its recent applications. We applied the recent CCA approach and reported the metrics that the recent guidelines for impactful PLS-PM research suggest, which promotes the adaptation of the improved reporting standards. This study also contributes to Theory of Reasoned Action and the Privacy–Trust–Behavioral Intention model research. This study may also be the first one to apply these theories to study the behavioral intention to participate in a digital WWP. Furthermore, the population of the study was working professionals in the fields of HR, business development and IT, whereas mostly college students were previously used in the testing of the research models, which may provide some further evidence of the validity and generalizability of prior results. The online survey instrument that was developed in the study could also be useful in future studies with similar objectives.

The implications of this study for practice are two-fold: 1) it provides empirical evidence for companies in that investments in improving PEPP are potentially beneficial for increasing trust and behavioral intention to participate in working professionals (at least in digital WWPs), and 2) it provides guidance on how to measure the effect of the investments. Companies can develop surveys using the scales presented in this thesis and measure the variables to analyze and optimize specific characteristics of their privacy policies based on the results. This is also in line with prior research in the context of ecommerce that suggests that accessible and effectively communicated privacy policies may gain companies more business (Tsai et al., 2011). Potential increased participation in digital WWPs could also increase the profitss of employers and the health outcomes of their employees. Product developers could also take the concept and turn it into a self-service SaaS product that would generate online surveys for uploaded privacy policies and automate the analysis of the collected data. The SaaS product could also make personalized recommendations on which specific aspects of the privacy policy should be developed to optimize PEPP.

## 5.4 Limitations

There are several limitations to our study. Time available to plan and conduct the study was the primary limitation as decisions about the research design of the study were required to be made rather quickly to accommodate to the time constraints imposed by the research setting. Further measures would have been taken to tackle the potential effects of Common Method Bias (Guide & Ketokivi, 2015; Podsakoff et al., 2012) in the design of the online survey instrument, had there been more time available. As we translated the survey items derived from the literature into Finnish and slightly adjusted the focus of the questions from surveying the participants' overall perceptions about an online service into an informed evaluation of the presented privacy policy of a WWP, we may have impacted the nature of some of the items and constructs into what may not be consistent with prior research. This may have impacted the data and the consistency of the items to reflect their intended behavioral concepts so that our research model became underidentified as a reflective measurement model. Furthermore, combining a convenience sample and a random sample introduced some bias in the results, although it was controlled by the sample group control variable.

For the purposes of this study, we took a realist perspective on the philosophy of science and used composite models as proxies for behavioral concepts (Rigdon et al., 2017). Furthermore, we ended up eliminating one of the three indicators that compose the final estimated constructs, which may somewhat impact the representativeness of the constructs in relation to the original behavioral concepts. Furthermore, the size of the population of Finnish white-collar telecommuters within the fields of HR, business development and IT is challenging to determine at the moment as the COVID-19 pandemic has increased

telecommuting drastically. To calculate the minimum sample size required, a statistical power analysis such as Cohen's power tables would be required (Benitez et al., 2020). Even though we collected over 100 responses from working professionals, a larger sample size will be needed to confirm the generalizability of the results in future research.

## 5.5 Future Research

The research model of this study is derived from prior research, but its composition is not identical to any of the past studies. Thus, the research model should be re-tested in future research. The research model could also be extended with the other FIPS Notice, Choice, Access and Enforcement as well as Privacy Concern to test related phenomena in the context digital WWPs. However, commensuration to prior research should be ensured. Similarly to the study of Muller et al. (2018), it would be interesting to compare the results of both reflective and composite model variants of the research model with the data and analyze whether there are significant differences in validity and reliability to be identified. It would also be beneficial for the generalizability of the results to collect data from a survey in which various privacy policies or their perceived manifestations in services/programs are evaluated. This could be carried out e.g. as a controlled lab experiment and/or in real-life settings as an industry collaboration. It would also be interesting to apply Theory of Planned Behavior to the research model which would introduce the concept of perceived behavioral control into the model.

## REFERENCES


Ajunwa, I., Crawford, K. & Schultz, J. (2017). Limitless Worker Surveillance. *California Law Review, 105(3),* 735-776.

