EXTENDING THE EXTENDED UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT2): THE MODERATION ROLE OF INFORMATION PRIVACY CONCERNS

by

Hussein Ghnaimeh

A dissertation submitted to the faculty of The University of North Carolina Charlotte in partial fulfillment of the requirements for the degree of Doctor of Business Administration

Charlotte

2024

Approved by:

_____
Dr. Franz Kellermanns

_____
Dr. Laura Stanley

_____
Dr. Chandra Subramaniam

_____
Dr. Gregory Martin

©2024
Hussein Ghnaimeh
ALL RIGHTS RESERVED

ABSTRACT

HUSSEIN GHNAIMEH. Extending the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2): The Moderation Role of Information Privacy Concerns (Under the direction of DR. FRANZ KELLERMANNS)

This dissertation enhances the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) by integrating information privacy concerns and examining their influence on adopting web-based healthcare portals. Through a survey of 298 U.S. residents using healthcare technologies, the study investigates the interplay between UTAUT2 predictors—Performance Expectancy, Effort Expectancy, Facilitating Conditions, Habit, Social Influence, and Hedonic Motivation—and the intention to use these technologies while assessing how privacy concerns modulate these relationships. Regression analysis highlights the positive impact of Performance Expectancy, Effort Expectancy, and Habit on adoption intent, with privacy concerns significantly moderating the relationship between Effort Expectancy and usage intention. The research enriches the UTAUT2 model by showcasing the pivotal role of privacy concerns, thus advancing theoretical understanding and enhancing model predictability in the context of healthcare technology. Practically, it offers insights for practitioners and policymakers on addressing privacy concerns to improve technology adoption. This synthesis of privacy concerns within the technology acceptance framework paves the way for targeted strategies to increase the uptake of healthcare technologies, marking a significant contribution to both academic discourse and practical application.

Keywords: Health information privacy, Healthcare portals, Privacy Concerns, UTAUT2, moderation.

ACKNOWLEDGMENTS

I am immensely grateful to my dissertation chair, Dr. Franz Kellermanns, for his expert guidance and invaluable support throughout this process. His mentorship has been a cornerstone of my academic development. My gratitude extends to my committee members, Dr. Laura Stanley and Dr. Chandra Subramaniam, for their insightful feedback. Their contributions have greatly enhanced the quality of my work. My sincere thanks also goes to Dr. Gregory Martin, who acted as the graduate school representative on my committee; thank you for your time and support.

I extend my deepest gratitude to my wife, Nadine El Doueiry, whose unwavering support and boundless patience have been the bedrock of my perseverance throughout this rigorous academic journey. Nadine, your strength and encouragement have been my guiding lights, and your belief in my capabilities has often surpassed my own. To my beloved daughters, Haya and Julia, your smiles and endless curiosity about the world rejuvenate my spirit. Every moment spent with you reminds me of why I embarked on this path. Your understanding and love during the times I was absorbed in my studies have made all the difference.

I also wish to thank Cohort Five for their camaraderie and mutual support, which have been a source of motivation and inspiration throughout the DBA journey. To everyone who has contributed to my journey, your support has been fundamental to my achievements. Thank you!

DEDICATION

This dissertation is solemnly dedicated to the memory of my father, who was the cornerstone of my academic aspirations and the most fervent believer in my pursuit of a doctoral degree. His lifelong dream was to see me achieve the title of Doctor, a vision that fueled my commitment and guided my steps through the demanding journey of higher education.

From the earliest days of my childhood, my father instilled in me the values of persistence, intellectual curiosity, and unwavering dedication. He was a beacon of wisdom and encouragement, often reminding me that education was not just a path to personal achievement but a means to contribute meaningfully to the world. His profound respect for academia and its potential to transform lives shaped my own perspective and aspirations.

Even as I stand at the culmination of this journey, his absence is profoundly felt. It is a poignant sorrow that he could not witness this milestone, having passed away just a few months before its fruition. Yet, I carry forward his legacy with each page I have written and each discovery I have made. This achievement, while marked by his absence, is imbued with his spirit and the lessons he imparted.

To my beloved father, thank you for dreaming big dreams for me, for pushing me towards them with love and conviction, and for inspiring me to fulfill not just your aspirations, but also the potential you so firmly believed I possessed. This doctoral degree is not only my achievement but is also a tribute to you, a testament to your profound impact on my life. May this work honor your memory and reflect the greatness you envisioned for me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

UTAUT	The extended Unified Theory of Acceptance and Use of Technology
WBHP	Web-based Healthcare Portal

CHAPTER 1: INTRODUCTION

In today's digital era, electronic services have become indispensable for governments' and businesses' survival and success (Bannister & Connolly, 2015; Yoo, Henfridsson, & Lyytinen, 2010). The ability of governments and businesses to offer many of these electronic services is fundamentally dependent on collecting different types of information online through different internet-enabled technologies, including web-based technologies (Alzahrani, Al-Karaghouli, & Weerakkody, 2017; Carter & Bélanger, 2005; Ritter & Pedersen, 2020). Individuals' personal information are often a cornerstone of the information collected online, and they present a strategic necessity impacting the efficacy and relevance of governments and business electronic services (Ritter & Pedersen, 2020). However, individuals have profound concerns that their personal information could be collected, stored, accessed, or utilized without their explicit consent when provided online (Auxier & Rainie, 2019; Chennamaneni & Gupta, 2023). These concerns about the privacy of personal information manifest in individuals' behaviors towards electronic services - from refusal to share information to deliberately providing inaccurate information or even retracting existing information (Ioannou, Tussyadiah, & Marshan, 2021; Son & Kim, 2008). These actions can disrupt the potential of businesses and governments and compromise the efficacy of their electronic services (Bélanger & Crossler, 2011). Therefore, understanding the relationship between information privacy concerns and individuals' behaviors towards electronic services is pertinent and has become a paramount issue of practice and information systems (IS) research (Rath & Kumar, 2021).

Within governmental and business contexts, individuals' concerns regarding the privacy of their personal information when handled online have been signified recently due to the growing number of online data breaches, identity theft, and privacy infringements and their

profound consequences (Ioannou et al., 2021). As a result, governments have enacted multiple regulations aiming to safeguard individuals' online personal information privacy, ease their concerns about online data privacy, and inspire their confidence to provide their personal information voluntarily when required for government electronic services (Dhotre, Olesen, & Khajuria, 2018). For example, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (U.S. Government Publishing Office (GPO), 2009), introduced requirements for the security of electronic health records and strengthened enforcement of HIPAA (HHS, 1996) rules. Similarly, many businesses have recently been alerted to implementing online data privacy programs to strengthen their data protection capabilities and mitigate the concerns of their customers. For example, major companies like Apple and Google have adopted transparent privacy policies informing users of their rights and offering greater visibility into how their data is handled online (Van Der Schyff, Foster, Renaud, & Flowerday, 2023). Moreover, organizations like hospitals and pharmaceutical companies have also prioritized patient privacy in the healthcare industry by implementing robust online security measures, including encryption of medical records and strict access controls (Semantha, Azam, Yeo, & Shanmugam, 2020).

In harmony, academic Research also paid great attention to online privacy concerns (Miltgen, Popovič, & Oliveira, 2013), and Online information privacy concerns emerged as a theoretical concept encompassing individuals' concerns regarding their control over collecting, using, and disclosing their personal information using an Internet-enabled or online technology (Yun, Lee, & Kim, 2019). Scholars adopted different perspectives to interpret the formation of online information privacy concerns and predict their subsequent behavioral consequences that impact individuals' decisions in online environments (Y. Li, 2012). Scholars grounded their

research in many theories, including the theory of reasoned action (Dinev & Hart, 2006; Rensel, Abbas, & Rao, 2006), the protection motivation theory (Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009; Zhang & McDowell, 2009), the expectancy theory (Dinev & Hart, 2006; Hann, Hui, Lee, & Png, 2007), the social contract theory (Faja & Trimi, 2006; Malhotra, Kim, & Agarwal, 2004), the procedural fairness theory (Culnan & Armstrong, 1999; Xu, Teo, Tan, & Agarwal, 2009), and the social presence theory (Pavlou, Liang, & Xue, 2007). Scholars applied these theories mainly to predict a wide range of consequences of online information privacy concerns, including the adoption of electronic health records (Angst & Agarwal, 2009), disclosing health information online (Bansal & Gefen, 2010), customer repurchasing in online shopping (Chiu, Chang, Cheng, & Fang, 2009), online purchase intention (Eastlick, Lotz, & Warrington, 2006; Janda & Fair, 2004), intention to transact on online portal (Dinev & Hart, 2005) among many others.

According to the often-cited Smith et al. (2011) interdisciplinary review of Privacy concerns research, the Privacy Concerns research typically utilizes theories within ‘‘antecedents – privacy concerns – outcomes’’ (APCO) frameworks, and the outcomes are usually subsequent forms of reluctance to provide personal information (H. J. Smith, Dinev, & Xu, 2011). In online contexts, the outcomes, influenced by the information privacy concerns of potential online identity theft, data misuse, or intrusive surveillance, often deter individuals from embracing online technologies, hindering the adoption and utilization of these online technologies (K. Liu & Tao, 2022). Hence, theoretical frameworks are employed to explain the impact of online information privacy concerns on the use and adoption of online technologies or to offer recommendations on strategies to alleviate the barriers to using online technologies (Ozdemir, Jeff Smith, & Benamati, 2017).

Although the outcomes of online information privacy concerns frameworks, as addressed in previous privacy concerns literature, ultimately are forms of adoption and utilization behaviors of online technologies, the Technology Adoption Models were rarely used as a theoretical foundation in the privacy concerns research (Y. Li, 2012). This is especially unexpected because Technology Adoption Models, such as the Technology Acceptance Model (TAM)(Davis, 1989a), the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003), and the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) (Venkatesh, Thong, & Xu, 2012) are the most prominent models in information systems research predicting users' adoption behavior and the factors influencing their acceptance of technology (Miltgen et al., 2013). Still, these models have been less frequently applied to explain the influence of information privacy concerns on adopting online technologies, which is a notable gap in privacy concerns research.

Closing this gap is important because recent privacy breaches and data misuse scandals involving prominent technology companies have captured individuals' attention and sparked widespread information privacy concerns (Bradely, 2019). These information privacy concerns may have had profound implications for individuals' trust in technology and willingness to adopt new online technologies critical to advancing healthcare systems, financial services, e-retail competitiveness, etc. (Dhagarra, Goswami, & Kumar, 2020; Trkman, Popovič, & Trkman, 2023; Wang, Ngien, & Ahmed, 2022). Given the inherent connection between information privacy concerns and technology adoption, deploying technology adoption models into online privacy concerns research may provide better insights into the influence of information privacy concerns on adopting online technologies.

To fill this gap, I employ the technology adoption model in this research as a theoretical foundation to examine the influence of online information privacy concerns on adopting online technologies.

The roots of the technology adoption model can be traced back to the original model introduced by Fred D. Davis in 1989 (Davis, 1989a). Davis's original model primarily centered around two fundamental constructs: "perceived usefulness," which assesses the extent to which individuals believe that a particular technology will enhance their performance, and "perceived ease of use," which gauges the degree to which individuals perceive the technology as easy to use. Over time, TAM has undergone numerous extensions and refinements to capture the complexities of technology adoption in various contexts. Among these extensions, the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) (Venkatesh et al., 2012) stands out as one of the most recognized and comprehensive models. I chose UTAUT2 to represent all previous technology adoption models because UTAUT2 is the most current extension of the Technology Adoption Models widely acknowledged by researchers to predict individuals' technology adoption (Y. Lee, Lim, & Eng, 2023).

I apply UTAUT2 in my research in line with Venkatesh and many other researchers who called for extending the model to enhance further the explanatory power and practical utility of the model to explain the individuals' technology adoption behaviors involving complex and multifaceted circumstances: "Future research should focus on identifying constructs that can add to the prediction of intention and behavior over and above what is already known and understood" (Venkatesh, Thong, & Xu, 2016). In this research, I incorporate Venkatesh's guidance by introducing the concept of Online Information Privacy Concerns, a multifaceted and complex construct (Y. Li, 2011) that could influence all aspects of the UTAUT2 relationships.

Given that the levels of concern about the privacy of the information are associated with perceived attributes of the information itself (Bansal & Gefen, 2010) and the most influential determinants of individuals' Information Privacy Concerns are the type of information and the perceived value associated with that information itself (Bélanger & Crossler, 2011), I posit in this research that individuals' concerns about the privacy of their online information can arise independently of their perceptions regarding a specific technology's suitability for handling that information. Consequently, in this research, Information Privacy Concerns are examined as a characteristic linked to an individual's perception of the information itself rather than solely contingent on their perception of the technology they intend to use for information management. For example, financial data, healthcare information, general demographic information, social media data, etc., can trigger different privacy concerns regardless of the technology used to store or handle these data types.

Conversely, an individuals' decision to adopt a particular technology is an intentional behavior closely tied to the characteristics of the technology itself (Duarte & Pinho, 2019). The intention to use or adopt a technology is often associated with a set of factors encompassing expectations, perceptions, and conditions related to that technology (Miltgen et al., 2013). These factors encompass usability, user-friendliness, security measures, performance, the context in which the technology is employed, and the perceived value offered by the technology (Y. Lee et al., 2023). Individuals undertake an evaluation of the technology, considering these factors, and an interplay of these factors shapes their ultimate adoption decision (Venkatesh et al., 2016).

While information privacy concerns undoubtedly hold significance, I posit they do not stand alone as an exclusive determinant of technology adoption; rather, they alter the strength of the influence of the factors that shape individuals' technology adoption behaviors. For

illustration, an individual might intend to use a web application designed to organize and store personal information. Initially, the individual assesses the web application characteristics, including factors like performance, usability, functionality, ease of access, ease of use, value, etc. Based on the assessment of these factors, the individual may strongly intend to use the web application. However, the individual intention to use the web application might be altered by the individual's concerns regarding the privacy of the information that will be provided to the web application. Suppose the individual is sensitive about financial information's privacy and is concerned that financial information's exposure can result in high financial loss. The individual concerns regarding financial information privacy reduce the individual's assessment of the web application's value, resulting in a lower intention to use the web application for financial information management. On the other hand, the individual might be less sensitive regarding the privacy of different types of information like schedule information and appointment details. In this case, the lower concerns for information privacy strengthen the individual's assessment of the web application's value, resulting in a higher intention to use the web application. This illustrates how the strength of individuals' assessments of technologies might vary depending on their concerns regarding the privacy of the information involved, influencing the adoption intention of the technology based on the privacy concerns regarding the information involved.

It is essential to highlight that I choose to study the privacy concerns regarding the information, not the type of information, as the factor impacting individuals' intention to use and adopt technologies. This is because privacy concerns about a specific type of information are more meaningful as they recognize the contextual relevance (Acquisti & Gross, 2006) -What may be considered a privacy concern in one context might not be in another for the same type of information; individual variation (Solove, 2007) - People's privacy concerns can vary widely

even for the same type of information; psychological factors (Margulis, 2011) - Privacy concerns are deeply tied to psychological factors, including perceptions of risk, trust, and perceived control. These factors can significantly shape how different individuals approach the sharing of the same type of information. Understanding the psychological dimensions of privacy concerns provides a richer understanding of their influence and behavioral implications (Pastalan, 1970) - Privacy concerns often translate into specific behaviors, they influence behavior and relationship dynamics, making them a crucial factor in understanding how individuals manage and share personal information in various contexts.

In my proposed conceptual model and according to UTAUT2, three dimensions, namely individual beliefs, social influence, and contextual factors, explain the underlying interactions influencing technology adoption by individuals (Tamilmani, Rana, Wamba, & Dwivedi, 2021). The individuals' beliefs dimension (Performance expectancy, Effort expectancy, Hedonic motivation, Price value, and habit) influence individuals' perception of the technology's usefulness, affecting their intention to adopt and use technologies (Y. Lee et al., 2023). However, online information privacy concerns can impact individuals' beliefs differently due to differences in their values and attitudes, and it can effectively alter the strength of the belief-driven rationale that informs technology adoption decisions (Iris A Junglas, Norman A Johnson, & Christiane Spitzmüller, 2008; Mirsch, Lehrer, & Jung, 2017).

The social influence dimension of UTAUT2 refers to influences in the forms of peer recommendations, societal expectations, subjective norms, and social comparisons, among other forms of influences shaped by interactions with others and impacting individuals' perception of the technologies' ease of use and usefulness, playing a crucial role in shaping individuals' decision to adopt technologies (Venkatesh et al., 2012). Then again, online information privacy

concerns can lead individuals to resist social influences regarding technology adoption, altering the power of social influences' impact on individuals' technology adoption behaviors (Cha, 2010).

The contextual factor dimension of UTAUT2 (facilitating conditions) addresses the conditions enabling the use of technologies, like the readiness of the resources, the availability of the needed infrastructure, the accessibility to technical support, the convenience of the training, etc. These conditions contribute to the individuals' perception of technologies' ease of use, lowering the barriers to using technologies and influencing the individuals' adoption behaviors (Bervell, Kumar, Arkorful, Agyapong, & Osman, 2022). Like the other dimensions of UTAUT2, online information privacy concerns may drive individuals to expect additional assurances and resources to protect their sensitive information, altering the degree of the impact of contextual factors on individuals' technology adoption behaviors (Yang & Forney, 2013).

Since online information privacy concerns is a construct that interacts with the strength of the relationships of the three UTAUT2 model dimensions (namely individual beliefs, social influence, and contextual factors), my conceptual model presents an extension of the UTAUT2 model that includes online information privacy concerns as a moderator of all the UTAUT2 model relationships.

The conceptual model at the core of this study is underpinned by a total of twelve hypotheses. These hypotheses serve as the fundamental building blocks for exploring the interactions of information privacy concerns within the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) relationships. Specifically, this comprehensive set of hypotheses comprises two distinct categories. First, six of these hypotheses represent the direct effect hypotheses derived from UTAUT2. These hypotheses articulate the primary relationships

between key constructs outlined in the theory. In this research, the construct of price value, one of the seven components of UTAUT2, has been omitted due to its lack of relevance within the specific research context. The exclusion of the price value construct from this research's model stems from a careful consideration of the specific research setting and its contextual nuances. In this particular investigation, the technology under examination operates in an environment where pricing does not play a significant role in influencing user adoption decisions. This is a result of the unique characteristics of the technology itself, as I will elaborate upon in subsequent sections of this study. Consequently, recognizing the limited relevance and impact of price as a determinant in this particular context, it has been deliberately excluded from the model. Instead, the model prioritizes constructs that are more aligned with the intricate dynamics of technology adoption within this research setting, ensuring a more accurate representation of the key factors influencing user acceptance and use. Second, the remaining six hypotheses are centered around the moderation effects of Information Privacy Concerns on each of the direct effect relationships. In essence, these moderation hypotheses delve into the nuanced impact of individuals' privacy concerns within the context of technology adoption, shedding light on how Information Privacy Concerns interact with and potentially alter the direct relationships proposed by UTAUT2. This dual-layered approach allows for a comprehensive examination of the multifaceted dynamics shaping technology acceptance and use in the presence of information privacy concerns.

To test the proposed model, I study the patients' adoption behavior of web-based healthcare portals in this research. I selected the web-based healthcare portal technology as the focus of this research because it provides a relevant context for examining the interactions between the UTAUT2 adoption model and information privacy concerns. First, UTAUT2 is frequently used to examine technology adoption in the healthcare sector, such as "Citizens"

adoption of m-health (Dwivedi, Shareef, Simintiras, Lal, & Weerakkody, 2016) and "nurses" willingness to use home telehealth (van Houwelingen et al., 2015). UTAT2 is sufficient to predict patients' adoption behavior of healthcare web-based portals, especially since Healthcare researchers frequently use it as a theoretical foundation to predict the use and adoption of similar technologies.

Moreover, the choice of UTAUT2 as the theoretical framework for this research aligns with the evolving paradigm in healthcare, which now recognizes patients as healthcare consumers. This paradigm shift acknowledges that patients increasingly expect healthcare technologies to provide experiences akin to those in other consumer-based industries. UTAUT2, being widely employed to elucidate consumer technology adoption and use behaviors, is well-suited to explore these changing dynamics in the healthcare domain (Chan, 2016). Second, online information privacy concerns are particularly significant within healthcare settings due to the sensitive and personal nature of the information involved (Laric et al., 2009). Hence, it is an important factor in the interactions determining the patients' adoption behavior of the healthcare web-based portals, and it is important to understand its impact on patients' technology adoption behaviors.

Much like the web application example that I addressed earlier, a web-based healthcare solution encompasses various patient services, such as appointment scheduling, communication with healthcare providers, access to medical information, and medical test results. Patients' intention to use these healthcare web-based portals is influenced by their beliefs, social influences, and contextual factors. However, patients' concerns regarding the privacy of specific healthcare information can significantly impact the influence of patients' beliefs, social influences, and contextual factors on their intention to use or adopt these portals. For instance, a

patient's expectations of performance and effort might drive them to use a web-based healthcare portal for general medical information and communication with their primary care physician. However, when faced with using the same portal for managing similar medical information related to a more sensitive health condition, like sexually transmitted diseases or cancer, different health information privacy concerns may arise. These concerns can diminish the patient's expectations of performance and effort associated with the web-based healthcare portal, ultimately leading to their reluctance to use it for handling such sensitive information. As previously discussed, one might argue that patients' perception of the health information's sensitivity or the information's type are the factors influencing patients' technology adoption decisions in the aforementioned example. However, I contend in this research that a more comprehensive understanding of the impact on technology adoption relationships is achieved by considering individual privacy concerns regarding the information instead of the limited assumption of information type or information sensitivity as the impacting factor in similar conditions. My perspective takes into account contextual relevance (Acquisti & Gross, 2006), individual variability (Solove, 2007), psychological factors (Margulis, 2011), and behavioral implications (Pastalan, 1970) of the interaction, as elaborated earlier in this paper. Consequently, it offers a broader and more nuanced explanation of the dynamics at play across various information scenarios.

To test the moderating impact of information privacy concerns on UTAUT2 relationships, I propose conducting a qualitative study utilizing a survey-based approach to collect data from U.S. patients, employing the QUALTRICS survey tool as the primary means of data collection. The online survey is constructed using a combination of established validated instruments (Dwivedi et al., 2016; Venkatesh et al., 2012; Fox et al., 2018) and tailored questions

specific to the research objectives. The data will be analyzed using SPSS statistical software, applying appropriate statistical techniques such as descriptive statistics and regression analysis to draw meaningful conclusions and derive insights that contribute to understanding the impact of information privacy concerns on patients' adoption behavior of the healthcare web-based portals.

I expect the research findings will conclude a negative moderation effect of Information Privacy Concerns on the relationships between Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Condition, Hedonic Motivation, Habit, and the intention to use Web-based healthcare portals.

Studying the moderating effect of the privacy concerns construct on the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) relationships in the healthcare context offers significant academic and practical contributions. From an academic perspective, this research answers the call in Information Systems literature to extend the UTAUT2 model. It fills a gap by exploring the nuanced role of privacy concerns in shaping individuals' acceptance and adoption of technology. This investigation contributes to theory development by enhancing our comprehension of the factors that drive or hinder the acceptance and utilization of technologies, ultimately advancing scholars' knowledge of the complex dynamics that influence technology adoption and usage behavior by examining how privacy concerns moderate the relationships proposed in the UTAUT2 model.

From a practical standpoint, investigating the moderating effect of privacy concerns in the UTAUT2 framework holds practical implications for practitioners and policymakers. By identifying the impact of privacy concerns on technology adoption and use, practitioners can enhance their privacy policies, and they can design interventions and tools to mitigate privacy-

related concerns among technology users. These interventions can lead to improved technology adoption rates and foster trust and confidence among users.

Investigating the moderating effect of privacy concerns in the UTAUT2 relationships within the healthcare context provides both academic and practical contributions. It enriches theoretical understanding and informs evidence-based practices that support the successful implementation and utilization of healthcare technologies while addressing privacy concerns effectively.

CHAPTER 2: LITERATURE REVIEW, CONCEPTUAL MODEL & HYPOTHESES

In this chapter, I review the prior research that incorporates insights into privacy concerns in areas that provide the foundation for my study. The review is structured into four distinct sections. The first section delves into the evolution of the theoretical concept of information privacy concerns, which serves as the fundamental conceptual construct for this study. Following that, the subsequent section examines the research on the influence of information privacy concerns on the use and adoption of online technologies, which offers insights from the prior research on the relationship that constitutes the central focus of this study. Afterward, the chapter delves into the theories that researchers have employed as theoretical foundations to study the influence of information privacy concerns on the use and adoption of online technologies. In the concluding section, I discuss my theoretical model as a novel theoretical framework designed to address the gaps in prior literature and enrich our comprehension of the relationship between information privacy concerns and technology use and adoption, in this section, I provide an elaborate explanation of UTAUT2, as it serves as the theoretical foundation upon which my research is built and I introduce the hypotheses of my research.

2.1 Evolution of the Information Privacy Concerns Theoretical Concept

In this section, I will explore the distinct eras that mark the evolution of the theoretical concept of privacy concerns, alongside the progress made in conceptualizing and measuring these concerns. This exploration will trace how the concept has developed and transformed in response to various technological advancements over time. This section will also delve into the advancements in how information privacy concerns have been conceptualized and the evolution of measurement scales used to quantify these concerns.

2.1.1 Evolution of Information Privacy Research

The concept of privacy has undergone significant transformations, paralleling the advancement of information and communication technologies (H. J. Smith et al., 2011). This concept expanded and diversified as digital technologies evolved, and privacy research underwent four evolution eras (Yun, Lee, & Kim, 2019). During the early development era, before 1960, the focus of privacy research was relatively narrow, limited to collecting and using personal information in a primarily offline context. It was a topic of limited concern, and there was a general sense of comfort with collecting information (Bennett, 1992).

During the second era, from 1961 to 1979, there was a growing recognition of the potential negative impacts of new technologies. This recognition led to the formulation of fair information practices regulatory mechanisms such as the Privacy Act of 1974 (COLIN & RAAB, 1997). The foundation of information privacy research can be traced back to that era, with significant contributions from scholars such as Westin (1967). Westin's definition of privacy as the ability to control personal information and his conceptualization of privacy that emphasized individuals' right to control their personal information (Westin, 1967) set the stage for subsequent empirical explorations in the privacy domain (H. J. Smith et al., 2011). This perspective was crucial in framing privacy as a personal preference, laying the groundwork for modern privacy research (Y. Li, 2011).

Moving into the third era, which covered the years from 1980 to 1989, computer network systems and the Internet emerged. This development prompted the introduction of federal legislation like the Privacy Protection Act of 1984, along with the establishment of European data protection laws. This era marked the beginning of online personal information privacy concerns research, highlighting issues related to data collection and usage by online platforms

(Y. Li, 2011). The fourth era, which began in 1990 and continues to the present day, saw the fast rise of the Internet and the advent of Web 2.0, in addition to the emergence of social media, and brought new challenges as user-generated content and networking services blurred the lines between public and private information. The emergence of the sharing economy and big data further complicated the privacy landscape during this era, introducing concerns about cloud computing and data analytics. This era marks the acknowledgment of privacy as a multifaceted construct influenced by technological, ethical, and legal dimensions (Ozdemir et al., 2017).

Smith, Milberg, and Burke's (H. J. Smith, Milberg, & Burke, 1996) introduction of the Concern for Information Privacy (CFIP) in the 1990s as a scale to measure individual-level privacy concerns significantly advanced the research in this domain during this era. Their work underscored the intricate relationship between individual perceptions of information privacy and information handling characteristics (Stewart & Segars, 2002) .

The latest shift towards an autonomous world, characterized by IoT, AI, and other emergent technologies, has further raised concerns for information privacy, introducing questions about the autonomy of personal information in an interconnected digital environment and the influence of information privacy on individuals' adoption of novel online technologies (Tawalbeh, Muheidat, Tawalbeh, & Quwaider, 2020).

2.1.2 The Operationalization of the Concerns for Information Privacy and the Evolution of Privacy Concerns Constructs

Due to the inherent challenges associated with quantifying the concept of privacy since it is shaped by individual thoughts and perceptions rather than objective or rational evaluations, the majority of empirical privacy research has deployed proxies such as beliefs, attitudes, and perceptions as privacy measures (Mwesiumo, Halpern, Budd, Suau-Sanchez, & Bråthen, 2021).

Over time, the information privacy concerns construct emerged as the central construct for assessing and measuring individuals' information privacy-related concerns (Preibusch, 2013).

Scholars operationalized the concept of information privacy concerns by introducing different measurement instruments. Smith et al. (1996) introduction of the Concern For Information Privacy (CFIP) instrument in 1996 to measure individuals' concerns about organizations information privacy practices constituted a seminal advancement in the operationalization of privacy concerns within the realm of information systems and technology (Holvast, 2007). They developed a scale to measure CFIP through an extensive literature review, expert input, and empirical testing. CFIP recognized the multi-dimensional nature of information privacy concerns, allowing for a more nuanced understanding and measurement of these concerns. The CFIP scale introduced four dimensions for information privacy concerns: Information Collection, focusing on concerns related to the extent and nature of personal information collected, these are concerns over the collection and storage of large quantities of personally identifiable information in organizations' databases; Unauthorized Access, addressing worries about unauthorized access to personal data, these are concerns about personal information given by individuals being accessible by members of the organization collecting the information who are neither supposed nor authorized to access such information; Information error, reflecting fears of how the collecting organization might misuse personal information, these are concerns regarding the intentional or unintentional errors in the handling of personal data by the organizations responsible for collecting this data; and Secondary Use, addressing concerns over the use of personal data for purposes other than originally intended, these are concerns about information being gathered from individuals for a specific purpose and then

being utilized for other secondary purposes within the same organization, without the consent of the information's owner. (H. J. Smith et al., 1996).

Smith et al.'s scale was subsequently reaffirmed and validated by Culnan & Armstrong in 1999 and Stewart and Segars in 2002, confirming its enduring validity (Culnan & Armstrong, 1999; Stewart & Segars, 2002). CFIP instrument robustness and multidimensionality have led to its widespread adoption in various research contexts. It significantly aided the research on privacy concerns representing users' interactions with information systems, shaping scholars understanding of how information privacy concerns impact online behavior while interacting with online technologies (Malhotra et al., 2004). Also, studies on consumer behavior and data sharing often utilized the CFIP instrument to measure individuals' concerns regarding personal data handling by organizations (Ma, Lou, Van Slyke, & Clary, 2020). Furthermore, CFIP played a crucial role in informing policymakers and regulatory bodies in developing privacy laws and guidelines, facilitating a structured approach to balancing privacy rights with organizational responsibilities (Culnan & Armstrong, 1999).

Despite the widespread and applicability of the CFIP scale, it has faced critiques by many scholars, particularly concerning its adaptability in diverse cultural contexts and in the rapidly evolving technological landscape (Dinev & Hart, 2006). These critiques underscored the need for continuous updates and revisions to information privacy instruments to remain relevant and reflect current consumer attitudes and privacy challenges (Xu, Dinev, Smith, & Hart, 2011).

As a result, the information privacy concerns witnessed continuous evolution in its measurement instruments. Each instrument reflected the changing technological landscape and societal attitudes toward privacy (Bartol, Vehovar, & Petrovčič, 2021). Some researchers developed specialized instruments to precisely measure the specific information privacy

constructs that they have focused on in their studies, for example, Deniv and Hart developed and validated an instrument to measure the privacy concerns of individuals who use the Internet and two antecedents, perceived vulnerability and perceived ability to control information (Dinev & Hart, 2004).

Conversely, some researchers developed instruments aimed at measuring information privacy concerns that are specific to technological environments. The most widely recognized example of this is the Internet Users' Information Privacy Concerns (IUIPC) instrument (Malhotra et al., 2004) that was specifically tailored to the context of the Internet. This scale specifically focused on the measurement of privacy concerns constructs that address the nuances of internet environments (Hong & Thong, 2013).

Key to the IUIPC scale is its focus on three primary dimensions: control over personal information, awareness of privacy practices by online entities, and concerns about the collection of personal data. The control dimension reflects the degree to which users feel they can influence their personal information within the internet environment; it represents individuals' concerns about whether they have control over their personal information, as evidenced by the presence of their power in deciding how their data is managed. The awareness dimension focuses on the extent to which users are informed about the privacy practices of internet operating entities with whom they interact. Lastly, the collection dimension deals with concerns about the extent, nature, and purposes of personal data collection in internet environments, it represents the extent to which an individual is worried about the quantity of their personal data held by others in comparison to the value of the benefits they receive (Malhotra et al., 2004).

The IUIPC scale has been particularly influential in advancing scholars' understanding of consumer attitudes toward online handling of sensitive personal information. It provides a robust

framework for examining how information privacy concerns impact consumers' willingness to engage in online transactions and share personal information using online tools (C. Sipior, T. Ward, & Connolly, 2013).

Additionally, the IUIPC scale's emphasis on the internet context makes it particularly relevant for contemporary privacy research, as it addresses the complexities and specificities of privacy concerns in a digital age. The IUIPC has been widely adopted in studies examining various aspects of online behavior, from e-commerce to social media usage, underscoring its versatility and importance in the field of information privacy research (Correia & Compeau, 2017; Groß, 2021).

Approaching privacy concerns from a different perspective, Dinev and Hart (2006) proposed the extended Privacy Calculus approach, offering a fresh viewpoint on comprehending online privacy concerns (Dinev & Hart, 2006). Their approach didn't concentrate on creating a measurement or scale. Instead, they presented a framework that emphasizes the interconnectedness of concerns about online privacy, internet trust, and online information practices. Their holistic perspective was essential for addressing the complex nature of privacy concerns within the growing sphere of online interactions(Bauer & Schiffinger, 2016).

The distinctiveness of this approach lies in its comprehensive measurement of individuals' attitudes and concerns about online privacy. It encompasses the measurement of factors that influence online behavior, including concerns about personal information privacy, the trust users place in internet sites, and the internet sites' information privacy practices. This approach recognizes that online privacy concerns are not just about the fear of personal information misuse but also about the broader trust dynamics between users and online entities (Kezer, Dienlin, & Baruh, 2022).

By addressing how privacy concerns and trust influence user engagement and decision-making in the internet contexts, the privacy calculus model has provided valuable insights for researchers and practitioners alike (Beke, Eggers, Verhoef, & Wieringa, 2022). This approach has been widely applied in exploring user behavior across various digital platforms, including social media and e-commerce sites. For instance, in the realm of social media, the model has been instrumental in understanding how privacy concerns affect users' willingness to share personal information and engage with different platforms (Krasnova & Veltri, 2010). Similarly, in the context of e-commerce, it has shed light on how privacy and trust concerns impact online purchasing decisions (Zhu, Ou, van den Heuvel, & Liu, 2017).

Its emphasis on trust, in particular, sets it apart from other privacy concern models, as trust is a crucial component in online interactions, where users often have to rely on the perceived credibility and reliability of websites and online services. By integrating trust as a dimension, Dinev and Hart's scale offered a more holistic view of the factors that shape online behavior in the context of privacy concerns (Kehr, Kowatsch, Wentzel, & Fleisch, 2015).

Scholars continued introducing scales tailored to capture specific facets of online privacy concerns that their predecessors did not entirely address. For example, Andrade et al. (2002) introduced a new scale to Investigate methods to promote the self-disclosure of personal information online. Their measurement scale included three dimensions: concerns related to identification information, sensitive information, and individual preferences and habits (Andrade, Kaltcheva, & Weitz, 2002). Similarly, Cheung and Liao (2003) introduced a new scale to test the supply challenges in B2C e-commerce in Hong Kong (Cheung & Liao, 2003), Janda (2008)introduced a new scale to study the impact of four different online concerns (privacy, security, etc.) on the intention to make online purchases, and the moderating role of gender

(Janda, 2008), and Janda and Fair (2004) introduced a new scale comprising eleven potential concerns individuals may have about the Internet, including privacy, fraud, etc (Janda & Fair, 2004).

On the other hand, some researchers merged some of the existing instruments to introduce scales specific to their research needs. For example, Hong and Thong (2013) deployed the multidimensional developmental theory, with insights from a comprehensive literature review, to amalgamate the CFIP and IUIPC privacy scales, focusing on further refining the scale to emphasize individuals' concerns about online tools behaviors. They empirically validated their scale through four large-scale online surveys involving nearly 4,000 internet users. Their scale comprised six first-order factors—collection, secondary usage, errors, improper access, control, and awareness (Hong & Thong, 2013).

Hong's scale uniquely amalgamated the strengths of two of the field's most recognized and validated scales. Additionally, his scale addressed calls of other scholars, including Kordzadeh et al., who called for considering control and awareness in the health context based on the Internet Users' Information Privacy Concerns (IUIPC) scale (Kordzadeh, Warren, & Seifi, 2016). Thus, Hong's synthesis resulted in a robust scale that is appropriate for the context of healthcare technologies.

This was evidenced by Fox's research (Fox & Connolly, 2018); They applied Hong's scale within the healthcare sector to assess how information privacy concerns influence patients' willingness to embrace mobile health technology. They selected this particular scale, recognizing its relevance in capturing patients' specific concerns when encountering new online technologies. They concluded that Hong's scale effectively measured patients' privacy concerns during interactions with mobile health solutions. Fox & Connolly's findings affirmed that Hong's scale

not only inherited the reliability of its predecessors but also adapted effectively to the specific context of mobile health privacy concerns. Drawing inspiration from Fox's methodology, my study adopts the same scale, given the close alignment between the aims of my research and those outlined in Fox's work.

Table 1 summarizes the most prominent information privacy scales and examples of the studies utilizing these scales.

Table 1: Information Privacy Scales

Scale	**Created By**	**Dimension**	**Example Literature**	**Scope of Literature**
CFIP	Smith, Milberg, Burke (H. J. Smith et al., 1996)	1. Collection 2. Unauthorized Access 3. Secondary Use 4. Errors	(H. J. Smith et al., 1996)	The research introduces the CFIP scale. Information Privacy is a scale that measures individuals' concerns about their organization's privacy practices
			(Angst & Agarwal, 2009)	Examine the shifts in individuals' attitudes and intentions to opt-in during the adoption of electronic health records.
			(Bellman, Johnson, Kobrin, & Lohse, 2004	Investigate the variations in information privacy concerns and the effects of their precursors.
			(Korzaan & Boswell, 2008	Test the possible impact of personality traits on Privacy Concerns

Table1: Information Privacy Scales (continued)

			Kumar, Mohan, & Holowczak, 2008)	Exploring the determinants that affect security protection measures adopted by home computer users.
IUIPC	Malhotra, Kim, Agarwal (Malhotra et al., 2004)	1. Collection 2. Control 3. Awareness of Privacy Practices	(Malhotra et al., 2004)	Presents the IUIPC scale and examines its impact on the behavior of online consumers under the theme "Internet Users' Information Privacy Concerns".
			(Groß, 2021)	Evaluating the reliability and validity of the Internet Users' Information Privacy Concerns (IUIPC) scale.
			(Pape et al., 2020)	Reassessing the information privacy concerns of Internet users through a case study in Japan.
			(Raber & Krüger, 2018)	Exploring if an individual's privacy practices can be inferred from sources of personality information.
			(Zeng, Lin, & Armstrong, 2020)	A conceptual replication of Malhotra, Kim, and Agarwal's (2004) model.
Privacy Calculus	Dinev and Hart (Dinev & Hart, 2006)	1. Concerns about online privacy 2. Internet trust 3. Information privacy practices.	(Beke et al., 2022)	Redevelopment of the privacy calculus (PRICAL) index and empirical confirmation of the scale validity.
			(Keith, Thompson, Hale, Lowry, & Greer, 2013)	Using information disclosure on mobile devices to examine the privacy calculus
			(Ozturk, Nusair, Okumus, & Singh, 2017)	An integration of privacy calculus theory and trust-risk framework to understand customers' loyalty of mobile hotel booking
			(Kehr et al., 2015)	General privacy concerns and general institutional trust effect on the privacy calculus
			(Meier, Schäwel, & Krämer, 2021)	Examining the intended use of privacy-protecting tools and self-disclosure

Table 1: Information Privacy Scales (continued)

Internet privacy concerns (Combined scale)	Hog & Thong (Hong & Thong, 2013)	1. Collection 2. Secondary usage 3. Errors 4. Improper access 5. Control 6. Awareness	(Fox & Connolly, 2018)	Investigating the Adoption of Mobile Health Technology Across Different Generations
Web privacy concerns (New scale)	Andrade, Kaltcheva and Weitz (Andrade et al., 2002)	1. Concerns for identification information 2. Sensitive information 3. Preferences and habits	Same	Examining approaches to encouraging self-disclosure of personal information on the Internet.
Health information privacy concerns (New scale)	(Bansal & Gefen, 2010	1. Perceived risk 2. Information misuse 3. Information compromise/secondary use	Same	Individuals' preferences influence on Information Sensitivity, Privacy Concerns, and Trust in Health Information Online.
Customer information privacy concerns (New)	Cazier, Jansen, and Dave (Cazier, Jensen, & Dave, 2008)	1. Perceived privacy risk likelihood 2. Perceived privacy risk harm	Same	Factors influencing customers 'intention to use RFID
Personal Information Privacy Concerns (New Scale)	Korzaan and Boswell (Korzaan & Boswell, 2008)	1. Big Five personality traits 2. Computer Anxiety	Same	Personality Traits and Privacy Concerns impact on Behavioral Intentions

2.2 Influence of Information Privacy Concerns on the Use and Adoption of Online Technologies

Building on the discussions in the preceding section, extensive research and many theoretical frameworks have been conducted to explore individuals' information privacy concerns in the online context (Y. Li, 2012; Pavlou, 2011). This body of work is centered around the formation of concerns about personal data being misused; such as being collected, stored, accessed, or utilized online without their permission (Stewart & Segars, 2002), and individuals' responses to these concerns. Common responses often include defensive behaviors like withholding information from websites, providing false details, or deleting their data from online

platforms (Son & Kim, 2008). Such actions have profound implications for online technologies that depend on user data to tailor their services (Sheng, Nah, & Siau, 2008; Xu, Luo, Carroll, & Rosson, 2011). This section of my research aims to present a comprehensive review of the literature addressing the influence of individuals' privacy concerns on the use and adoption of online technologies.

The review is organized into the following four distinct categories: Information privacy concerns influence on individuals' intentions to adopt and use online technologies, influence on individuals' attitudes toward online technologies, influence on individuals' trust in online technologies, and influence on individuals' online technologies adoption behaviors.