Allen, M. W., Coopman, S. J., Hart, J. L. & Walker, K. L. (2007). Workplace Surveillance and Managing Privacy Boundaries. *Management Communication Quarterly, 21(2),* 172-200.

Altman, I. (1974). Privacy: a conceptual analysis. In D. H. Carson (Eds.), *Man-Environment Interactions: Evaluations and Applications: Part 2* (p. 3-28). Washington DC: Environmental Design Research Association.

Baicker, K., Cutler, D. & Song, Z. (2010). Workplace Wellness Programs Can Generate Savings. *Health affairs, 29(2),* 304-311.

Bansal, G., Zahedi, F. â. & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems, 24(6),* 624-644.

Bartel Sheehan, K. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13(4),* 24-38.

Bélanger, F. & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35(4),* 1017-1042.

Benitez, J., Henseler, J., Castillo, A. & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management, 57(2),* 103168.

Bottles, K. (2015). Workplace wellness programs right or wrong? *Physician Leadership Journal, 2(3),* 34-37.

Brown, T. A. (2006). *Confirmatory factor analysis for applied research.* New York, NY, US: The Guilford Press.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F. & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, 35(3),* 445-459.

Charalampous, M., Grant, C. A., Tramontano, C. & Michailidis, E. (2019). Systematically reviewing remote e-workers' well-being at work: a multidimensional approach. *, 28(1),* 51-73.

De Mooy, M. & Yuen, S. (2016). Towards Privacy-Aware Research and Development in Wearable Health. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (p. 3658-3667). Hilton Waikoloa Village, Hawaii: IEEE Computer Society.

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

Earp, J. B., Anton, A. I., Aiman-Smith, L. & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management, 52(2),* 227-237.

Fishbein, M. (1967). A behavior theory approach to the relations between beliefs about an object and the attitude toward the object. In M. Fishbein (Eds.), *Readings in attitude theory and measurement* (p. 389-400). New York: New York: John Wiley & Sons.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Frampton, B. D. & Child, J. T. (2013). Friend or Not to Friend: Coworker Facebook Friend Requests As an Application of Communication Privacy Management Theory. *Computers in Human Behavior, 29(6),* 2257-2264.

Gaskin, J. (2016). Data Screening, Gaskination's StatWiki. Accessed 2020-11-08 available at http://statwiki.kolobkreations.com

Giddens, L., Leidner, D. & Gonzalez, E. (2017). The Role of Fitbits in Corporate Wellness Programs: Does Step Count Matter? In *Proceedings of the 50th Hawaii International Conference on System Sciences* (p. 3627-3635). Hilton Waikoloa Village, Hawaii: IEEE Computer Society.

Goetzel, R. Z., Henke, R. M., Tabrizi, M., Pelletier, K. R., Loeppke, R., Ballard, D. W., Grossmeier, J., Anderson, D. R., Yach, D., Kelly, R. K., McCalister, T., Serxner, S., Selecky, C., Shallenberger, L. G., Fries, J. F., Baase, C., Isaac, F., Crighton, K. A., Wald, P., Exum, E., Shurney, D. & Metz, R. D. (2014). Do Workplace Health Promotion (Wellness) Programs Work? *Journal of Occupational and Environmental Medicine, 56(9),* 927-934.

Gorm, N. & Shklovski, I. (2016). Sharing Steps in the Workplace: Changing Privacy Concerns Over Time. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (p. 4315-4319). New York, NY: ACM.

Groves, R. M., Kalton, G., Rao, J. N. K., Schwartz, N. & Skinner, C. (2004). *Survey Methodology.* Hoboken, NJ: John Wiley & Sons Inc.

Guide, V. D. R. & Ketokivi, M. (2015). Notes from the Editors: Redefining some methodological criteria for the journal. *Journal of Operations Management, 37(1),* v-viii.

Henseler, J. (2017). Bridging Design and Behavioral Research With Variance-Based Structural Equation Modeling. *Journal of Advertising, 46(1),* 178-192.

Henseler, J. & Dijkstra, T.,K. (2020). ADANCO 2.2. Kleve, Germany: Composite Modeling GmbH & Co. KG.