2.2.1 Information Privacy Concerns Influence on Individuals' Intentions to Adopt and Use Online Technologies

Understanding how information privacy concerns influence individuals' intentions to use online technologies is a focus of a substantial body of literature (Barth & De Jong, 2017). Intention to adopt or use online technology refers to an individual's expressed plan or inclination to engage in specific actions or behaviors related to the use of digital tools or services. It encompasses the conscious decision-making process through which individuals decide whether they are willing or likely to adopt, utilize, or interact with online technologies (Ajzen, 1991; Davis, 1989b). Individuals' information privacy concerns exert a profound influence on their intentions to adopt online technologies (Ozdemir et al., 2017). For example, when individuals have concerns about the privacy and security of their health data within a mobile health application, the fear of potential data breaches or unauthorized access can lead individuals to hesitate in fully embracing the mobile health technology, impacting their readiness to actively engage with its features (Angst & Agarwal, 2009). These privacy concerns act as crucial determinants shaping individuals' intentional decisions and underscoring the influence of privacy

concerns on individuals' willingness to adopt and use online technologies (Ozdemir et al., 2017). Numerous studies within the fields of information systems, information privacy, healthcare, and consumer behavior have delved into the relationship between privacy concerns and individuals' willingness to adopt and engage with various online technologies (Bélanger & Crossler, 2011; Y. Li, 2011; H. J. Smith et al., 2011). Scholars have explored how perceived information privacy concerns, encompassing issues such as data security, unauthorized access, and potential misuse, can shape individuals' cognitive processes and decision-making regarding the acceptance and utilization of tools and systems, including online technologies (Y. Li, 2011).

For example, investigated the impact of privacy concerns on individuals' intention to use e-commerce platforms. Their studies found that individuals with heightened privacy concerns were less likely to express a strong intention to use online shopping technology to purchase online. The findings emphasized the role of perceived privacy in shaping shoppers' behavioral intentions toward the adoption of e-commerce platforms (Eastlick et al., 2006; Janda, 2008).
Similarly, a mixed methods study conducted by Fox and Connolly (2018) presented an explanation of the mobile health digital divide, underscoring that this divide is intensifying among older adults, primarily attributed to their strong information privacy concerns as a prominent factor influencing the older population's hesitancy towards adoption of mobile health technologies. Notably, the study advocates for the development of privacy literacy as a pivotal strategy to alleviate privacy concerns among older patients and as a crucial pathway to boost their intention to adopt mobile health technologies (Fox & Connolly, 2018).

Information privacy concerns also emerged consistently as a significant factor influencing individuals' information disclosure intentions, thereby consistently impacting their adoption of online technologies requiring the collection of personal information (Frye &

Dornisch, 2010; Xu et al., 2009). This was also consistent with healthcare research, where information privacy concerns were found to play a significant role in shaping patients' intentions to opt in, consequently maintaining a consistent impact on the adoption of electronic health record technologies (Angst & Agarwal, 2009).

In an alternative to the aforementioned research approach focusing on the direct impact of information privacy concerns on technology use and adoption, information privacy concerns were examined as a moderator affecting the intensity of the relationships that predict the intention to adopt online technologies. For instance, Le et al. (2023) posited that information privacy concerns serve as a moderator in the relationship between customers' acceptance of mobile functions, acceptance of advertisements, and their intention to engage with mobile-based advertising. Their study concluded significant information privacy concerns moderation impact on the relationships that shape the adoption of mobile-based advertising technology by customers (Le, Yoo, & Park, 2023).

Another study addressing the moderating role of information privacy concerns on a technology adoption intention relationship was concluded by Mirsa et al.'s (2018). Their research investigated the impact of perceived usefulness and trust on users' continuance intention towards mobile health applications. Their findings posit that information privacy concerns can enhance the influence of perceived usefulness on continuance intention and significantly strengthen the effect of trust on continuance intention (Misra, Kumar, & Munnangi, 2019).

2.2.2 Information Privacy Concerns Influence on Individuals' Attitudes Toward Online Technologies

Individuals' information privacy concerns play a pivotal role in shaping individuals' attitudes toward various online technologies (Lian & Lin, 2008). An attitude in the online environment encompasses an individual's overall evaluation, feelings, and predisposition toward

a specific online tool or service (Bano, Sarfraz, Salameh, & Jan, 2022). Take the example of a social media platform where individuals engage in online interactions. Individuals' concerns about their personal information, such as concerns about the misuse or unauthorized access to their personal information, may lead individuals to develop negative sentiments and reservations, ultimately shaping their attitude toward the social media platform (Elueze & Quan-Haase, 2018). According to the theory of planned behavior, attitudes exert an impact on behavior by intertwining with beliefs about the consequences of the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991). Hence, the connection between information privacy concerns and the shaping of attitudes ultimately dictates individual adoption behaviors of online technologies.

Several research examined the influence of information privacy concerns on individuals' attitudes toward online technologies. For example, Lian and Lin (2008) analyzed the online purchases context. Their research concluded that individuals with elevated privacy concerns exhibited more negative attitudes towards online shopping platforms. This negativity was prompted by the necessity to provide private information during online transactions, thereby triggering a significant impact on some shoppers' overall evaluation, feelings, and predisposition toward the online shopping tool due to their heightened privacy concerns (Lian & Lin, 2008).

In a study addressing the moderating effect of information privacy concerns, Zarouali et al. (2017) investigated the relationship between targeted advertising and adolescents' attitudes toward Facebook ads. They specifically examined the moderating role of information privacy concerns in this online interaction. Their experimental study that involved 363 adolescents aged 16-18 years indicated that adolescents with elevated privacy concerns demonstrated an increased skeptical attitude toward ads, leading to a decrease in intentions to use Facebook for purchasing

online (Zarouali, Ponnet, Walrave, & Poels, 2017). In alignment with the literature concluding the significance of information privacy concerns as a moderator of relationships affecting behavioral intention to adopt online technologies, the research conducted by Zarouali et al. (2017) also underscores the relevance of a comparable moderation effect of information privacy concerns on relationships that shape attitudes toward using and adopting online technologies.

2.2.3 Information Privacy Concerns Influence on Individuals' Trust in Online Technologies

Trust is a multifaceted and complex concept with varying conceptualizations across different fields (Lewis & Weigert, 1985; McKnight, Choudhury, & Kacmar, 2002). For instance, in the field of psychology, trust might be viewed through the lens of interpersonal relationships, emphasizing emotions and social bonds (Lewis & Weigert, 1985). In contrast, in the context of information systems, trust is defined as the belief or confidence that users place in the reliability, security, and effectiveness of a digital system, technology, or online platform. It involves the expectation that the system will perform as intended, safeguard users' information and privacy, and fulfill their needs or expectations (Gefen, Karahanna, & Straub, 2003). Past research has established that the perceived level of trust significantly influences individuals' decision-making processes when considering the adoption of online services (M.-C. Lee, 2009; Mou, Shin, & Cohen, 2017; Reichheld & Schefter, 2000).

Previous research indicates that information privacy concerns serve as a robust predictor of trust in the context of online technologies (Bansal & Gefen, 2010; Casaló, Flavián, & Guinalíu, 2007; Cases, Fournier, Dubois, & Tanner Jr, 2010; Kim, 2008; Malhotra et al., 2004). Theoretical frameworks, such as the Privacy Calculus Model, argue that individuals assess the perceived risks and benefits associated with disclosing personal information online (Dinev & Hart, 2006). When information privacy concerns are high, individuals are more likely to perceive greater risks, leading to a diminished level of trust in the online tool's ability to protect their

sensitive data. As trust is a fundamental element in technology adoption (Gefen et al., 2003), this reduced trust, in turn, negatively influences users' willingness to adopt the online tool (Xu et al., 2009). In essence, a high level of information privacy concerns acts as a barrier to the development of trust, consequently hindering the adoption of the online tool.

Bansal et al.'s (2010) study in the healthcare sector aligns with the aforementioned impact of privacy concerns on trust and the resulting impact on the adoption of online technologies. Their research underscores that a patient's intention to disclose information through online healthcare technology is intricately linked to the level of trust in the technology. Importantly, the study reveals that this trust is significantly influenced by the patient's privacy concerns. In the context of healthcare, where the sensitivity of personal information is paramount, privacy concerns play a pivotal role in shaping patients' trust in online healthcare technology (Bansal & Gefen, 2010). This study emphasizes the multifaceted nature of trust and information privacy concerns in the healthcare sector, providing valuable insights for the development and adoption of online healthcare technologies.

2.2.4 Information Privacy Concerns Influence on Individuals' Actions Toward Online Technologies

This information privacy concerns line of research delved into understanding the impact of information privacy concerns on individuals' actions and behaviors during interactions with online technologies (Segijn, Voorveld, & Vakeel, 2021; Sheehan & Hoy, 1999; Yao & Zhang, 2008). Individuals' actions and behaviors during interactions with online technologies serve as a direct and tangible measure of their adoption, offering a more concrete assessment compared to the traditional approach using the theory of planned behavior, which often relies on behavioral intention as a proxy for actual technology adoption (Ajzen, 1991). Unlike behavioral intention, which reflects an individual's expressed plan or willingness to use a technology, observing actual

actions provides a real-time evaluation of their engagement with the technology (Hennessy, Kinsella, & Thorne, 2016).

For instance, consider an individual who expresses a positive behavioral intention to use a mobile health app due to perceived benefits. In the traditional approach, this intention might be considered a proxy for adoption. However, by observing the individual's actual behavior, such as the frequency of app usage, the completion of health-related tasks, or the sustained use over time, researchers can gain more accurate insights into the genuine adoption of the technology. This approach of assessing concrete actions offers a more nuanced understanding of how information privacy concerns influence the tangible adoption of online technologies in real-world scenarios.

This approach has received comparatively less attention in research than the previous types of research, primarily because of the challenges associated with observing and measuring actual adoption behaviors. An example of this research is Sheehan & Hoy's (1999) study, which investigates the connection between privacy concerns and consumer online behavior. The research explored the correlation between consumer information privacy concerns and actions taken to protect privacy, ultimately influencing consumers' adoption of the online environment. Participants' concerns about various situations affecting online information privacy were evaluated. The overall level of concern was subsequently correlated with the frequency of respondents adopting seven different online behaviors. The analysis revealed that the frequency of adopting five out of the seven behaviors increased as respondents' privacy concerns heightened. For example, with escalating privacy concerns, respondents reported a greater likelihood of providing incomplete information to websites and requesting removal from online lists. Furthermore, as privacy concerns increased, respondents indicated a decreased likelihood of registering for website functionalities (Sheehan & Hoy, 1999). These actions collectively

represent adoption behaviors, underscoring the direct impact of information privacy concerns on the acceptance and utilization of online technologies.

Within this research approach, information privacy concerns were also studied as a moderator influencing the strength of the relationship that shapes adoption behaviors in online environments. This was illustrated in Segijn et al. (2021) study that investigated whether synchronized advertising on tablets influences consumers' memory and attention toward tablet advertisement features. The study utilized an eye-tracking experiment to explore the moderating influence of consumers' privacy concerns as a personal factor. Findings indicated that consumers with elevated privacy concerns paid less attention to advertising features on tablets compared to those with lower privacy concerns. These results highlight that the strength of synchronized advertising's impact on consumers' use of advertising features on tablets is contingent on their privacy concerns (Segijn et al., 2021). This serves as yet another example underscoring the importance of information privacy concerns as a moderator influencing relationships impacting online behaviors.

The aforementioned research underscores the pivotal role that information privacy concerns play in shaping users' decisions and behaviors toward online technologies. Whether examined through the lens of behavioral intention, attitudes, trust, or direct influences on behavior, conclusions across diverse studies provide compelling support for the overarching impact of information privacy concerns on the adoption and utilization of online technologies. In the coming section, I delve into the theoretical foundations used by researchers to explain this relationship.

2.3 Theories Utilized in Researching Online Information Privacy Concerns

In the exploration of online information privacy concerns, scholars adopted a variety of theoretical perspectives to understand and explain the formation of individuals' concerns and their influence on individuals' online behaviors (Y. Li, 2012; Pavlou, 2011). These theories, drawn from diverse academic disciplines, offer rich theoretical insights that explain the multifaceted nature of privacy concerns and their influence in online environments (Bélanger & Crossler, 2011).

Starting with Agency Theory, scholars delved into the principal-agent problem, which is particularly pertinent in online transactions (Bergen, Dutta, & Walker Jr, 1992). This theory underscores the issues of information asymmetry and the potential for opportunistic behavior by online agents (Eisenhardt, 1989). In the context of online privacy, Agency Theory suggests that consumers, as principals, are often at a disadvantage due to the lack of knowledge on how the online technologies (agents) are going to use the individuals' personal information. This imbalance raises concerns about privacy as individuals are uncertain about how their personal information is being used by these agents. Accordingly, the individuals decide whether to provide information to participate in the online transactions or take alternative action to mitigate the risk of providing the information (Culnan & Armstrong, 1999). In their research on understanding and mitigating uncertainty in online exchange relationships, Pavlou et al. applied agency theory. Their findings suggested that to alleviate uncertainties in these relationships, it is essential to address agency issues such as hidden information. They identified four critical factors that can mitigate uncertainty and help facilitate online exchanges by adopting a principal-agent perspective (Pavlou et al., 2007). Similarly, Peslak utilized the agency theory as a theoretical framework to conclude that application of Fair Information Practices is a significant

factor to reduce the privacy issues of RFID and influence it's adoption by the consumers (Peslak, 2005).

Likewise, Social Contract Theory, rooted in the philosophical works of Rousseau and Locke (Rousseau, 2018), provides another lens through which online privacy is examined. This theory posits that fair practices in business transactions are governed by social contracts (Donaldson & Dunfee, 1994). In the online context, this translates into the importance of informed consent and the right of exit for online users. Studies leveraging this theory have highlighted that online services must honor the implicit social contracts with their customers, particularly in handling personal information, to mitigate the individuals' information privacy concerns and encourage the use of the online services (Andrade et al., 2002; Jahangir & Begum, 2007).

Another particularly intuitive theories for the information privacy concerns application are the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB), originating from the works of Ajzen and Fishbein (1975, 1980), focus on the individual's intentions to disclose personal information (Ajzen, 1991). These theories posit that such intentions are influenced by attitudes, subjective norms, and perceived behavioral control. In online privacy studies, these theories have been instrumental in explaining how individuals decide whether or not to share personal information online based on their beliefs, norms, and perceived control over their information (Angst & Agarwal, 2009; Chiu et al., 2009; Dai & Palvi, 2009; Kumar, Mohan, & Holowczak, 2008; C. Liu, Marchewka, Lu, & Yu, 2005) .

As discussed earlier, Deniv and Hart (2006) deployed the Privacy Calculus Theory (Laufer & Wolfe, 1977) to introduce the Privacy Calculus model which is widely used as a theoretical model in the information privacy concerns research. The perspective of privacy

calculus theory is used directly or through the privacy calculus model in information privacy research suggesting that individuals' intention to disclose information online is a trade-off between the expected benefits and perceived privacy risks (Culnan & Armstrong, 1999; Dinev & Hart, 2006). This theory has been particularly useful in understanding behaviors in e-commerce, where consumers weigh the benefits of personalized services against the risks of personal data exposure (Hann et al., 2007; H. Li, Sarathy, & Xu, 2010; Xu et al., 2009).

Utility Maximization Theory (Haring & Smith, 1959), derived from economic theory, is another theory that has been employed to understand how individuals make decisions regarding the disclosure of personal information by balancing the utility gained against privacy concerns (Premazzi et al., 2010). The theory applies the concept of maximizing total utility or satisfaction to the context of information privacy (Bansal & Gefen, 2010).

Expectancy Theory of Motivation and Expectancy-Value Theory, rooted in psychological theories of motivation (Vroom, 1966), emphasize how individuals' motivations and attitudes are shaped by their expectations of outcomes and the value they place on these outcomes. In the realm of online privacy, these theories have been used to explain how expectations about the privacy and security of personal information influence user behavior (Sheng et al., 2008; Shin, 2010).

Procedural Fairness Theory focuses on the perception of fairness in organizational processes, particularly in how customer information is managed and used (Barrett-Howard & Tyler, 1986). This theory has been pivotal in exploring consumer reactions to data breaches and privacy policies, as perceptions of fairness in these situations significantly impact trust and subsequent behavior (Faja & Trimi, 2006).

Social Presence Theory and Social Response Theory (Rice, 1993), examining the impact of social elements in online environments, offered insights into how the presence of others influences privacy concerns. Studies using these theories have shown that the perceived social presence in online platforms can affect how comfortable individuals feel sharing personal information (Joinson, Reips, Buchanan, & Schofield, 2010).

Protection Motivation Theory, often applied in information security studies (Lebek, Uffen, Neumann, Hohler, & H. Breitner, 2014), has also been adapted by scholars for research in information privacy, given the interconnectedness of these fields. This theory examines the ways in which an individual's intent to safeguard against threats is shaped by various factors, including the perceived intensity and vulnerability to these threats (Rogers, 1975). It has been applied to understand how users respond to privacy threats in the online world. This theory has been particularly useful in examining behaviors related to the adoption of privacy-protecting measures in online environment (Iris A. Junglas, Norman A. Johnson, & Christiane Spitzmüller, 2008) .

Likewise, Information Boundary Theory, Social Cognitive Theory, and various Personality Theories have been utilized by researchers in diverse studies. Researchers applied these theories to provide distinct theoretical viewpoints on the development and repercussions of information privacy concerns in online settings (Y. Li, 2012).

In sum, these theories collectively provide a comprehensive understanding of the dynamics of online information privacy. By drawing from diverse disciplines, they offer nuanced insights into the complex interplay of individual, societal, and technological factors that shape privacy concerns and the resulting online behaviors. Interestingly, it was quite uncommon to find the Technology Adoption Model being applied as a theoretical basis in information privacy research. There's a notable scarcity of research utilizing TAM in this domain, this is a surprising

observation, especially considering that the implications of information privacy concerns in online environments frequently influence usage and adoption behaviors, as demonstrated above in the application of various theories in this field. Given the Technology Adoption Model's established role in forecasting technology usage and adoption, one might anticipate its broader adoption in research as a foundational theory, yet this appears not to be the prevalent trend.

2.4 Conceptual Model and Hypotheses

From the thorough literature review conducted, two key conclusions emerge: First, the construct of information privacy concerns is well-established in theory and has been empirically proven by various researchers, using diverse theoretical frameworks, to significantly affect individuals' usage and adoption of online technologies. Second, despite their established status and recognized capability to elucidate technology use and adoption, technology adoption models have seldom been employed to explain the consistently observed influence of information privacy concerns on the use and adoption of online technologies.

The identified disconnect between these two conclusions highlights a research gap in the field of information privacy. To address this, I suggest the conceptual model presented in Figure 1 as a means to enhance the existing body of research on information privacy concerns.

2.4.1 Conceptual Model

In order to validate the proposed model, this research focuses on examining patients' adoption behaviors towards web-based healthcare portals. The choice of web-based healthcare portal technology as the subject of this study is strategic, given its relevance in exploring the interplay between the UTAUT2 adoption model and information privacy concerns.

Firstly, UTAUT2 has been a popular model for studying technology adoption within the healthcare sector. Instances include research on citizens' adoption of mobile health (Dwivedi et

al., 2016) and nurses' engagement with home telehealth systems (van Houwelingen et al., 2015). UTAUT2 is considered an effective predictor of patient behavior concerning the adoption of web-based healthcare portals, corroborated by its frequent use in healthcare research to predict the use and adoption of analogous technologies. Furthermore, the application of UTAUT2 in this study is particularly relevant due to the evolving perception of patients as consumers in healthcare. This shift acknowledges that patients now expect healthcare technologies to offer consumer-like experiences, similar to those in other consumer industries. UTAUT2, with its extensive application in understanding consumer technology adoption and use, is aptly suited for investigating these shifting paradigms within the healthcare context (Chan, 2016).

Secondly, the issue of online information privacy is of heightened significance in healthcare due to the confidential and personal nature of health information (Laric et al., 2009). Understanding its impact on the adoption behavior of healthcare web-based portals is crucial, as it plays a critical role in shaping patients' technology adoption decisions. This research aims to delve into these dynamics, providing insights into how privacy concerns influence patient behavior in the context of web-based healthcare technologies.

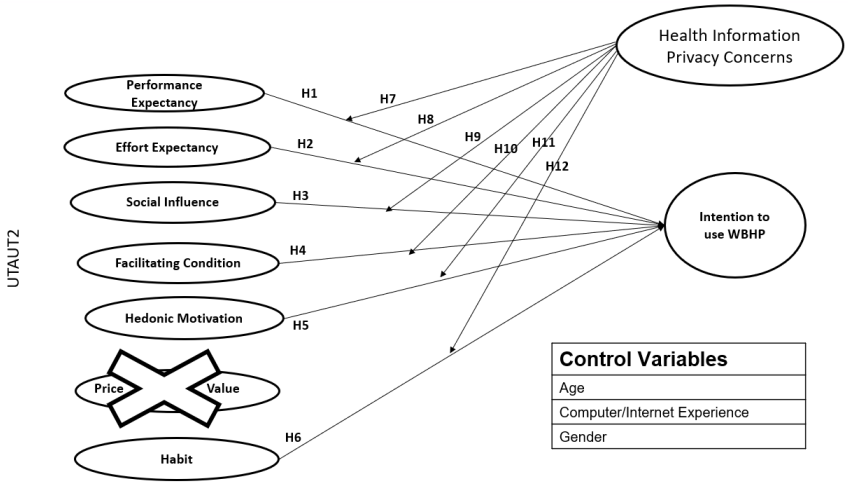

Figure 1: Conceptual Model

2.4.2 Direct Effect Hypotheses

2.4.2.1 Performance Expectancy

Performance expectancy, in general, refers to the degree to which an individual believes that using a particular system or technology will enhance their job performance (Venkatesh et al., 2012). When applied in healthcare research, scholars posit that it encompasses the belief that using healthcare technologies, such as mobile health (m-health) systems or privacy-enhanced Health Information Systems (HIS), will improve an individual's health management performance (Dwivedi et al., 2016; Hsu, Lee, & Su, 2013).

In the context of web-based healthcare portals, performance expectancy presents the extent to which patients perceive web-based healthcare portals as effective tools for managing their health. Previous research consistently demonstrated a strong positive relationship between performance expectancy and the intention to use various technologies (Ahmed et al., 2020; Zhou et al., 2019), including technologies in the healthcare domain (Beh, Ganesan, Iranmanesh, & Foroughi, 2021; Hsu et al., 2013; Reyes-Mercado, 2018). The underlying rationale is that individuals are more inclined to adopt technologies if they believe they will enable them to attain gains in job performance (Venkatesh et al., 2012). Similarly, patients are more inclined to adopt healthcare technologies if they believe they will enable them to manage their health more effectively (Dwivedi et al., 2016). This relationship can be particularly applicable to web-based healthcare portals, which are increasingly recognized for their potential to empower patients' health self-management, especially those with chronic conditions (Goldzweig et al., 2013).

For example, web-based healthcare portals offer several functionalities that can help patients to attain health benefits, including access to test results, health appointment management, educational materials, and access to healthcare providers (Goldzweig et al., 2013).

Moreover, the notification functionalities embedded in these portals assist in managing health risk factors by providing personalized feedback and alerts. Web-based healthcare portals can facilitate proactive health management and can potentially lead to improved health outcomes (Emont, 2011). Hence, I hypothesize that:

H1: Performance expectancy is positively associated with the intention to use web-based healthcare portals.

2.4.2.2 Effort Expectancy

In technology adoption research, effort expectancy refers to the ease of use associated with a particular system or technology (Venkatesh et al., 2012). Similarly, In the healthcare context, this concept was applied to refer to the degree of ease associated with the remote and self-use of the overall healthcare system (Dwivedi et al., 2016). Effort expectancy in web-based healthcare portal settings involves patients' perceptions of how user-friendly and accessible these portals are. The ease of navigation, understanding of the interface, and the overall simplicity of interaction with the portal all contribute to the effort expectancy.

Research has shown that effort expectancy is a critical factor influencing technology adoption (Chatterjee & Bhattacharjee, 2020; Talukder, Chiong, Bao, & Hayat Malik, 2019). For patients, the ease of using technology plays a significant role, especially considering the diverse demographic, including patients of varying ages, health conditions, and technological proficiency (Holden & Karsh, 2010). When healthcare technologies are perceived as easy and straightforward to use, patients are more likely to adopt them for managing their health (Gao, Li, & Luo, 2015). This is particularly true for web-based healthcare portals since they require regular interaction, such as scheduling appointments, accessing test results, or managing medications.

For instance, web-based healthcare portals designed with user-friendly interfaces and clear instructions can enhance patients' confidence in managing their health online. Features like simplified navigation, easily accessible information, and responsive design for various devices significantly reduce the effort required to use these portals (Weng, Hsieh, Hsieh, & Lai, 2007). The reduced effort and increased ease of use are likely to enhance patients' satisfaction and their intention to use the web-based healthcare portals. Therefore, I propose the following hypothesis:

H2: Effort expectancy is positively associated with the intention to use web-based healthcare portal.

2.4.2.3 Social Influence

Social influence, within the framework of technology adoption models, refers to the degree to which individuals perceive that important others believe they should use a new system (Venkatesh et al., 2003). Like other UTAUT2 determinants, this concept was also used in healthcare setup referring to the degree of which an individual perceives that important others believes he or she should use a specific healthcare technology (Hsu et al., 2013). For my study, social influence can be understood as the impact of peers, family, healthcare providers, and societal norms on individuals' intentions to use web-based healthcare portals.

The decisions to adopt new healthcare technologies are often influenced by the recommendations and behaviors of healthcare providers, family members, and peers (Holden & Karsh, 2010). The impact of social influence on increasing the adoption of technologies, particularly in the healthcare domain, is well-documented (Adapa, Nah, Hall, Siau, & Smith, 2018; Giovanis, Assimakopoulos, & Sarmaniotis, 2019; Oliveira, Thomas, Baptista, & Campos, 2016). For instance, when healthcare providers encourage the use of web-based portals for managing health, patients are more likely to perceive these portals as beneficial and credible.

Similarly, when family members and peers use or endorse these portals, it can create a social norm, further motivating individuals to adopt the technology. Moreover, If important social contacts are actively using web-based healthcare portals, their usage becomes normative, potentially leading patients who are not utilizing these portals to feel socially outdated and experience an influence to adopt them in order to align with prevailing social norms. Web-based healthcare portals also gain legitimacy and perceived usefulness when endorsed by respected figures or peers in patients' social circles.

In summary, the perceived pressure or encouragement from important others, including healthcare providers and social circles, positively influences an individual's intention to use web-based healthcare portals. In light of this, the following hypothesis is proposed:

H3: Social influence is positively associated with the intention to use web-based healthcare portals.

2.4.2.4 Facilitating Condition

Facilitating conditions refer to the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system (Venkatesh et al., 2003). In their research on the adoption of mobile health technology, Dwivedi et al. referred to facilitating conditions as the degree to which an individual believes that an organizational and technical infrastructure and continuous trustworthy support system exists to support the use of the system continuously from any justified remote places with reliability (Dwivedi et al., 2016). For this research, facilitating conditions encompass the availability of necessary technical support, infrastructure, and resources that enable the patients to effectively use the web-based healthcare portals.

The influence of facilitating conditions on technology adoption is significant as concluded in previous literature (Al-Emran, AlQudah, Abbasi, Al-Sharafi, & Iranmanesh, 2023; Beh et al., 2021; Reyes-Mercado, 2018). In the case of web-based healthcare portals, when patients perceive that the necessary support, training, technical assistance, simple internet speed requirements, and compatibility with a wide range of hardware are readily available, their likelihood of adopting and effectively using these portals increases (Sadeghi, Thomassie, & Sasangohar, 2017). This is especially important in healthcare settings, where the user base includes individuals with varying degrees of technical expertise and comfort with digital tools.

For instance, the presence of a responsive helpdesk to assist with technical issues, user-friendly tutorials guiding patients through the portal, and assurance of data security and privacy are all examples of facilitating conditions that can encourage the adoption of web-based healthcare portals. Considering these factors, the following hypothesis can be proposed:

H4: Facilitating conditions is positively associated with the intention to use web-based healthcare portals.

2.4.2.5 Hedonic Motivation

Hedonic motivation refers to the fun or pleasure derived from using technology (Venkatesh et al., 2012). In the case of web-based healthcare portals, hedonic motivation would relate to the enjoyment or satisfaction patients experience while using these portals, beyond just the utilitarian aspects of managing health.

Several studies concluded findings suggesting a positive impact of hedonic motivation on individuals' adoption of different technologies (Brown & Venkatesh, 2005; Thong, Hong, & Tam, 2006). For example, Van der Heijden (2004) concluded that intrinsic utility is important in increasing individuals' willingness to adopt new technologies (Van der Heijden, 2004), and

Rahim et al. (2022) found that fun and enjoyment significantly influence students' intentions to utilize new technologies (Rahim, Iahad, Yusof, & Al-Sharafi, 2022).

In the case of web-based healthcare portals, when patients find intrinsic enjoyment or satisfaction in interacting with these portals, their likelihood of continual intention to use and adopt these portals increases. This aspect of hedonic motivation is particularly salient in the healthcare context, where the use of technology can often be perceived as a necessity rather than a choice.

For instance, a web-based healthcare portal that offers an engaging, interactive, and aesthetically pleasing interface may enhance user enjoyment. Features such as personalized health tips, interactive health tracking tools, or gamification elements that reward users for health-related achievements can contribute to this hedonic value. When patients find using the portal to be a pleasurable experience, it can lead to higher levels of engagement and a positive intentions towards using the technology for health management. Based on this understanding, I propose the following hypothesis:

H5: Hedonic Motivation is positively associated with the intention to use web-based healthcare portals.

2.4.2.6 Habit

Similarly, Habit refers to the extent to which individuals tend to perform behaviors automatically due to learning (Limayem & Hirt, 2003). In relation to web-based healthcare portals, habit is the degree to which patients automatically use these portals as part of their routine health management practices.

Like all UTAUT2 determinants, the role of habit in technology adoption is pivotal. Researchers in different fields addressed such a role (Bower, DeWitt, & Lai, 2020; Foroughi et

al., 2023). When the patients' use of web-based healthcare portals becomes habitual, it signifies a transition from deliberate usage to automatic behavior (Ferreira, Oliveira, & Neves, 2023). This habitual use is often a result of repeated interactions with the portal, leading to increased familiarity and ease of use over time.

For example, when patients habitually log into a healthcare portal to schedule appointments, view test results, or communicate with their healthcare providers, it reflects the integration of the portal into their daily health management practices. The development of such habits is crucial, as it indicates a deep level of engagement and reliance on the portal, suggesting a shift from conscious decision-making to automaticity in usage. Given these considerations, the following hypothesis is proposed:

H6: Habit is positively associated with the intention to use web-based healthcare portals.

2.4.3 Moderation Relationships

Web-based healthcare portals, which may host sensitive health information, are online technologies that can be a source of concern regarding the online privacy of personal health information. To fully grasp the nature of patients' information privacy concerns in this technological healthcare context, it is essential to consider a range of dimensions that directly impact patients' perceptions of information privacy. These dimensions include concerns about the collection of health data, its potential secondary use, the risk of improper access, possibilities of errors, the level of control patients have over their information, and their awareness of how their information is managed within these portals (Fox & Connolly, 2018).

The information collection process in web-based healthcare portals, which involves gathering patient data, often raises concerns about the extent and necessity of data acquired, leading to concerns about potential privacy exposure of sensitive or excessive amounts of

information (H. J. Smith et al., 1996). This is exacerbated by issues related to secondary use, where health information initially collected for specific purposes might be repurposed for others, such as research, without explicit consent from patients, thereby engendering concerns about secondary parties accessing patients' health information without patients' consent (Hong & Thong, 2013). Furthermore, the risk of improper access, encompassing unauthorized or unintended viewing of patients' data, is also a significant concern. Incidents like security breaches that facilitate unauthorized access to patient records contribute to patient concerns about the intentional or unintentional exposure of their health information (Andrade et al., 2002). Alongside this, the possibilities of errors in handling patient data, from data entry inaccuracies to transmission faults, may violate privacy and foster a climate of information privacy concerns (Auxier & Rainie, 2019). Control over information, defined as the degree to which patients can manage their health information, is another critical dimension. The ability, or lack thereof, for patients to update or restrict access to their records directly influences their perceptions of autonomy and control over their personal health data (Malhotra et al., 2004). Lastly, patient awareness regarding web-based healthcare portals' information policies and practices also plays a crucial role. The extent to which privacy policies and terms of use are made clear and accessible to patients affects their understanding and trust in the ability of healthcare web-based portals to manage their information (Andrade et al., 2002). In essence, these dimensions collectively shape the patients' information privacy concerns regarding web-based healthcare portals (Hong & Thong, 2013).

Patients' privacy concerns regarding their health information significantly influence their willingness to adopt healthcare technologies that collect such private data (Frye & Dornisch, 2010; Joinson et al., 2010). This underscores a crucial relationship where concerns about

information privacy have been found to introduce a negative influence on patients' behavior in the context of digital healthcare adoption (Bansal & Gefen, 2010)

My study centers on exploring the moderation interaction between information privacy concerns and the determinants of technology adoption intentions, specifically investigating through UTAUT2 lenses how these health information privacy concerns influence the intention to adopt web-based healthcare portals. This approach follows in the footsteps of the seminal work of Angst and Agarwal (2009), who, in their study on the adoption of Electronic Health Records amidst privacy concerns, shifted focus from studying the direct effects of privacy concerns, a topic extensively examined in various studies linking different privacy concerns constructs to attitudes and technology usage intention (Eastlick et al., 2006), to the moderating role of information privacy concerns. Their study articulated the importance of examining "the extent to which concern for information privacy interacts with the determinants of attitude change," thereby providing a foundation for my study's focus on the interaction between privacy concerns and the determinants of technology adoption intentions (Angst & Agarwal, 2009).

Exploring the moderating interaction of information privacy concerns within the context of UTAUT2 relationships offers a more comprehensive understanding of the multifaceted influence of these privacy concerns. This approach transcends the limitations of viewing the multidimensional nature of information privacy concerns through the lens of a single direct impact relationship. Instead, it situates these concerns as a contextual phenomenon, impacting all aspects of the UTAUT2 relationships. This broader perspective enables a deeper insight into the complex interplay between privacy concerns and technology adoption dynamics. Studying the moderation impact of information privacy concerns on the determinant of technology adoption intentions is building upon calls from previous literature, including the insights of Malhotra et al.

(2004), who emphasized the importance of a comprehensive perspective in understanding consumer reactions to information privacy-related issues, and advocated that “researchers should not only focus on consumers' privacy concerns at a general level but also delve into salient beliefs and contextual differences at a specific level” (Malhotra et al., 2004)

The privacy concerns literature acknowledges the existence of such a moderating relationship; for example, Zarouali et al. (2017) specifically examined the moderating role of information privacy concerns on the relationship between targeted advertising and adolescents’ attitudes toward Facebook ads (Zarouali et al., 2017). In healthcare literature, Le et al. (2023) concluded significant information privacy concerns moderation impact on the relationships that shape the adoption of mobile-based advertising technology by customers (Le et al., 2023), and Mirsa et al. (2018) pointed out that information privacy concerns can enhance the influence of perceived usefulness on continuance intention and significantly strengthen the effect of trust on continuance intention towards mobile health applications (Misra et al., 2019).

Therefore, privacy concerns in my study serve as an additional factor related to patients’ concerns about their health information rather than a web-based portal characteristic that directly affects patients’ behavioral intentions towards adopting the healthcare web-based portal. In the following sections of this chapter, I present the hypotheses supporting the moderation effect of information privacy concerns on UTAUT2 predictors of the patients’ intention to use web-based healthcare portals..

2.4.3.1 Performance Expectancy

Individuals with heightened concerns about the privacy of their personal information have an intrinsic apprehension about potential online data breaches involving their personal information (T. T. Smith, 2016). For patients, similar concerns regarding their health information

on web-based healthcare portals can become paramount (Xu & Gupta, 2009). They may recognize the potential benefits and performance of web-based healthcare portals. However, their information privacy concerns can represent a critical factor that can significantly impact the influence of performance expectancy on their intention to use web-based healthcare portals. For example, patients with heightened privacy concerns may have apprehensions about the potential inefficiencies that they could face if they experience a data breach involving their health information within the web-based healthcare portal (Schlackl, Link, & Hoehle, 2022). In this case, the influence of performance expectancy on these patients' intention to adopt web-based healthcare portals may become less important. On the other hand, the intention to use web-based healthcare portals might be significantly positively influenced by the performance expectancy in the case of patients with low privacy concerns. In other words, even when the performance of the healthcare portal is deemed high and beneficial if the privacy concerns are high, the influence of performance expectation is reduced in the case of privacy-concerned patients compared to patients with low privacy concerns, Hence, I hypothesize:

H7: Health Information Privacy Concerns have a negative moderation effect on the relationship between Performance expectancy and intention to use web-based healthcare portals.

2.4.3.2 Effort Expectancy

Similarly, despite recognizing the convenience of web-based healthcare portals, patients' privacy concerns could shadow the influence of the effort expectancy on the patients' intentions to adopt these portals. For example, individuals with concerns about the privacy of their personal information might be uncomfortable with the default or basic privacy settings of web-based portals (Schettino, Fabbricatore, & Caso, 2023). Privacy settings are usually a set of

configuration options that users of online systems can choose from to indicate whether or not they give consent for the collection, use, and disclosure of their personal information (Ibrahim, Blandford, & Bianchi-Berthouze, 2012). Identifying and selecting these privacy settings options are usually additional tasks that privacy-concerned online system users would learn, perform, and validate regularly as systems' features change (Khandelwal, Linden, Harkous, & Fawaz, 2021). Accordingly, for patients with heightened privacy concerns, performing these tasks is a form of privacy concern that might reduce the overall influence of the effort expectancy on their intention to use web-based healthcare portals. For these patients, effort expectancy may not be a very strong influencer of their intentions to use web-based healthcare portals if their concerns about the privacy of their information are strong enough to overshadow the ease-of-use influence on their intentions. In contrast, information privacy concerns might not have similar impact on patients who are less concerned about the privacy of their health information. For those patients, their intention to use web-based healthcare portals might be strongly influenced by their effort expectancy. Therefore, the usually strong impact of effort expectancy on the intention to use web-based healthcare portals may be weakened when privacy concerns are high. Consequently, the following hypothesis is proposed:

H8: Health Information Privacy Concerns have a negative moderation effect on the relationship between Effort Expectancy and Intention to Use Web-Based Healthcare Portals.

2.4.3.3 Social Influence

Slepian et al. (2017) describe a secret as information an individual intentionally hides (Slepian, Chun, & Mason, 2017). This definition applies irrespective of the nature of the information that my be kept secret for various reasons, including privacy(Caughlin & Vangelisti, 2015). Secrecy is inherently a social phenomenon as it always involves at least two parties: the

person holding the secret and those from whom it is either kept or shared (Vangelisti, 1994). Secrets play several crucial roles in social interactions, and they have a significant influence on social relationships (Bedrov, Gable, & Liberman, 2021). Since patients who have privacy concerns regarding their health information are interested in the secrecy of their health information, such patients will likely experience heightened concerns over the social consequences of potential health information exposure due to adopting web-based healthcare portals. This unease is rooted in a complex interplay between the secrecy of personal information and perceived societal pressures in case of personal information exposure.

Accordingly, in the case of web-based healthcare portals, patients' fear of potential health information exposure and the resulting impact of such exposure on patients' social relationships can greatly reduce the persuasive power of patients' social networks. This fear is not unfounded, as the consequences of compromised health information can range from social stigma to discrimination (Stangl et al., 2019). The apprehension surrounding these potential outcomes can significantly undermine the otherwise positive role of social influence in encouraging the adoption of web-based healthcare portals. Consequently, the raised privacy concerns may reduce the impact of robust social encouragement or recommendations. Alternatively, the likelihood of embracing such portals is noticeably higher when privacy concerns are less pronounced.

This leads to the formulation of the following hypothesis:

H9: Health Information Privacy Concerns have a negative moderating effect on the relationship between Social Influence and the Intention to Adopt Web-Based Healthcare Portals.

2.4.3.4 Facilitating Condition

Similarly, Patients with higher privacy concerns about their health information may perceive a need for extra protective measures when considering the adoption of web-based healthcare portals (Chen, Beaudoin, & Hong, 2017). This perception can adversely modulate the influence of facilitating conditions, the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system (Venkatesh et al., 2016). Even when facilitating conditions, such as user support and system compatibility, are favorable, these heightened privacy concerns might lead patients to believe that additional protective measures are necessary. For example, they may feel the need to implement extra virus or spam protection tools or seek more advanced encryption methods for their data. This belief that extra layers of privacy protections are required is just an example of how privacy concerns can diminish the positive impact of the facilitating conditions on patients' intention to adopt the healthcare portal. So, while existing infrastructure might be supportive, privacy concerns can create a barrier, reducing the impact of the facilitating condition on the intention to adopt web-based healthcare portals compared to scenarios where privacy concerns are less pronounced. Hence:

H10: Health Information Privacy Concerns have a negative moderation effect on the relationship between Facilitating conditions and intention to use web-based healthcare portals.

2.4.3.5 Hedonic Motivation

The hedonic motivation was previously examined in research as an internal utility contributing to a technology's overall appeal (Van der Heijden, 2004). In the context of the impact of privacy concerns on the relationship between hedonic motivation and the intention to

use web-based healthcare portals, privacy concerns can indeed be argued as a utility reducer. While hedonic motivation typically enhances the perceived utility of technology by making its use pleasurable or enjoyable, privacy concerns can significantly reduce the effect of this relationship.

When patients have high privacy concerns, the enjoyment and satisfaction derived from using the healthcare portal (the essence of hedonic motivation) are overshadowed by concerns about data privacy. This anxiety acts as a utility reducer because it reduces the strength of the overall impact of the appeal relationship. The privacy concerns undermine the impact of the enjoyment on patients' intention to use the web-based healthcare portal.

Therefore, in scenarios where privacy concerns are high, the utility of the healthcare portal, as perceived by the patients, is reduced. This reduction in perceived utility due to privacy concerns weakens the influence of hedonic motivation on the intention to use he web-base healthcare portals. The end result is that, despite the inherent enjoyment and satisfaction the portal could provide, its overall appeal is lessened in the eyes of patients worried about their privacy, thus affecting their willingness to adopt and use the technology.

H11: Health Information Privacy Concerns have a negative moderation effect on the relationship between Hedonic Motivation and intention to use web-based healthcare portals.