Henseler, J. & Schuberth, F. (2020). Using confirmatory composite analysis to assess emergent variables in business research. *Journal of Business Research, 120(11),* 147-156.

Koster, A., Caserotti, P., Patel, K. V., Matthews, C. E., Berrigan, D., Van Domelen, D.,R., Brychta, R. J., Chen, K. Y. & Harris, T. B. (2012). Association of sedentary time with mortality independent of moderate to vigorous physical activity. *PloS one, 7(6),* e37696-e37696.

Li, Y. (2012). Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. *Decision Support Systems, 54(1),* 471-481.

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

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

Lupton, D. (2016). *The quantified self: A sociology of self-tracking cultures.* Cambridge, UK: Polity Press.

Lupton, D. & Michael, M. (2017). 'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance. *Surveillance & Society, 15(2),* 254-268.

Lupton, D. (2016). The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society, 45(1),* 101-122.

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

Mattila, E., Orsama, A., Ahtinen, A., Hopsu, L., Leino, T. & Korhonen, I. (2013). Personal health technologies in employee health promotion: usage activity, usefulness, and health-related outcomes in a 1-year randomized controlled trial. *JMIR mHealth and uHealth, 1(2),* 1-18.

Müller Tobias, Florian, S. & Henseler Jörg (2018). PLS path modeling – a confirmatory approach to study tourism technology and tourist behavior. *Journal of Hospitality and Tourism Technology, 9(3),* 249-266.

Pan, Y. & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82(4),* 331-338.

Perez-Calhoon, M. (2017). *A Mixed-Methods Study: Self-Efficacy and Barriers to Participation in Workplace Wellness Programs.* Doctor of Education (EdD). Brandman University.

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

Podsakoff, P. M., MacKenzie, S. B. & Podsakoff, N. P. (2012). Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual Review of Psychology, 63(1),* 539-569.

Rigdon, E. E. (1995). A Necessary and Sufficient Identification Rule for Structural Models Estimated in Practice. *Multivariate Behavioral Research, 30(3),* 359-383.

Rigdon, E. E., Sarstedt, M. & Ringle, C. M. (2017). On Comparing Results from CB-SEM and PLS-SEM: Five Perspectives and Five Recommendations. *Marketing ZFP, 39(3),* 4-16.

Riquelme, I.,P. & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets, 24(2),* 135-149.

Rönkkö, M., McIntosh, C. N., Antonakis, J. & Edwards, J. R. (2016). Partial least squares path modeling: Time for some serious second thoughts. *Journal of Operations Management, 47-48(11),* 9-27.

Schwaig, K. S., Segars, A. H., Grover, V. & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50(1),* 1-12.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35(4),* 989-1015.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154(3),* 477-560.

Staats, H. (2004). Pro-environmental Attitudes and Behavioral Change. In C. D. Spielberger (Eds.), *Encyclopedia of Applied Psychology* (p. 127-135). New York: Elsevier.

Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research, 22(2),* 254-268.

Tu, H. T. & Mayrell, R. C. (2010). *Employer wellness initiatives grow, but effectiveness varies widely.* Washington, DC: National Institute for Health Care Reform.

Westin, A. F. (1967). *Privacy and Freedom.* New York, NY: Atheneum.

Willis Towers Watson (2016). 21st Annual Willis Towers Watson Best Practices in Health Care Employer Survey.

Wu, K., Huang, S. Y., Yen, D. C. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28(3),* 889-897.

Wu, Y., Ding, Y., Tanaka, Y. & Zhang, W. (2014). Risk Factors Contributing to Type 2 Diabetes and Recent Advances in the Treatment and Prevention. *Int J Med Sci, 11( ),* 1185-1200.

Xu, H., Dinev, T., Smith, H. & Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. In *Proceedings of the International Conference on Information Systems* (p. 1-16). Paris, France.

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

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

Zimmer, M., Kumar, P., Vitak, J., Liao, Y. & Kritikos, K. C. (2018). "There's nothing really they can do with this information": unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society, 23(7),* 1020-1037.

Zwick, D. & Dholakia, N. (2004). Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. *Journal of Macromarketing, 24(1),* 31-43.