2.4.3.6 Habit

In the context of web-based healthcare portals, 'habit' refers to patients' automatic and repeated use of these portals, a behavior pattern formed by past experiences (Ivanov, 2008). However, this habitual usage can be disrupted when patients become aware of privacy breaches within the healthcare sector (Wairimu & Fritsch, 2022). High-profile incidents, such as unauthorized access to patient records or the hacking of healthcare databases, gain significant

media attention and heighten concerns over the privacy of personal health information (Seh et al., 2020). The awareness of these breaches can diminish the habitual influence on the adoption level of web-based healthcare portals.

Moreover, if a patient has personally suffered a data breach in other technological contexts, this negative experience can profoundly erode their trust in digital platforms, intensifying their concerns regarding the privacy of health information on healthcare portals. Such personal experiences with breaches significantly diminish the role of habit in shaping a patient's intention to adopt web-based healthcare portals. When privacy concerns are elevated through personal experiences or publicized incidents, patients are likely to reassess the influence of their habits on their technology-related intentions and decisions, particularly in sensitive areas like health information. Consequently, in these scenarios, the typically automatic habit of using web-based healthcare portals may be overridden by privacy concerns, impacting the adoption and use of healthcare portals.

H12: Health Information Privacy Concerns have a negative moderation effect on the relationship between Habit and intention to use web-based healthcare portals.

CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY

This chapter explains the research model and methodological strategies that I will employ to pursue the research objectives. It commences with delineating the overarching research design, the selection of participants, and the rationale for sample size determination. The chapter then delves into the data collection and instruments used to collect the data. Furthermore, the section explains the research variables and constructs, encompassing independent, dependent, moderating, and control variables. Finally, I outline the statistical tools and analytical techniques I plan to use for data analysis. Together, these elements construct a robust methodological foundation for this dissertation.

3.1 Overview

In this qualitative research, I will adhere to a comprehensive set of research methodological recommendations, which include clearly defining variables and measures, selecting appropriate statistical techniques, meticulous data preprocessing, ensuring adequate sample size, and abiding by the assumptions underlying statistical tests (Creswell & Creswell, 2017). These thorough efforts facilitate the rigorous and systematic analysis of quantitative data that will be used in this research and safeguard the credibility and reliability of the research outcomes. By following these recommendations, I aim to enhance the validity and robustness of my findings, ensuring that they withstand scrutiny and contribute substantively to the existing body of knowledge in my field and fostering confidence in the results and their potential implications for both academia and practical applications. Following the approach extensively employed by researchers in information systems (Bervell et al., 2022; Meet, Kala, & Al-Adwan, 2022), data privacy (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2021; Ioannou et al.,

2021), and healthcare fields (Duarte & Pinho, 2019; Yuan, Ma, Kanthawala, & Peng, 2015), I employ a survey instrument to collect structured data that I plan to use in my analyses.

3.2 Sample

Sample size determination for this study was conducted using GPower analysis, a widely recognized software tool for power and sample size calculations (Faul, Erdfelder, Lang, & Buchner, 2007). In the context of a regression analysis with six predictor variables, the chosen statistical test type was regression. With an effect size of 0.35, a significance level (alpha) of 0.05, and a desired power of 0.8, the recommended sample size was computed. GPower estimated that a sample size of 120 participants would be necessary to detect the specified effect size with the desired level of power and significance. These calculations were based on established statistical principles and considerations, ensuring that the study would have an adequate sample size to draw meaningful conclusions.

3.3 Data Collection

This study will be conducted within the United States, with a focus on examining patients who have encountered web-based healthcare portals and whether or not they opted to utilize them. To gather comprehensive data, an online questionnaire will be administered through the Qualtrics online tool.

Qualtrics is a versatile and widely recognized online survey tool that offers a plethora of tools for conducting academic research (Belliveau, Soucy, & Yakovenko, 2022). The questionnaire instrument utilized in this research was adopted from previous literature and carefully tailored to suit the specific objectives and context of this study (Appendix). Drawing upon established scales and items from prior research (Dwivedi et al., 2016; Fox & Connolly, 2018), I sought to leverage the reliability and validity of existing instruments while ensuring

their alignment with the research's unique focus. The questionnaire is adjusted to make it contextually relevant and responsive to the healthcare web-based portal context regarding the impact of information privacy concerns on the UTAUT2 model relationship.

The Qualtrics survey distribution options, including email invitations and anonymous response collection, cater to the specific needs of my academic research, ensuring data integrity and participant anonymity. Given the widespread deployment of web-based healthcare portals by healthcare providers in the U.S., particularly in the aftermath of the COVID-19 pandemic (Mheidly & Fares, 2020), I anticipate a substantial proportion of survey recipients to have encountered these portals.

The survey will collect data from participants, focusing on their concerns related to health information privacy and their intentions regarding the adoption of web-based healthcare portals. This approach allows for efficient data collection and ensures that a diverse range of patients who encountered web-based healthcare portals can be reached. By conducting the study in the U.S. and utilizing a popular online survey format, the research aims to provide valuable insights into the dynamics of the interaction between patient information privacy concerns and their intention to adopt web-based healthcare portals.

3.4 Measures

The questionnaire for this research is based on established constructs that were adapted to the context of a web-based healthcare portal. The questionnaire consists of three primary sections: demographic information, UTAUT constructs, and information privacy concerns construct.

3.4.1 Demographic Information

Within this section, we gather demographic information encompassing variables such as age, gender, computer, and Internet experience. These variables are meticulously collected to serve as control variables in our study in alignment with the recommendations of Venkatesh et al. (2012). The purpose of collecting this data is to examine and account for potential variations in participants' responses that may be attributed to these demographic factors.

By including these control variables, we aim to isolate the effects of information privacy concerns and other independent variables, allowing us to better understand their unique impact on technology adoption behavior. This comprehensive approach ensures that our analysis takes into account any potential confounding factors, thus enhancing the robustness and validity of our research findings.

3.4.2 UTAUT2 Constructs

This section includes Likert-scale questions assessing the UTAUT constructs. Respondents are asked to rate their agreement with statements related to the acceptance of technology in web-based healthcare portals.

The primary dependent variable, "Intention to use web-based portals," serves as a critical focal point in this research and is assessed through a construct adapted from Dwivedi, Shareef, and Simintiras (2016). This construct has been carefully chosen for its proven reliability and validity in capturing users' intentions in the context of technology adoption. Participants in the study will be asked to provide ratings indicating the extent of their intention to engage with the web-based healthcare portal, thereby quantifying their willingness to adopt and use this technological solution.

The construct, extracted from Dwivedi et al.'s work, encompasses seven distinct dimensions thoughtfully designed to gauge different dimensions of users' intentions. The items measuring these dimensions have been tailored to fit the specific context of this research and are included in Appendix for reference. The items will be measured by a five-point Likert scale ranging from 1(strongly disagree) to 5 (strongly agree).

By employing this multi-item construct, I aim to capture the nuances and complexities associated with users' intentions, allowing for a comprehensive assessment of their readiness to embrace the web-based healthcare portal. This approach ensures that my measurement of intention is both robust and sensitive to the various factors that may influence participants' web-based healthcare portals assessment within the healthcare technology adoption landscape.

All the independent variables in this study have also been selected and adapted from Dwivedi, Shareef, and Simintiras (2016) and will be measured by five-point Likert scales ranging from 1(strongly disagree) to 5 (strongly agree). For instance, the first independent variable, *Performance Expectancy*, consists of four items thoughtfully tailored to capture distinct facets of performance expectations (see Appendix). Participants will be asked to provide ratings that reflect their perceptions of how well the web-based healthcare portal is expected to perform in facilitating their healthcare-related tasks.

Similarly, the second independent variable, *Effort Expectancy*, comprises four items. Respondents will be prompted to evaluate the perceived ease of use and effort required to interact with the web-based portal, reflecting their expectations in this regard. The third independent variable, *Social Influence*, assesses the impact of social factors on users' intentions. This construct is comprised of three items and will help me understand how the influence of others within users' social networks shapes their decision to adopt the technology. The fourth

independent variable, *Facilitating Conditions*, evaluates the extent to which participants believe that they have the necessary resources and support to use the web-based healthcare portal effectively. This construct involves four items, providing a comprehensive view of participants' perceptions of facilitating conditions.

The fifth independent variable, *Hedonic Motivation*, focuses on users' emotional and experiential aspects related to using the portal. This construct includes three items that capture users' feelings of enjoyment and pleasure associated with the technology. Lastly, the sixth independent variable, *Habit*, includes four items and aims to assess the extent to which users have developed habitual patterns of engaging with the technology.

These adapted constructs, each comprising multiple items, provide a comprehensive scale for assessing the various dimensions of users' perceptions and intentions within the context of web-based healthcare portal adoption. They have been used in similar research contexts and established for their relevance and effectiveness in capturing the intricate interplay of factors influencing users' adoption behaviors.

3.4.3 Health Information Privacy Concerns Construct

The measurement of health information privacy concerns is of paramount importance, as it serves as a central construct that underpins the research. To assess health information privacy concerns comprehensively, thoughtfully selected to capture the multifaceted nature of information privacy concerns responses and adjusted to the healthcare web-based portal context.

The *Collection* dimension consists of four items, measuring participants' apprehensions related to the initial gathering of their health information. The *Secondary Use* dimension consists of three items and measures participants' worries regarding the subsequent utilization of their health information beyond its primary purpose. The three items' *Improper Access* dimension

measures participants' concerns regarding unauthorized or inappropriate individuals gaining access to their health information. The *Errors* dimension comprises three items that measure participants' anxieties regarding the accuracy and integrity of their health information. The *Control* dimension measures participants' perceptions of their ability to manage and regulate access to their health information. With three items, this dimension investigates the extent to which individuals feel they can maintain control over their sensitive data. Finally, the *Awareness* dimension encompasses three dimensions and measures participants' levels of knowledge and awareness regarding the handling of their health information. By including three items in this dimension, we seek to understand how well-informed participants are about data privacy practices.

To gauge participants' responses within each of these dimensions, a Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) will be utilized. Overall, this measurement approach ensures a thorough examination of the multifaceted nature of health information privacy concerns, providing valuable insights into participants' perceptions and anxieties within the context of healthcare technology adoption.

3.5 Data Analysis

3.5.1 Data Cleaning and Composite Measure Construction

Once the data collection phase is completed, meticulous data cleaning procedures will be implemented. Data cleaning involves a systematic process of identifying and rectifying any inconsistencies, errors, or outliers within the dataset. This rigorous step will ensure the accuracy and reliability of the collected data.

Subsequently, we will proceed to construct composite average measures for each variable in our study. This process involves aggregating individual item responses within each variable to

create an overarching composite score. These composite measures serve as a concise representation of participants' responses to a particular variable.

By employing this approach, we generate an overall average measurement for each variable, offering a consolidated and meaningful representation of participants' perceptions, attitudes, and intentions. These composite measures facilitate a more comprehensive analysis, allowing us to delve into the intricate relationships between variables and gain a deeper understanding of the research phenomenon.

3.5.2 Statistical Analysis

Data collected from the survey will be subjected to analysis using the Statistical Package for the Social Sciences (SPSS). Descriptive statistics, correlation analysis, and hierarchical regression analysis will be employed. This hierarchical regression analysis will assess whether information privacy concerns moderate the UTAUT2 relationships by including moderation terms in the models.

3.6 Ethical Considerations

Ethical considerations regarding data privacy, informed consent, and participant anonymity are paramount throughout the research process. The study adheres to all relevant data protection regulations and guidelines.

CHAPTER 4: RESULTS

This chapter outlines the survey results and the data analysis in a step-by-step format. It starts with a preliminary review that includes a basic sample review and a description of the techniques I use to analyze the survey data. Then, a reliability check, using Cronbach's Alpha, is described to ensure the survey scales are consistent and reliable. After the reliability of the measures is discussed, the results of the multiple regression analysis to test the study hypotheses are explained. The chapter ends with a comprehensive explanation of what was discovered through the data analysis.

4.1 Survey and Data Collection

Data collection for this research was facilitated through the utilization of a questionnaire instrument. The questionnaire was administered via the Qualtrics survey platform. Invitations to participate were distributed to approximately 3100 individuals selected from the Prolific platform, specifically targeting users of healthcare technology. The invitations contained links that directed the participants to the Qualtrics survey platform to provide their responses to the questionnaire questions. To ensure eligibility, participants were required to meet the participation criteria, being 18 years or older, residing in the U.S., and voluntarily have used web-based healthcare portals. The survey was designed to terminate the participants who provided answers that did not meet the participation criteria. After completing the participation criteria questions, eligible participants were allowed to start answering the survey questions. I leveraged the capabilities of the Prolific Academic platform to collect the responses. The initial phase involved identifying a suitable participant pool; this was accomplished by accessing the platform and selecting a pre-determined group of participants. Specifically, a pool of 3,100 members, each with a professed experience in healthcare technology. This pool of participants was already

provided by Prolific, which created this pool based on detailed profiles provided by the participants at the time of their registration on Prolific. Subsequently, in alignment with the research requirements and following a power analysis—coupled with consultations with Dr. Franz—a decision was made to solicit a total of 300 responses. This figure was not only above the minimum suggested by the power analysis but was also deemed sufficient to augment the study's analytical depth. To this end, the Prolific tool was configured to offer monetary compensation to the first 300 respondents out of the 3100 recipients. The distribution phase saw the questionnaire distributed to the identified pool of healthcare technology users—3100 recipients—accompanied by the invitation to participate in the research. Monitoring the responses was an ongoing task conducted in real-time through the platform, which was adept at automatically limiting acceptance to the first 300 completed questionnaires, adhering to the pre-set study parameters. After the initial 300 responses were collected, a review process was undertaken to ensure each response met the defined research criteria. This entailed assessing the completeness of each submission and its adherence to the expected average response time. Submissions that were hastily completed or that lacked necessary information were rejected. In instances where responses were disqualified, the Prolific platform reopened the survey to additional participants from the same predefined pool. This iterative process continued until 300 responses of satisfactory quality were secured. The final stage of data collection entailed a careful evaluation of the approved responses, which excluded two additional submissions that were later deemed insufficient for the research needs. The survey was structured to mandate the completion of all questions, resulting in no missing data in the received 298 completed responses.

4.2 Descriptive Statistics and Reliability Analyses

This section provides in-depth descriptive and reliability analyses of the dependent, independent, and moderator variables essential to my study. By meticulously examining each variable, I aim to explain the reliability of the study's constructs in addition to the variables' central tendencies, variability, and distributional characteristics. This comprehensive exploration lays the groundwork for a nuanced understanding of my dataset, facilitating informed interpretations and subsequent analyses within my research.

4.2.1 Demographic and Control Variables

Participants' ages were categorized into age groups, as detailed in Table 2. The majority of participants, comprising 39.3%, fell within the 25 to 34-year-old category, making it the mode of the data. Subsequently, 29.5% of participants were aged between 35 and 44 years, while 19.5% fell within the 45 to 54-year-old range. Participants older than 55 years accounted for only 11.8% of the total, with no participants exceeding the age of 75. The data exhibited a normal distribution, with a skewness value of 0.476 and a skewness standard error of 0.141. The prevalence of participants in the 25 to 34 age range, coupled with the lower representation in older age groups, may contribute to the findings discussed in the forthcoming sections.
Nearly equal representation of male and female participants was observed in the collected data, with 153 males and 145 females participating.

Table 2: Age distribution

Age Range	Frequency	Percent	Valid Percent	Cumulative Percent
18-24	21	7.0	7.0	7.0
25-34	96	32.2	32.2	39.3
35-44	88	29.5	29.5	68.8
45-54	58	19.5	19.5	88.3
55-64	27	9.1	9.1	97.3
65-74	8	2.7	2.7	100.0
Total	298	100	100	

Participants' Internet experiences were classified into experience groups, as outlined in Table 3. The predominant group, constituting 89.6% of participants, possessed 15 or more years of experience, establishing it as the mode of the data. Following this, 8.4% of participants reported having between 10 and 15 years of experience. A mere 2% of participants indicated having less than 10 years of experience, with only one participant reporting less than 5 years of internet experience.

Table 3: Internet Experience

	Frequency	Percent	Cumulative Percent
Less than 5 years	1	.3	.3
5 – 10 years	5	1.7	2.0
10 – 15 years	25	8.4	10.4
15 + years	267	89.6	100.0
Total	298	100.0	100.0

4.2.2 Dependent Variable

To measure the dependent variable, intention to use web-based healthcare portals, I employed a 3-item, 5-point Likert scale adapted from Dwivedi, Shareef, and Simintiras (2016). Respondents were asked to rate their agreement on a scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). A reliability analysis was conducted to assess the consistency of the multi-item scale, employing the coefficient alpha as a measure of scale reliability. Alpha values can vary between 0.0 and 1.0, with values below 0.70 considered undesirable (Peterson & Kim, 2013). Utilizing SPSS, the alpha value for the scale was found to be .810, surpassing the 0.70 threshold and indicating acceptable internal consistency among the items. A composite variable was derived using SPSS, aggregating the three items through the calculation of their mean, thereby facilitating a consolidated representation of the construct under investigation in accordance with established methodological practices.

The composite variable was assessed for normal distribution, revealing a skewness of -0.47 and a kurtosis of -0.0576. Skewness values close to zero suggest approximately symmetrical distributions, with negative values indicating a slight leftward skew. Similarly, kurtosis values near zero suggest a mesokurtic distribution, with negative values indicating slightly less peakedness compared to a normal distribution. Furthermore, visual inspection of the variable values supports the assumption of normality, bolstering confidence in the statistical analysis.

4.2.3 Independent Variable

All independent variables in this study were sourced and adapted from Dwivedi, Shareef, and Simintiras (2016), employing five-point Likert scales ranging from 1 (strongly disagree) to 5 (strongly agree). Appendix delineates the multi-item scales utilized to assess the independent variables. For example, the initial independent variable, Performance Expectancy, comprises four items gauging participants' beliefs regarding their performance expectations of the web-based healthcare portal. The scale's alpha coefficient yielded a value of .844, exceeding the 0.70 threshold and indicating satisfactory internal consistency among the items. Likewise, the reliability analyses conducted on all other independent variables indicate acceptable internal consistency, as evidenced by their Cronbach's Alpha values exceeding 0.8, as presented in Table 4. A composite variable creation process was undertaken for all six independent variables, where composite variables were generated using SPSS. This involved aggregating the respective items through the computation of their mean, thereby creating integrated representations of each construct in line with recognized methodological methods.

The results of skewness and kurtosis analyses for all six independent variables collectively suggest a normal distribution. Skewness values close to zero (ranging from -0.769 to 0.339) indicate relatively symmetrical distributions, with none exceeding the threshold of ±2 for

significant skewness. Additionally, kurtosis values (ranging from -0.281 to 1.097) are near zero, suggesting moderate peakedness compared to a normal distribution, but well within the acceptable range. These findings are further corroborated by visual inspection of plot diagrams for each variable, which visually confirm the assumption of normal distribution. Refer to Table 6 for detailed skewness and kurtosis values for each independent variable.

Table 4: Reliability and distribution – Independent variables

Independent Variable	Number of items	Cronbach's Alpha	Skewness	Kurtosis
Performance Expectation	4	0.844	-0.769	0.686
Effort Expectancy	4	0.831	-0.690	0.611
Social Influence	3	0.926	-0.224	0.050
Facilitating Condition	4	0.703	-0.618	1.097
Hedonic Motivation	3	0.912	0.146	0.349
Habit	4	0.781	0.339	-0.281

4.2.3 Moderator Variable

The Health Information privacy concerns, utilized as a moderator variable in this study, are adapted from the research conducted by Fox and Connolly (2018). This construct comprises six distinct dimensions: Collection, Secondary Use, Improper Access, Errors, Control, and Awareness, each consisting of multiple items. A reliability assessment was conducted for all dimensions to evaluate the internal consistency of the measure, employing Cronbach’s alpha coefficient, as illustrated in Table 5. The reliability analyses conducted on all dimensions demonstrate satisfactory internal consistency, with Cronbach's Alpha values surpassing 0.8. Employing a procedure akin to the previous composite process, composite values were computed for each dimension using SPSS. Skewness and kurtosis analyses for all six composite variables suggest normal distribution, with skewness values ranging from -0.711 to 0.249 and kurtosis values from -1.148 to -0.149. Visual inspection of plot diagrams also supports this conclusion. Detailed results are provided in Table 5.

Table 5: Reliability and distribution – Moderator variable

Dimension	Number of items	Cronbach's Alpha	Skewness	Kurtosis
Collection	4	0.923	0.249	-0.891
Secondary Use	3	0.937	-0.268	-1.148
Improper Access	3	0.944	-0.332	-0.943
Errors	3	0.887	-0.094	-0.843
Control	3	0.895	-0.477	-0.735
Awareness	3	0.857	-0.711	-0.149

Subsequently, an overall Mean-calculated composite value was derived to represent the moderator variable comprehensively.

4.2.4 Common Method Bias

Given that this study relies on self-reported data obtained through a survey questionnaire, it was imperative to assess for common method bias, ensuring that any variability in the data primarily stems from measurement methods rather than the underlying constructs. Harman's single-factor test was employed for this purpose, aiming to identify and confirm the absence of bias caused by a single factor explaining more than half of the variance in exploratory factor analysis. This test involved subjecting all items of the model's variables (eleven factors, encompassing three control variables, six independent variables, one mediator, and one dependent variable) to factor analysis to ascertain the number of factors generated and the proportion of variance accounted for. The results revealed the emergence of four variables which collectively explained 68.94% of the variance, with the first factor alone elucidating 38.17%. This outcome suggests that common method bias is not a significant concern in this study (Podsakoff & Organ, 1986).

4.3 Correlation Analysis

The correlation analysis presented in Table 6 reveals several key findings regarding the relationships among the model variables. Firstly, the correlation matrix demonstrates positive

correlations among the six independent variables, with coefficients ranging from .332 to 0.703, all statistically significant at the 0.01 level ($p < .01$). This correlation among the independent variables of the UTAUT2 model is anticipated and aligns with prior research, as each predictor is expected to contribute to technology adoption positively. Moreover, the correlation strength among five out of the six independent variables remains below 0.7, indicating less possibility of redundancy in their measurement. Notably, the one strong positive correlation (correlation coefficient = 0.703) between effort expectancy and facilitating conditions is expected, given that individuals who anticipate low effort in using web-based healthcare portals often perceive that they have access to conditions facilitating their seamless use.

Second, The correlation matrix shows a positive correlation between the six independent variables and the dependent variable with coefficients ranging from .438 to 0.632, all statistically significant at the 0.05 level ($p < .05$) or beyond. A positive correlation between the independent variables and the intention to adopt web-based healthcare portals aligns with the UTAUT2 theory and the result of previous research. According to the UTAUT2 framework, performance expectancy, effort expectancy, social influence, facilitating condition, hedonic motivation, and habit positively influence individuals' intentions to adopt the technology. These predictors are rooted in established psychological theories such as the Technology Acceptance Model (TAM), which posits that perceived usefulness and ease of use are key determinants of technology adoption. Previous research in various contexts has consistently demonstrated the positive relationship between these predictors and technology adoption, further supporting my study's hypothesis of positive relationships.

Third, a negative correlation exists between health information privacy concerns and intention to use web-based healthcare portals ($r= -0.323$, $p < .01$). The negative correlation

between individuals' health information privacy concerns and their intention to adopt web-based healthcare portals reflects an expected aspect of individuals' behavior in technology adoption processes. Individuals with higher levels of information privacy concerns are likely to exhibit lower intentions to adopt web-based healthcare portals, as their apprehensions regarding data collection, access, control, secondary use, awareness, and error may deter them from engaging with such web-based portals.

Finally, no noteworthy correlation findings were identified regarding the relationship between the control and the remaining model variables.

Table 6: Descriptive Statistics and Bivariate Correlations

	Mean	SD	1	2	3	4	5	6	7	8	9	10	11
Age	2.99	1.186	1										
Gender	0.51	0.501	-.028	1									
Internet exp	3.87	0.434	.103	.031	1								
Perf Expectancy	4.0856	0.6894	.086	-.037	.021	1							
Effort Expectancy	4.1233	0.6472	.043	-.025	.136*	.589**	1						
Social Influence	3.4698	0.8808	.100	.098	.006	.516**	.344**	1					
Facilitated Condition	4.1653	0.5513	.093	-.046	.091	.650**	.703**	.405**	1				
Hedonic Motivation	2.9407	0.9979	.057	.005	-.098	.374**	.398**	.395**	.332**	1			
Habit	2.7919	0.9019	.112	-.087	-.066	.450**	.332**	.539**	.323**	.599**	1		
Privacy Concerns	3.0739	0.9557	-.020	-.105	.034	-.427**	-.371**	-.281**	-.348**	-.267**	-.207**	1	
User Int WBHP	3.7248	0.80471	.150**	-.127*	.089	.632*	.540**	.512**	530**	.438**	.661**	-.323**	1

** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).
C.Listwise N= 298

4.4 Regression Analysis

Regression analysis is employed as the primary statistical method to investigate the moderating effect of health information privacy concerns on the dependent variable, "intention to use web-based healthcare portals". This analytical approach is particularly suited for my study due to its robust capacity to not only explore direct relationships between independent and dependent variables but also to examine how these relationships change under the influence of a moderating variable, in this case, privacy concerns. The study adopts a methodical approach by proceeding through multiple regression models, where different sets of variables are systematically added at each stage. The regression analysis employed in my research and summarized in Table 7 unfolds across four sequentially developed models.

The regression analysis results across all models indicate the absence of multicollinearity among the variables, as evidenced by the tolerance, Variance Inflation Factor (VIF), and condition index values, which all fall below commonly accepted thresholds for concern. Specifically, tolerance levels range from 0.768 to 0.991, comfortably above the threshold for concern with a value below 0.1, suggesting that independent variables are not explained by the other independent variables in the model, and each variable independently contributes a significant amount of new information. VIF values are maintained below 3, far from the threshold that typically indicates multicollinearity concerns, implying a low level of redundancy among predictors. Furthermore, the maximum condition index observed is 29.801, just under the critical threshold of 30, indicating that the predictor variables do not exhibit high collinearity levels.

Table 7: Regression Analysis

Variables	Model 1	Model 2	Model 3	Model 4
	β	β	β	β
Control				
Age	.094*	.033	.034	.038
Gender	-.202*	-.128*	-.136*	-.162**
Participant Experience	.147	.143*	.149*	.113
Independent variables				
Zscore: Performance Expectation		.206**	.195**	.107*
Zscore: Effort Expectation		.135**	.129**	.197**
Zscore: Social Influence		.058	.056	.065
Zscore: Facilitating Condition		.057	.056	.066
Zscore: Hedonic motivation		-.030	-.033	-.015
Zscore: Habit		.356**	.359**	.344**
Moderating variable				
Zscore: Privacy Concerns			-.037	-.030
Interaction effect				
Zscore: Privacy Concerns* Zscore: Performance				.137**
Zscore: Privacy Concerns* Zscore: Effort Expectation				-.182**
Zscore: Privacy Concerns* Zscore: Social Influence				-.039
Zscore: Privacy Concerns* Zscore: Facilitating				.050
Zscore: Privacy Concerns* Zscore: Hedonic motivation				-.038
Zscore: Privacy Concerns* Zscore: Habit				.061
R	.209	.792	.793	.811
R^2	.044	.628	.629	.657
Adjusted R^2	.034	.616	.616	.638
ΔR^2	.044	.584	.002	.028
F change	4.485*	75.277**	1.230	3.812**
F	4.485*	53.946**	48.713**	33.665**

Significant at: ** $p < 0.001$ * $p < 0.05$

Initially, Model 1 establishes a foundational regression model incorporating the control variables (Internet experience, Participants' gender, and Age categories). The regression results show that the model provides a modest explanation of only 4.4% of the variance in the dependent variable, which, despite its small magnitude, is statistically significant (p=.004). Model 1 presents an F value of 4.485 with a significance level of .004. This indicates that, collectively, these control variables significantly predict the dependent variable, albeit explaining a relatively small portion of the variance (R^2 = .044). The statistical significance suggests that

there is a foundational relationship worth exploring further, even if the effect size is modest at this stage.

Advancing to Model 2, I include the independent variables (performance expectancy, hedonic motivation, social influence, effort expectancy, habit, and facilitating conditions) to the regression model. Model 2 markedly enhances the model's explanatory power explain 62.8% of the variance in the dependent variable (R^2 =0.628, p<.001). This significant increase underscores the critical role of independent variables in influencing the individual's intention to use web-based healthcare portals. This model dramatically increases in explanatory power, as reflected by an F value of 53.946 and a highly significant p-value (< .001). The considerable rise in both the F value and the R2 demonstrates that the variables incorporated in Model 2 - namely, performance expectancy, effort expectancy, and habit - exert a noteworthy and meaningful influence on the dependent variable. This is evidenced by their statistically significant coefficients at the p level < 0.001. Such findings provide strong support for hypotheses 1, 2, and 3.

The subsequent model adds the moderator variable (health information privacy concerns) to the regression analysis. Model 3 yields a negligible increase in the dependent variable's explained variance (R^2 =0.629). Although incorporating privacy concerns into the analysis resulted in a slight increase in the R^2 to .629, the F value for this change is 1.230 with a p-value of .268, indicating that adding privacy concerns alone does not significantly enhance the model's explanatory power over and above the variables already included in Model 2. This suggests that while privacy concerns are important, their direct impact on individuals' intention to adopt web-based healthcare portals may be less pronounced without considering their interaction with other factors. This finding is important as it supports this study's proposition that health information

privacy concerns are not a direct antecedent of an individual's intentions to adopt web-based healthcare portals.

Model 4 represents a pivotal development in the analysis by incorporating interaction terms to assess the moderating effects of privacy concerns. This model reveals a more substantial portion of the variance (R2 =0.657), with the increase from the previous model (ΔR2 =0.028) being statistically significant (p=.001). This reinforces the validity of the interaction effects. This model explains 65.7% of the variance in the dependent variable, which is a 2.8% increase compared to the previous model. The F value for this model is 33.665 with a significance level of < .001, signaling a significant relevance of the improvement in the model's capacity to explain the variance in the dependent variable. The increase in both the F value and R Square, compared to Model 3, underscores the critical importance of examining the interactions between privacy concerns and the independent variables. This model robustly confirms that privacy concerns has a form of moderating effect on the relationship between performance expectancy, effort expectancy, and individuals' intention to adopt web-based healthcare portals. Specifically, the analysis of coefficients in Model 4 highlights the exact moderating role of privacy concerns and suggests support for hypotheses 7 and 8. The interaction between privacy concerns and performance expectancy is positively significant (B=0.137, p=.002), indicating that the effect of performance expectancy on individuals' intention to use web-based healthcare portals is strengthened under higher privacy concerns. The interaction plot provided in Figure 2 below offers a visual representation of this effect. The graph depicts two separate slopes corresponding to low and high health information privacy concerns, intersecting with performance expectancy on the x-axis and the intention to adopt web-based healthcare portals on the y-axis. For low health information privacy concerns, the slope reveals a more gradual decrease in the intention to

adopt web-based healthcare portals with rising performance expectancy. In contrast, the slope associated with high health information privacy concerns exhibits a sharp increase, indicating that the intention to adopt web-based healthcare portals escalates significantly as performance expectancy grows in the context of high health information privacy concerns.

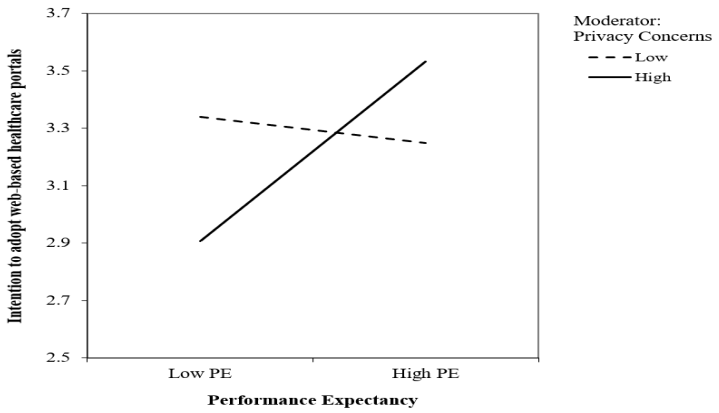

Figure 2: Interaction Plot for the moderating effect of Privacy Concerns on Perf Expectancy

This outcome diverges from my hypothesis that healthcare information privacy concerns would negatively modulate the positive influence of performance expectancy on the intention to adopt web-based healthcare portals. This outcome will be explored in greater detail in the upcoming discussion chapter.

The analysis of coefficients in Model 4 also highlights the statistically significant negative coefficient for the interaction between privacy concerns and effort expectancy ($B=-0.182$, $p<.001$), suggesting that increasing privacy concerns diminishes the positive impact of effort expectancy on individuals' intention to use web-based healthcare portals. The

interaction plot provided in figure 3 below offers a visual representation of this effect.

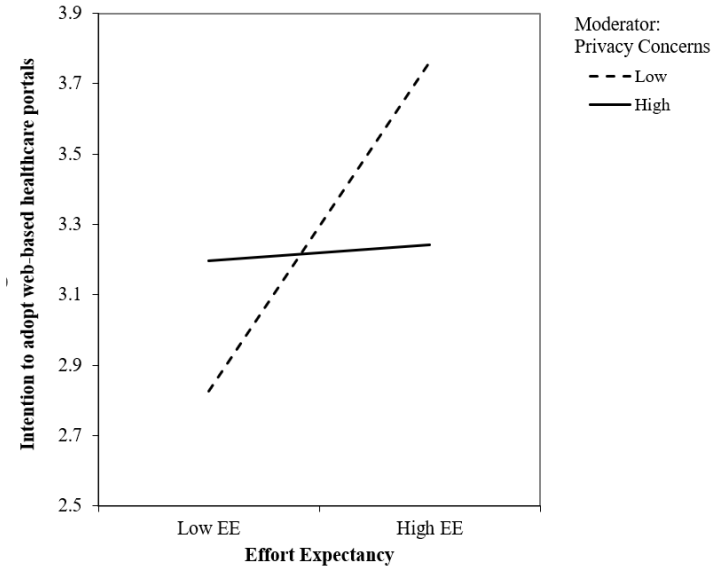

Figure 3: Interaction Plot for the moderating effect of Privacy Concerns on Efrt Expectancy

For low health information privacy concerns, the slope demonstrates a steep increase in the intention to adopt web-based healthcare portals alongside rising effort expectancy. This indicates that low health information privacy concerns amplify the positive correlation between effort expectancy and the intention to use web-based healthcare portals. Conversely, the slope corresponding to high health information privacy concerns shows a more moderate increase, suggesting that the intention to adopt web-based healthcare portals grows only modestly with increasing effort expectancy in scenarios of high health information privacy concerns. This modest incline is attributed to health information privacy concerns dampening the positive relationship between effort expectancy and intention to adopt.

As discussed in the previous chapter, the employment of regression analysis is the cornerstone statistical methodology in this research to validate the research hypotheses. As detailed in the preceding sections, the comprehensive interpretation of the regression models—ranging from basic control variables influences to the detailed examination of moderating

effects—provides a solid foundation for confirming or rejecting the hypothesized relationships. Table 8 displays the conclusion regarding the support or rejection of these hypotheses.

Table 8: Hypotheses

	Hypothesized Relationship	Result
Direct Effect		
H1	Performance expectancy is positively associated with the intention to use a web-based healthcare portal.	**Supported**
H2	Effort expectancy is positively associated with the intention to use web-based healthcare portals	**Supported**
H3	Social influence is positively associated with the intention to use web-based healthcare portals	Not Supported
H4	Facilitating conditions is positively associated with the intention to use web-based healthcare portals	Not Supported
H5	Hedonic Motivation is positively associated with the intention to use web-based healthcare portals	Not Supported
H6	Habit is positively associated with the intention to use web-based healthcare portals	**Supported**
Moderating Effect		
H7	Health Information Privacy Concerns have a negative moderation effect on the relationship between Performance expectancy and intention to use web-based healthcare portals.	Not Supported
H8	Health Information Privacy Concerns have a negative moderation effect on the relationship between Effort Expectancy and Intention to Use Web-Based Healthcare Portals.	**Supported**
H9	Health Information Privacy Concerns have a negative moderating effect on the relationship between Social Influence and the Intention to Adopt Web-Based Healthcare Portals.	Not Supported
H10	Health Information Privacy Concerns have a negative moderation effect on the relationship between Facilitating conditions and intention to use web-based healthcare portals.	Not Supported
H11	Health Information Privacy Concerns have a negative moderation effect on the relationship between Hedonic Motivation and intention to use web-based healthcare portals.	Not Supported
H12	Health Information Privacy Concerns have a negative moderation effect on the relationship between Habit and intention to use web-based healthcare	Not Supported

CHAPTER 5: DISCUSSION AND CONCLUSION

This chapter discusses the research findings, limitations, contributions, implications for practice and future research, and a conclusion.

5.1 Interpretation of Key Findings

Previous studies have utilized various theoretical frameworks to explore how privacy concerns affect individuals' intentions to adopt and use technologies. While the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) (Venkatesh et al., 2012) stands out as the latest and most recognized evolution of the technology adoption models that are a cornerstone of information systems research for predicting individuals' intentions to adopt and use technologies, UTAUT2 has rarely been applied to examine how privacy concerns impact individuals' readiness to embrace and use online technologies (Y. Li, 2012). This research aims to bridge this gap by investigating the influence of information privacy concerns on the dynamics within the UTAUT2 framework and understanding how these interactions shape individuals' intentions to adopt and use online technologies. This study utilizes the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) as a core theoretical framework to explore how information privacy concerns influence individuals' intentions to adopt online technologies. Specifically, it examines information privacy concerns as a moderating factor that affects the relationship between several key antecedents—performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, and habit—and the intention to adopt online technologies.

Using data collected from 298 participants through a survey instrument that is adopted from established research, this research analyses two sets of Hypotheses in the context of web-based healthcare portals. The first set consists of six direct-effect hypotheses proposing a positive association of performance expectancy, effort expectancy, facilitating condition, social influence,

hedonic motivation, and habit with the individual intention to use the web-based healthcare portal technology. The second set of hypotheses consists of six moderating-effect hypotheses proposing a negative moderation impact of information privacy concerns on the direct-effect relationships. The information privacy concerns construct used in this research is an established construct adopted from information privacy literature and suited to fit the context of the tested healthcare technology. It comprises six dimensions: Collection, Access, Secondary Use, Control, Awareness, and Error.

In predicting individuals' intention to use web-based healthcare portals, the research model that includes information privacy concerns as a moderator variable of the UTAUT2 relationships yielded an R^2 of 0.657, explaining 65.7 of the total variance in individuals' intention to use web-based healthcare portals. The model, in which information privacy concerns were a precondition for the intention to use web-based healthcare portals, didn't add significant explanatory power to the direct UTAUT2 model that initially explained only 62.8% of the total variance in individuals' intention to use web-based healthcare portals. As a result, the integrated model with the moderating effect of information privacy concerns explained a greater variance.

With respect to the direct UTAUT2 relationships, the results support hypotheses 1, 2, and 6 indicating that performance expectancy, effort expectancy, and habit significantly influenced the participants' intention to use the web-based healthcare portals. The positive association between performance expectancy and participants' intention to use technology (Hypothesis 1) corresponds with the findings from previous research (Dwivedi et al., 2016; Hsu et al., 2013). This association underlies the principle that individuals are more likely to adopt technologies they expect to enhance their job performance (Venkatesh et al., 2012) or, in this context, their ability to manage health effectively (Dwivedi et al., 2016). Web-based portals may be vital in

empowering patients, especially those with chronic conditions, to self-manage their health effectively (Emont, 2011). Web-based healthcare portals' comprehensive functionalities, ranging from access to test results and healthcare appointment management to educational resources and direct communication with healthcare providers, coupled with notification systems for personalized feedback and alerts, may be crucial for effective health management (Goldzweig et al., 2013). These personalized functionalities will likely improve individuals' performance expectancy and motivate them to use web-based healthcare portals more frequently.

The positive association found in this research between effort expectancy and individuals' intention to use technology (Hypothesis 2) is also supported by previous research (Chatterjee & Bhattacharjee, 2020; Talukder et al., 2019). Web-based healthcare portals that are designed with user-friendly interfaces and clear instructions may enhance individuals' confidence in the ease of managing their health online. Features like simplified navigation, easily accessible information, and responsive design for various devices may significantly reduce the effort required to use these portals (Weng, Hsieh, Hsieh, & Lai, 2007). The ease of use of web-based healthcare portals will likely enhance participants' intention to use the web-based healthcare portals.

Similarly, the positive association in this research between habit and individuals' intention to use technology (Hypothesis 6) also corresponds with findings from previous research (Bower, DeWitt, & Lai, 2020; Foroughi et al., 2023). In case of web-based healthcare portals, the formation of habits such as regularly logging in to schedule appointments, view test results, or communicate with healthcare providers, signifies the integration of these portals into individuals' daily health management routines. This habitual use may demonstrate a profound level of engagement and dependence on the portal, indicating that individuals have moved beyond conscious decision-making to a state of automaticity in their interactions with the healthcare

web-based portal. This transition to habitual use may suggest that the more ingrained these practices become in a patient's routine, the greater their intention to continue using web-based healthcare portals.

The research findings reveal that social influence does not significantly impact individuals' intentions to use web-based healthcare portals deviating from hypothesis 3 and the outcomes of previous research by Adapa et al. (2018), and Giovanis et al. (2019), and Oliveira et al. (2016). This inconsistency can be attributed to the highly personal and confidential nature of the information accessed through these portals encompassing details that individuals are reluctant to discuss or share with others (Bellamy, 6, Raab, Warren, & Heeney, 2008). This privacy concern can lead to a reticence to openly talk about the use of healthcare portals, preventing the formation of social norms around their usage. Without these norms, the typical pathways through which social influence operates become less relevant (Jasperson, Sambamurthy, & Zmud, 1999). Consequently, social influence may not play a significant role in shaping individuals' intentions to use these web-based healthcare portals. This could also be attributed to the web-based healthcare portals relatively recent emergence as a widely adopted technology, primarily accelerated by the COVID-19 pandemic. Given this recent adoption, there hasn't been sufficient time for these portals to become established as a social norm within communities. As web-based healthcare portals continue to evolve and become more integrated into daily healthcare management, it's possible that the social norms surrounding their use may also develop, potentially altering the role of social influence in adoption intentions. Previous studies (Varshneya, Pandey, & Das, 2017) have indicated that social influence often has a minimal impact on the acceptance and adoption of new technologies.

Unexpectedly, our research revealed that facilitating conditions do not significantly predict individuals' intentions to use web-based healthcare portals, a result that diverges from hypothesis 4. This outcome stands in contrast to previous studies by Al-Emran et al. (2023), Beh et al. (2021), and Reyes-Mercado (2018), all of which posit that facilitating conditions play a crucial role in the adoption and utilization of technology. This could be attributed to the familiarity and ease with which individuals use similar online portals for various purposes, such as shopping or banking. The routine nature of accessing and using user-friendly platforms, which typically only require an internet connection, may have made the process straightforward for many individuals. This widespread comfort with and accessibility to digital portals may suggest that the need for additional technical support or specific facilitating conditions might be less relevant for users of web-based healthcare portals (Foroughi et al., 2023). Since the basic requirements to use these healthcare portals are similar to those for other online services that people are already accustomed to, the role of facilitating conditions as a determinant for the intention to use web-based healthcare portals may become insignificant.

Similarly, our research revealed that hedonic motivation does not significantly predict individuals' intentions to use web-based healthcare portals, a result that diverges from hypothesis 5 and several studies suggesting a positive impact of hedonic motivation on individuals' adoption of different technologies (Brown & Venkatesh, 2005; Thong, Hong, & Tam, 2006). This finding can likely be explained by the nature of the tasks the web-based healthcare portals facilitate. Typically, the use of web-based healthcare portals is associated with tasks that are transactional rather than enjoyable, aimed at executing necessary steps for health maintenance rather than being driven by fun or internal interest. These tasks often involve checking medical records, scheduling appointments, or managing prescriptions, these activities are crucial for individuals'

health but my not be designed to be engaging or pleasurable. This functional and utilitarian aspect of healthcare portals' tasks may contrast with applications meant for entertainment or fun, where hedonic motivation plays a more significant role in impacting the use of such applications (Tamilmani, Rana, Prakasam, & Dwivedi, 2019). Additionally, the context of healthcare information and the importance of its privacy may further distance these portals from hedonic use cases, making the pleasure derived from the use of such technologies an unlikely factor in impacting individuals' intentions to adopt or use these portals (Yang Meier, Barthelmess, Sun, & Liberatore, 2020).

In the context of the moderation relationships explored in this research, the findings revealed that information privacy concerns serve as a negative moderator between effort expectancy and individuals' intentions to use web-based healthcare portals, supporting hypothesis 8. This finding was anticipated because individuals with heightened information privacy concerns might prioritize the effort involved in managing potential health information breaches over the ease of use offered by the web-based healthcare portals. Such concerns could diminish the significance of how easy the web-based healthcare portals are to use, impacting individual's intention to adopt or utilize these platforms. Despite the recognized convenience of these portals, privacy worries may reduce the positive influence of effort expectancy on patients' intentions to adopt the web-based healthcare portals. This also can be because Individuals concerned about their personal information's privacy might find the default or essential privacy settings of web-based portals insufficiently secure (Schettino et al., 2023), and these privacy settings, which allow them to control the collection, use, and disclosure of their personal information (Ibrahim et al., 2012), may become another layer of tasks for individuals concerned about privacy of their health information. For those individuals, the need to regularly learn,

perform, and validate these settings as system features evolve (Khandelwal et al., 2021) introduces a layer of effort that might detract from the ease of use of the portals. This added effort can reduce the overall impact of effort expectancy on these individuals' intention to use the web-based healthcare portals.

The results also reveal a remarkably unexpected and counterintuitive finding, indicating that privacy concerns might positively moderate the relationship between performance expectancy and the intention to use web-based healthcare portals. This finding contradicts with Hypothesis 7, which posited that health information privacy concerns have a negative moderation effect on the relationship between performance expectancy and intention to use web-based healthcare portals. Hypothesis 7 posited that individuals with high health information privacy concerns may perceive inefficiencies and risks linked to potential data breaches via web-based healthcare portals (Schlackl et al., 2022), thereby diminishing the influence of performance expectancy on their intentions to use the web-based healthcare portals.

One possible interpretation of the observed positive moderation effect might be that individuals with significant privacy concerns may view web-based healthcare portals as more secure channels for managing their health information compared to traditional methods such as paper-based records, phone communication, or postal services. This perception of enhanced security and data protection could amplify the influence of performance expectancy on individuals' intentions to use web-based healthcare portals, particularly among those with heightened concerns about the privacy of their health information. However, it is important to note that while this interpretation is plausible, it remains a research question that is not fully substantiated by the current findings. Thus, it could serve as a valuable topic for future research, as I discuss in the subsequent section.

The study inability to yield statistically significant support for the hypothesized negative moderating influence of information privacy concerns on the association of social influence (Hypothesis 9), facilitating conditions (Hypothesis 10), and hedonic motivation (Hypothesis 11), and habit (Hypothesis 12) with the intention to use web-based healthcare portals can be attributed to several methodological and contextual factors. Methodologically, given the lack of support for the direct relationships between social influence, facilitating conditions, and hedonic motivation with individuals' intention to use web-based healthcare portals, attempting to identify moderation effects of health information privacy concerns on these relationships would be challenging. Without evidence of significant direct effects, there is little basis to investigate how privacy concerns might moderate these relationships. Therefore, the absence of statistically significant moderation impacts can be attributed to the foundational issue of unsupported direct relationships in the data.

Contextually, individuals may have prioritized the perceived benefits of the web-based healthcare portals, such as convenience and accessibility to medical information, over their privacy concerns, which aligns with the privacy paradox phenomenon (Barth & De Jong, 2017) that explains the tendency of individuals to express concerns about privacy but engage in behaviors that seem to contradict these concerns. Similar findings were concluded in previous research in social media and healthcare (Fox, 2020; Kokolakis, 2017). For instance, in web-based healthcare portals context, an individual with a chronic illness may prioritize remote management through web-based portals despite privacy concerns due to the habit of accessing medical records and online consultations through the portals.

Similarly, trust in healthcare providers and institutions can mitigate privacy concerns, as positive experiences with providers may foster confidence in the security of personal health

information online (Iott, Campos-Castillo, & Anthony, 2019). This trust could lead individuals to overlook privacy concerns when using web-based portals recommended by trusted healthcare professionals. Additionally, the ease of use and positive user experience offered by web-based portals may outweigh privacy concerns for some individuals. For example, a user-friendly interface and efficient features could motivate busy professionals to utilize web-based portals despite underlying privacy concerns. Moreover, the existence of compliance with regulatory frameworks and transparent privacy policies in the U.S may have alleviated individuals' apprehensions about the health information provided online.

The research results also reveal important insights regarding the control variables. For instance, the Gender control variable consistently shows a negative relationship with the intention to use web-based healthcare portals (β= -0.162, $p<0.05$), indicating that females might exhibit higher intentions to use web-based healthcare portals than males. Performance expectancy shows a statistically significant positive relationship with the intention to use web-based healthcare portals in model 2 (β= .206, $p<0.01$), model 3 (β= .195 $p<0.01$), and model 3 (β=.107, $p<0.05$). This indicates that the performance expectancy of the web-based healthcare portals contributes positively to individuals' intention to adopt them, although the effect slightly diminishes as more variables are introduced in subsequent models. Similarly, effort expectancy shows a statistically significant positive relationship with the intention to use web-based healthcare portals in model 2 (β= .135, $p<0.01$), model 3 (β= .129 $p<0.01$), and model 3 (β=.197, $p<0.01$). This indicates that the effort expectancy of the web-based healthcare portals contributes positively to individuals' intention to adopt them. Finally, habit shows a statistically significant positive relationship with the intention to use web-based healthcare portals in model 2 (β= .356, $p<0.01$), model 3 (β= .359 $p<0.01$), and model 3 (β=.344, $p<0.01$). This indicates that the habit

of using web-based healthcare portals contributes positively to individuals' intention to adopt them.

5.2 Research Limitations

Several limitations warrant attention when reflecting upon this dissertation's methodological underpinnings and analytical approaches. Firstly, relying on self-reported data through a survey instrument introduces inherent constraints (Brutus, Aguinis, & Wassmer, 2013). While surveys are instrumental in gathering large volumes of data efficiently, self-disclosure accuracy can be compromised by social desirability bias, where respondents may portray themselves in a more favorable light (Larson, 2019). Or by recall bias, affecting the precision of reported behaviors and perceptions (Tarrant, Manfredo, Bayley, & Hess, 1993)These aspects can be particularly pertinent in this study, where the nature and sensitivity of the subject matter could influence individuals' willingness and ability to answer questions regarding their apprehensions accurately. Consequently, the findings might not fully encapsulate the depth and complexity of individuals' privacy concerns and their impact their intentions to adopt the web-based healthcare portals.

Another limitation stems from recruiting participants through a paid online tool, Prolific. Although Prolific is renowned for its high-quality participant pool (Turner, Engelsma, Taylor, Sharma, & Demiris, 2020), the use of monetary incentives could compromise the responses quality and sample composition (Gritz, 2004). Participants motivated by financial rewards may not accurately represent the broader population's views and behaviors, potentially introducing a selection bias due to the non-representative nature of the Internet population or the `volunteer effect' (Eysenbach & Wyatt, 2002). This aspect raises questions about the generalizability of the

findings, as the participant pool may over-represent certain demographics or user groups who are more inclined to participate in online studies for compensation.

Employing multiple regression analysis as the statistical tool for data analysis also presents limitations (Kincaid, 2012). While multiple regression is a powerful technique for understanding the relationships between multiple independent variables and a dependent variable, it assumes a linear relationship among variables. This assumption may not always hold true in complex behavioral studies, where relationships can be non-linear or influenced by unmeasured variables (Osborne & Waters, 2019). Furthermore, despite diagnostic checks, the potential for multicollinearity among predictors remains a concern, as it can inflate standard errors and lead to misleading interpretations of the data.

Additionally, this study's cross-sectional design limits the ability to capture changes in privacy concerns and technology adoption intentions over time. As technology and societal norms evolve, so do individuals' privacy concerns and responses to technology offerings. A longitudinal approach would provide a richer understanding of these dynamics and how they influence technology adoption in the long run.

Finally, this research focused exclusively on the healthcare technology context, limiting the findings' applicability to other sectors where privacy concerns and technology adoption may interact differently. The unique sensitivity associated with health-related information may elicit privacy concerns distinct from those in less personal contexts, such as retail or entertainment technologies. Exploring a wider range of technologies and contexts could reveal additional nuances in the interplay between privacy concerns and technology adoption.

5.3 Contributions

The exploration of the moderating role of privacy concerns within the framework of the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2), particularly in the healthcare sector, can pave new avenues for academic inquiry and practical applications (Venkatesh et al., 2016). This study responds to the growing calls within the Information Systems field for an expansion of the UTAUT2 model and ventures into previously underexplored territories by delineating the intricate manner in which constructs like privacy concerns influence technology acceptance and adoption (Chang, Chao, Yu, & Lin, 2021). By dissecting the complex interplay between various constructs of the UTAUT2 model and the multifaceted nature of privacy concerns, this research enriches theoretical paradigms and extends our understanding of the dynamic forces at play in the technology adoption landscape. The detailed examination of privacy concerns as a moderating variable augments existing literature by providing deeper insights into the barriers and facilitators of technology utilization, thereby facilitating a nuanced comprehension of user behavior.

From a practical standpoint, the implications of this study are manifold. By highlighting the significant impact of privacy concerns on the adoption of healthcare technologies, this research offers valuable insights for developers, policymakers, and healthcare providers. It underscores the importance of crafting robust privacy policies and creating targeted interventions designed to alleviate user apprehensions about privacy. Such measures not only enhance user trust and confidence in technology but also contribute to higher adoption rates, thereby optimizing the integration of innovative technologies in healthcare settings. Furthermore, the findings serve as a guiding light for the design and implementation of user-centric technologies

that prioritize privacy, ensuring that technological advancements align with user expectations and ethical standards.

The investigative journey into the moderating effects of privacy concerns on UTAUT2's predictive capabilities within the healthcare domain bridges significant gaps between theoretical assumptions and real-world applications. It provides a solid foundation for future research initiatives aimed at exploring these dynamics across different technological platforms and industry sectors. This research could promote the curiosity for a renewed academic exploration of technology acceptance models and could catalyze the interest in the development of practical strategies for enhancing digital adoption in an era where privacy considerations are paramount. This research aims to offer a harmonious blend of theoretical innovation and practical foresight, offering a comprehensive blueprint for navigating the challenges and opportunities presented by the increasing privacy concerns among individuals during an era of continuous introduction of new technologies.

5.4 Future Research

The findings of this dissertation offer a rich ground for future investigations aimed at understanding the different dynamics between privacy concerns and technology adoption across various sectors and technologies. For example, future research can explore the potential positive moderating role of privacy concerns in the context of online services, particularly for individuals who exhibit high levels of trust in the security of technology and demonstrate a preference for advanced technological solutions over traditional methods such as paper, telephone, or mail. While existing literature often focuses on the negative impact of privacy concerns on technology adoption (Dhagarra et al., 2020), the privacy concerns may exert a positive moderating influence under certain conditions, especially among technologically savvy individuals who value

technological data security and digital privacy. Such future research can investigate how individuals with high trust in technology perceive and respond to privacy concerns when utilizing online services. Understanding how trust in technology interacts with privacy concerns can shed light on the conditions under which privacy concerns may serve as a positive moderating factor, bolstering rather than inhibiting technology adoption. For instance, the privacy concerns of individuals who have a strong belief in the security measures implemented by online service providers may increase their intention to use the technological services offered by these service providers.

Similarly, future studies could investigate how contextual factors, such as industry regulations, platform transparency, and user education initiatives, influence the moderating effect of privacy concerns on technology adoption behaviors. Regulatory frameworks, which prioritize data protection and privacy rights (Mendelson, 2017), may strengthen the positive moderating role of privacy concerns by providing assurances to users regarding the handling of their personal information.

Given the concluded role that privacy concerns play in moderating the relationship between user intentions and technology adoption, as highlighted in this research within the web-based healthcare portals context through the lens of the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2), there exists a compelling avenue to explore these dynamics within other technological filed like the field of Artificial Intelligence (AI) technology. AI presents a unique context where privacy concerns may manifest differently (Foroughi et al., 2023), largely due to the complex nature of AI algorithms and the potential use of personal data in training these models. The concern that individuals' data, once fed into AI systems, could become part of training datasets accessible by unknown entities amplifies privacy concerns

(Oseni et al., 2021), making the findings from this research particularly salient. Exploring the moderating role of privacy concerns on AI technology adoption could uncover additional insights, given the distinct privacy challenges posed by AI compared to healthcare technologies. Such research could benefit from the methodological foundations laid in this dissertation while tailoring the investigation to the specific contours of privacy concerns in the AI ecosystem.

Methodologically, transitioning from the controlled environments of survey-based research to observing individuals in real-world settings may offer another promising direction for future research. Real-environment observations could yield insights into individuals' behavior and decision-making processes that are more nuanced and reflect genuine individuals' experiences (Boyko, 2013). This approach may reveal the complexities and variances in how privacy concerns are perceived and acted upon across different contexts, potentially uncovering more accurate impact for the privacy concerns on the relationships between the UTAUT2 predictors and technology adoption intentions.

Furthermore, employing alternative privacy concern measurement scales, such as the Concern for Information Privacy (CFIP) (H. J. Smith et al., 1996) or the Internet Users' Privacy Concerns (IUPC) (Malhotra et al., 2004), could provide a broader perspective on the interaction between privacy concerns and technology adoption. These scales, with their distinct dimensions, offer a diversified lens through which to examine privacy concerns (Bartol, Vehovar, & Petrovčič, 2023). The differential impact of these dimensions on the predictors of the UTAUT2 model might reveal complex patterns of influence not observed in the current study. For instance, the granularity of the CFIP or IUPC scales could illuminate specific aspects of privacy concerns that have a more pronounced or nuanced moderating effect on technology adoption intentions.

5.5 Conclusion

This dissertation augments the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) by examining the nuanced role of information privacy concerns on the intention to use web-based healthcare portals. Through a meticulously designed survey administered to 298 U.S. residents who are active users of healthcare technologies, this study ventures into the complex interplay between technology acceptance predictors and the multifaceted construct of Privacy Concerns, which includes the Collection, Unauthorized Access, Secondary Use, Control, Awareness, and Error dimensions. Employing regression analysis via SPSS, the study tested twelve hypotheses to delineate the direct effects of UTAUT2 predictors, namely Performance Expectancy, Effort Expectancy, Facilitating Conditions, Habit, Social Influence, and Hedonic Motivation, on the intention to adopt healthcare technologies, alongside exploring the moderating impact of privacy concerns on these relationships.

The empirical findings underscored the significance of Performance Expectancy, Effort Expectancy, and Habit in positively influencing individuals' intentions to use web-based healthcare portals. Notably, the investigation revealed a singular moderating effect of health information privacy concerns, which attenuates the positive relationship between Effort Expectancy and individuals' intention to use this technology. This dissertation contributes to the extant literature by embedding information privacy concerns within the UTAUT2 framework, thereby offering a more granular understanding of the factors influencing technology adoption. This study broadens the applicability of the UTAUT2 model by underscoring the essential influence of privacy concerns, providing a theoretical contribution that improves the model's predictivity.

From a practical standpoint, the findings can provide actionable insights for practitioners and policymakers, emphasizing the importance of addressing privacy concerns to bolster technology adoption rates. By pinpointing specific privacy-related factors that deter user acceptance, the study paves the way for targeted interventions designed to mitigate these concerns, ultimately facilitating a more widespread and effective use of technologies.

REFERENCES

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the International workshop on privacy enhancing technologies.

Adapa, A., Nah, F. F.-H., Hall, R. H., Siau, K., & Smith, S. N. (2018). Factors influencing the adoption of smart wearable devices. *International Journal of Human–Computer Interaction, 34*(5), 399-409.

Ahmed, M. H., Bogale, A. D., Tilahun, B., Kalayou, M. H., Klein, J., Mengiste, S. A., & Endehabtu, B. F. (2020). Intention to use electronic medical record and its predictors among health care providers at referral hospitals, north-West Ethiopia, 2019: using unified theory of acceptance and use technology 2 (UTAUT2) model. *BMC Medical Informatics and Decision Making, 20*(1), 1-11.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al-Emran, M., AlQudah, A. A., Abbasi, G. A., Al-Sharafi, M. A., & Iranmanesh, M. (2023). Determinants of using AI-based chatbots for knowledge sharing: evidence from PLS-SEM and fuzzy sets (fsQCA). *IEEE Transactions on Engineering Management*.

Alzahrani, L., Al-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International business review, 26*(1), 164-175.

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *ACR North American Advances*.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 339-370.

Auxier, B., & Rainie, L. (2019). Key takeaways on Americans' views about privacy, surveillance and data-sharing.

Bannister, F., & Connolly, R. (2015). The great theory hunt: Does e-government really have a problem? *Government Information Quarterly, 32*(1), 1-11.

Bano, S., Sarfraz, U., Salameh, A. A., & Jan, A. (2022). COVID-19 Paradox: The Role of Privacy Concerns and Ad Intrusiveness on Consumer's Attitude Toward App Usage Behavior. *Frontiers in Psychology, 13*, 836060.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Barrett-Howard, E., & Tyler, T. R. (1986). Procedural justice as a criterion in allocation decisions. *Journal of Personality and Social Psychology, 50*(2), 296.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics, 34*(7), 1038-1058.

Bartol, J., Vehovar, V., & Petrovčič, A. (2021). *Should we be concerned about how information privacy concerns are measured in online contexts? A systematic review of survey scale development studies.* Paper presented at the Informatics.

Bartol, J., Vehovar, V., & Petrovčič, A. (2023). Systematic review of survey scales measuring information privacy concerns on social network sites. *Telematics and informatics*, 102063.

Bauer, C., & Schiffinger, M. (2016). Perceived risks and benefits of online self-disclosure: Affected by culture? A meta-analysis of cultural differences as moderators of privacy calculus in person-to-crowd settings.

Bedrov, A., Gable, S., & Liberman, Z. (2021). It takes two (or more): The social nature of secrets. *Wiley Interdisciplinary Reviews: Cognitive Science, 12*(6), e1576.

Beh, P. K., Ganesan, Y., Iranmanesh, M., & Foroughi, B. (2021). Using smartwatches for fitness and health monitoring: the UTAUT2 combined with threat appraisal as moderators. *Behaviour & Information Technology, 40*(3), 282-299.

Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2022). Consumers' privacy calculus: The PRICAL index development and validation. *International Journal of Research in Marketing, 39*(1), 20-41.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 1017-1041.

Bellamy, C., 6, P., Raab, C., Warren, A., & Heeney, C. (2008). Information-sharing and confidentiality in social policy: Regulating multi-agency working. *Public Administration, 86*(3), 737-759.

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*: Cornell University Press.

Bergen, M., Dutta, S., & Walker Jr, O. C. (1992). Agency relationships in marketing: A review of the implications and applications of agency and related theories. *Journal of marketing, 56*(3), 1-24.

Bervell, B. B., Kumar, J. A., Arkorful, V., Agyapong, E. M., & Osman, S. (2022). Remodelling the role of facilitating conditions for Google Classroom acceptance: A revision of UTAUT2. *Australasian Journal of Educational Technology, 38*(1), 115-135.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953-977.

Bower, M., DeWitt, D., & Lai, J. W. (2020). Reasons associated with preservice teachers' intention to use immersive virtual reality in education. *British Journal of Educational Technology, 51*(6), 2215-2233.

Boyko, E. J. (2013). Observational research—opportunities and limitations. *Journal of Diabetes and its Complications, 27*(6), 642-648.

Bradely. (2019). Data privacy concerns: An overview for 2019. Medium

Brown, S. A., & Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. *MIS Quarterly*, 399-426.

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports: Analysis and recommendations. *Journal of management, 39*(1), 48-75.

C. Sipior, J., T. Ward, B., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management, 26*(6), 661-678.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5-25.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online information review, 31*(5), 583-603.

Cases, A.-S., Fournier, C., Dubois, P.-L., & Tanner Jr, J. F. (2010). Web Site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes. *Journal of Business Research, 63*(9-10), 993-999.

Caughlin, J. P., & Vangelisti, A. L. (2015). Why people conceal or reveal secrets: A multiple goals theory perspective. In *Uncertainty, information management, and disclosure decisions* (pp. 279-299): Routledge.

Cha, J. (2010). Factors affecting the frequency and amount of social networking site use: Motivations, perceptions, and privacy concerns. *First Monday*.

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

Chan, J. L. (2016). *The patient paradigm shifts: Profiling the new healthcare consumer*: Business Expert Press.

Chang, Y.-T., Chao, C.-M., Yu, C.-W., & Lin, F.-C. (2021). Extending the utility of UTAUT2 for hospital patients' adoption of medical apps: moderating effects of e-health literacy. *Mobile Information Systems, 2021*, 1-10.

Chatterjee, S., & Bhattacharjee, K. K. (2020). Adoption of artificial intelligence in higher education: A quantitative analysis using structural equation modelling. *Education and Information Technologies, 25*, 3443-3463.

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

Chennamaneni, A., & Gupta, B. (2023). The privacy protection behaviours of the mobile app users: Exploring the role of neuroticism and protection motivation theory. *Behaviour & Information Technology, 42*(12), 2011-2029.

Cheung, M. T., & Liao, Z. (2003). Supply-side hurdles in internet B2C e-commerce: an empirical investigation. *IEEE Transactions on Engineering Management, 50*(4), 458-469.

Chiu, C. M., Chang, C. C., Cheng, H. L., & Fang, Y. H. (2009). Determinants of customer repurchase intention in online shopping. *Online information review, 33*(4), 761-784.

COLIN, J., & RAAB, B. C. D. (1997). The adequacy of privacy: The European Union data protection directive and the North American response. *The Information Society, 13*(3), 245-264.

Correia, J., & Compeau, D. (2017). Information privacy awareness (IPA): a review of the use, definition and measurement of IPA.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

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

Dai, H., & Palvi, P. C. (2009). Mobile commerce adoption in China and the United States: a cross-cultural study. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 40*(4), 43-61.

Davis, F. D. (1989a). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.

Davis, F. D. (1989b). Technology acceptance model: TAM. *Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption*, 205-219.
Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective. *International journal of medical informatics, 141*, 104164.
Dhotre, P. S., Olesen, H., & Khajuria, S. (2018). *User privacy and empowerment: Trends, challenges, and opportunities.* Paper presented at the Intelligent Computing and Information and Communication: Proceedings of 2nd International Conference, ICICC 2017.
Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.
Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.
Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.
Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of management review, 19*(2), 252-284.
Duarte, P., & Pinho, J. C. (2019). A mixed methods UTAUT2-based approach to assess mobile health adoption. *Journal of Business Research, 102*, 140-150.
Dwivedi, Y. K., Shareef, M. A., Simintiras, A. C., Lal, B., & Weerakkody, V. (2016). A generalised adoption model for services: A cross-country comparison of mobile health (m-health). *Government Information Quarterly, 33*(1), 174-187.
Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886.
Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review, 14*(1), 57-74.
Elueze, I., & Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *American Behavioral Scientist, 62*(10), 1372-1391.
Emont, S. (2011). Measuring the impact of patient portals. *California Healthcare Foundation*, 1-20.
Eysenbach, G., & Wyatt, J. (2002). Using the Internet for surveys and health research. *Journal of medical Internet research, 4*(2), e862.
Faja, S., & Trimi, S. (2006). Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the association for information Systems, 17*(1), 27.
Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods, 39*(2), 175-191.
Ferreira, L., Oliveira, T., & Neves, C. (2023). Consumer's intention to use and recommend smart home technologies: The role of environmental awareness. *Energy, 263*, 125814.
Foroughi, B., Senali, M. G., Iranmanesh, M., Khanfar, A., Ghobakhloo, M., Annamalai, N., & Naghmeh-Abbaspour, B. (2023). Determinants of intention to use ChatGPT for educational purposes: Findings from PLS-SEM and fsQCA. *International Journal of Human–Computer Interaction*, 1-20.

Fox, G. (2020). “To protect my health or to protect my health privacy?” A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology, 71*(9), 1015-1029.
Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal, 28*(6), 995-1019.
Frye, N. E., & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior, 26*(5), 1120-1127.
Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems, 115*(9), 1704-1723.
Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and tam in online shopping: An integrated model1. *MIS Quarterly, 27*(1), 51-90.
Giovanis, A., Assimakopoulos, C., & Sarmaniotis, C. (2019). Adoption of mobile self-service retail banking technologies: The role of technology, social, channel and personal factors. *International Journal of Retail & Distribution Management, 47*(9), 894-914.
Goldzweig, C. L., Orshansky, G., Paige, N. M., Towfigh, A. A., Haggstrom, D. A., Miake-Lye, I., . . . Shekelle, P. G. (2013). Electronic patient portals: evidence on health outcomes, satisfaction, efficiency, and attitudes: a systematic review. *Annals of internal medicine, 159*(10), 677-687.
Gritz, A. S. (2004). The impact of material incentives on response quantity, response quality, sample composition, survey outcome and cost in online access panels. *International Journal of Market Research, 46*(3), 327-345.
Groß, T. (2021). Validity and reliability of the scale internet users’ information privacy concerns (iuipc). *Proceedings on Privacy Enhancing Technologies*.
Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of management information systems, 24*(2), 13-42.
Haring, J. E., & Smith, G. C. (1959). Utility theory, decision theory, and profit maximization. *The American Economic Review, 49*(4), 566-583.
Hennessy, T., Kinsella, A., & Thorne, F. (2016). Planned intentions versus actual behaviour: assessing the reliability of intention surveys in predicting farmers’ production levels post decoupling. *International Journal of Agricultural Management, 5*(1029-2019-900), 70-77.
HHS, U. S. D. o. H. a. H. S. (1996). Health Insurance Portability and Accountability Act of 1996 (HIPAA). .
Holden, R. J., & Karsh, B.-T. (2010). The technology acceptance model: its past and its future in health care. *Journal of biomedical informatics, 43*(1), 159-172.
Holvast, J. (2007). History of privacy. In *The history of information security* (pp. 737-769): Elsevier.
Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 275-298.
Hsu, C.-L., Lee, M.-R., & Su, C.-H. (2013). The role of privacy protection in healthcare information systems adoption. *Journal of medical systems, 37*, 1-12.
Ibrahim, S. Z., Blandford, A., & Bianchi-Berthouze, N. (2012). *Privacy settings on Facebook: Their roles and importance.* Paper presented at the 2012 IEEE International Conference on Green Computing and Communications.

Ioannou, A., Tussyadiah, I., & Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing, 38*(10), 1766-1778.

Iott, B. E., Campos-Castillo, C., & Anthony, D. L. (2019). *Trust and privacy: how patient trust in providers is related to privacy behaviors and attitudes.* Paper presented at the AMIA Annual Symposium Proceedings.

Ivanov, D. I. (2008). *Ensuring long-term adoption of technology: Mandated use and individual habit as factors that establish technology into healthcare practice.* Case Western Reserve University,

Jahangir, N., & Begum, N. (2007). Effect of perceived usefulness, ease of use, security and privacy on customer attitude and adaptation in the context of e-banking. *Journal of Management Research, 7*(3), 147-157.

Janda, S. (2008). Does gender moderate the effect of online concerns on purchase likelihood? *Journal of Internet Commerce, 7*(3), 339-358.

Janda, S., & Fair, L. L. (2004). Exploring consumer concerns related to the internet. *Journal of Internet Commerce, 3*(1), 1-21.

Jasperson, J., Sambamurthy, V., & Zmud, R. (1999). Social influence and individual IT use: Unraveling the pathways of appropriation moves. *ICIS 1999 Proceedings*, 10.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1-24.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*, 387-402.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402. doi:10.1057/ejis.2008.29

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of human-computer studies, 71*(12), 1163-1173.

Kezer, M., Dienlin, T., & Baruh, L. (2022). Getting the privacy calculus right: Analyzing the relations between privacy concerns, expected benefits, and self-disclosure using response surface analysis. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(4).

Khandelwal, R., Linden, T., Harkous, H., & Fawaz, K. (2021). *{PriSEC}: A Privacy Settings Enforcement Controller.* Paper presented at the 30th USENIX Security Symposium (USENIX Security 21).

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13-45.

Kincaid, H. (2012). Mechanisms, causal modeling, and the limitations of traditional multiple regression. *The Oxford handbook of philosophy of social science*, 46-64.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security, 64*, 122-134.

Kordzadeh, N., Warren, J., & Seifi, A. (2016). Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management, 36*(5), 724-734.
Krasnova, H., & Veltri, N. F. (2010). *Privacy calculus on social networking sites: Explorative evidence from Germany and USA.* Paper presented at the 2010 43rd Hawaii international conference on system sciences.
Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254-264.
Larson, R. B. (2019). Controlling social desirability bias. *International Journal of Market Research, 61*(5), 534-547.
Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues, 33*(3), 22-42.
Le, H. T. P. M., Yoo, W., & Park, J. (2023). The effects of brand trustworthiness and credibility on location-based advertising: moderating effects of privacy concern and social influence. *International Journal of Advertising*, 1-26.
Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management research review, 37*(12), 1049-1092. doi:10.1108/MRR-04-2013-0085
Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic commerce research and applications, 8*(3), 130-141.
Lee, Y., Lim, W., & Eng, H. S. (2023). A systematic review of UTAUT2 constructs' analysis among MSMEs in non-OECD countries. *Journal of Science and Technology Policy Management*.
Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces, 63*(4), 967-985.
Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62-71.
Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the association for information Systems, 28*(1), 28.
Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.
Lian, J.-W., & Lin, T.-M. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior, 24*(1), 48-65.
Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems, 4*(1), 3.
Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304.
Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior, 127*, 107026.
Ma, X., Lou, H., Van Slyke, C., & Clary, G. (2020). Concern for Information Privacy and Online Consumer Purchasing in China. *AIS Transactions on Replication Research, 6*(1), 6.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Margulis, S. T. (2011). Three theories of privacy: An overview. *Privacy online: Perspectives on privacy and self-disclosure in the social web*, 9-17.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

Meet, R. K., Kala, D., & Al-Adwan, A. S. (2022). Exploring factors affecting the adoption of MOOC in Generation Z using extended UTAUT2 model. *Education and Information Technologies, 27*(7), 10261-10283.

Meier, Y., Schäwel, J., & Krämer, N. C. (2021). Between protection and disclosure: Applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites. *SCM Studies in Communication and Media, 10*(3), 283-306.

Mendelson, D. (2017). Legal protections for personal health information in the age of Big Data–a proposal for regulatory framework. *Ethics, Medicine and Public Health, 3*(1), 37-55.

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems, 56*, 103-114.

Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital nudging: Altering user behavior in digital environments.

Misra, S. C., Kumar, A., & Munnangi, A. K. (2019). Cloud-based healthcare management: Identifying the privacy concerns and their moderating effect on the cloud-based health-care services. *Security and Privacy, 2*(3), e63.

Mou, J., Shin, D.-H., & Cohen, J. (2017). Understanding trust and perceived usefulness in the consumer acceptance of an e-service: a longitudinal investigation. *Behaviour & Information Technology, 36*(2), 125-139.

Mwesiumo, D., Halpern, N., Budd, T., Suau-Sanchez, P., & Bråthen, S. (2021). An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns. *Journal of Business Research, 136*, 63-75.

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior, 61*, 404-414.

Osborne, J. W., & Waters, E. (2019). Four assumptions of multiple regression that researchers should always test. *Practical assessment, research, and evaluation, 8*(1), 2.

Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. *arXiv preprint arXiv:2102.04661*.

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European journal of information systems, 26*(6), 642-660.

Ozturk, A. B., Nusair, K., Okumus, F., & Singh, D. (2017). Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers, 19*, 753-767.

Pastalan, L. A. (1970). Privacy as a behavioral concept. *Social Science*, 93-97.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 977-988.
Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 105-136.
Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics, 59*, 327-345.
Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of management, 12*(4), 531-544.
Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of human-computer studies, 71*(12), 1133-1143.
Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., & Hofacker, C. F. (2010). Customer information sharing with e-vendors: The roles of incentives and trust. *International Journal of Electronic Commerce, 14*(3), 63-91.
Rahim, N. I. M., Iahad, N. A., Yusof, A. F., & Al-Sharafi, M. A. (2022). AI-Based chatbots adoption model for higher-education institutions: A hybrid PLS-SEM-Neural network modelling approach. *Sustainability, 14*(19), 12726.
Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level-a literature review. *Vilakshan-XIMB Journal of Management, 18*(2), 171-186.
Reichheld, F. F., & Schefter, P. (2000). E-loyalty: your secret weapon on the web. *Harvard business review, 78*(4), 105-113.
Rensel, A. D., Abbas, J. M., & Rao, H. R. (2006). Private transactions in public places: an exploration of the impact of the computer environment on public transactional web site use. *Journal of the Association for Information Systems, 7*(1), 2.
Reyes-Mercado, P. (2018). Adoption of fitness wearables: Insights from partial least squares and qualitative comparative analysis. *Journal of Systems and Information Technology, 20*(1), 103-127.
Rice, R. E. (1993). Media appropriateness: Using social presence theory to compare traditional and new organizational media. *Human communication research, 19*(4), 451-484.
Ritter, T., & Pedersen, C. L. (2020). Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. *Industrial Marketing Management, 86*, 180-190.
Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The journal of psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803
Rousseau, J.-J. (2018). *Rousseau: The Social Contract and other later political writings*: Cambridge University Press.
Sadeghi, M., Thomassie, R., & Sasangohar, F. (2017). *Objective assessment of functional information requirements for patient portals.* Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.
Schettino, G., Fabbricatore, R., & Caso, D. (2023). "To be yourself or your selfies, that is the question": The moderation role of gender, nationality, and privacy settings in the relationship between selfie-engagement and body shame. *Psychology of Popular Media, 12*(3), 268.
Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management, 59*(4), 103638.

Segijn, C. M., Voorveld, H. A., & Vakeel, K. A. (2021). The role of ad sequence and privacy concerns in personalized advertising: An eye-tracking study into synced advertising effects. *Journal of advertising, 50*(3), 320-329.
Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). *Healthcare data breaches: insights and implications.* Paper presented at the Healthcare.
Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A systematic literature review on privacy by design in the healthcare sector. *Electronics, 9*(3), 452.
Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of advertising, 28*(3), 37-51.
Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems, 9*(6), 1.
Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, 22*(5), 428-438.
Slepian, M. L., Chun, J. S., & Mason, M. F. (2017). The experience of secrecy. *Journal of Personality and Social Psychology, 113*(1), 1.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 989-1015.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.
Smith, T. T. (2016). Examining data privacy breaches in healthcare.
Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev., 44*, 745.
Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 503-529.
Stangl, A. L., Earnshaw, V. A., Logie, C. H., Van Brakel, W., C. Simbayi, L., Barré, I., & Dovidio, J. F. (2019). The Health Stigma and Discrimination Framework: a global, crosscutting framework to inform research, intervention development, and policy on health-related stigmas. *BMC medicine, 17*, 1-13.
Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information systems research, 13*(1), 36-49.
Talukder, M. S., Chiong, R., Bao, Y., & Hayat Malik, B. (2019). Acceptance and use predictors of fitness wearable technology and intention to recommend: An empirical study. *Industrial Management & Data Systems, 119*(1), 170-188.
Tamilmani, K., Rana, N. P., Prakasam, N., & Dwivedi, Y. K. (2019). The battle of Brain vs. Heart: A literature review and meta-analysis of "hedonic motivation" use in UTAUT2. *International Journal of Information Management, 46*, 222-235.
Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021). The extended Unified Theory of Acceptance and Use of Technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management, 57*, 102269.
Tarrant, M. A., Manfredo, M. J., Bayley, P. B., & Hess, R. (1993). Effects of recall bias and nonresponse bias on self-report estimates of angling participation. *North American Journal of Fisheries Management, 13*(2), 217-222.

Tawalbeh, L. a., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences, 10*(12), 4102.
Thong, J. Y., Hong, S.-J., & Tam, K. Y. (2006). The effects of post-adoption beliefs on the expectation-confirmation model for information technology continuance. *International Journal of human-computer studies, 64*(9), 799-810.
Trkman, M., Popovič, A., & Trkman, P. (2023). The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications. *Government Information Quarterly, 40*(1), 101787.
Turner, A. M., Engelsma, T., Taylor, J. O., Sharma, R. K., & Demiris, G. (2020). *Recruiting older adult participants through crowdsourcing platforms: Mechanical Turk versus Prolific Academic.* Paper presented at the AMIA Annual Symposium Proceedings.
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 Public Law 111-5 C.F.R. (2009).
Van der Heijden, H. (2004). User acceptance of hedonic information systems. *MIS Quarterly*, 695-704.
Van Der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: a scoping review and research agenda. *Future Internet, 15*(5), 164.
van Houwelingen, C. T., Barakat, A., Best, R., Boot, W. R., Charness, N., & Kort, H. S. (2015). Dutch nurses' willingness to use home telehealth: Implications for practice and education. *Journal of Gerontological Nursing, 41*(4), 47-56.
Vangelisti, A. L. (1994). Family secrets: Forms, functions and correlates. *Journal of Social and Personal Relationships, 11*(1), 113-135.
Varshneya, G., Pandey, S. K., & Das, G. (2017). Impact of social influence and green consumption values on purchase intention of organic clothing: a study on collectivist developing economy. *Global business review, 18*(2), 478-492.
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.
Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157-178.
Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328-376.
Vroom, V. H. (1966). Organizational choice: A study of pre-and postdecision processes. *Organizational behavior and human performance, 1*(2), 212-225.
Wairimu, S., & Fritsch, L. (2022). *Modelling privacy harms of compromised personal medical data-beyond data breach.* Paper presented at the Proceedings of the 17th International Conference on Availability, Reliability and Security.
Wang, Y., Ngien, A., & Ahmed, S. (2022). Nationwide adoption of a digital contact tracing app: Examining the role of privacy concern, political trust, and technology literacy. *Communication Studies, 73*(4), 364-379.
Weng, Y.-C., Hsieh, S.-L., Hsieh, S.-H., & Lai, F. (2007). *Design and enhance a dynamic healthcare portal site.* Paper presented at the 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology-Workshops.
Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM, 10*(9), 533-537.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 1.

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*, 137-149.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems, 51*(1), 42-52.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems, 26*(3), 135-174.

Yang Meier, D., Barthelmess, P., Sun, W., & Liberatore, F. (2020). Wearable technology acceptance in health care based on national culture differences: cross-country analysis between Chinese and Swiss consumers. *Journal of medical Internet research, 22*(10), e18801.

Yao, M. Z., & Zhang, J. (2008). Predicting user concerns about online privacy in Hong Kong. *CyberPsychology & Behavior, 11*(6), 779-781.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. *Information systems research, 21*(4), 724-735.

Yuan, S., Ma, W., Kanthawala, S., & Peng, W. (2015). Keep using my health apps: Discover users' perception of health and fitness apps with the UTAUT2 model. *Telemedicine and e-Health, 21*(9), 735-741.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, 56*(4), 570-601.

Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior, 69*, 157-165.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3-4), 180-197.

Zhou, L. L., Owusu-Marfo, J., Asante Antwi, H., Antwi, M. O., Kachie, A. D. T., & Ampon-Wireko, S. (2019). Assessment of the social influence and facilitating conditions that support nurses' adoption of hospital electronic information management systems (HEIMS) in Ghana using the unified theory of acceptance and use of technology (UTAUT) model. *BMC Medical Informatics and Decision Making, 19*(1), 1-9.

Zhu, H., Ou, C. X., van den Heuvel, W.-J. A., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management, 54*(4), 427-437.

APPENDIX: SURVEY INSTRUMENT QUESTIONS

Performance Expectancy:

PE1. I find using web-based healthcare portals useful in managing my overall healthcare-related tasks.

PE2. Using web-based healthcare portals increases my chances of achieving healthcare-related tasks that are important to me.

PE3. Using web-based healthcare portals helps me accomplish healthcare-related tasks more quickly.

PE4. Using web-based healthcare portals increases my overall productivity.

Effort Expectancy:

EE1 . Learning how to access self-health records through web-based healthcare portals is easy for me.

EE2. My interaction with medical professionals through web-based healthcare portals is clear and understandable.

EE3. I find web-based healthcare portals easy to use.

EE4. It is easy for me to become skillful at receiving, monitoring, and interpreting healthcare data through web-based healthcare portals.

Social Influence:

SI1 . People who are important to me think that I should use web-based healthcare portals

SI2. People who influence my behavior think that I should use web-based healthcare portals.

SI3. People whose opinions I value prefer that I use web-based healthcare portals.

Facilitating Condition:

FC1. I have the resources necessary to use web-based healthcare portals.

FC2. I gathered the knowledge necessary to use web-based healthcare portals

FC3. web-based healthcare portals are compatible with my daily routine.

FC4. I can get reliable help from medical professionals when I have difficulties using web-based healthcare portals.

Hedonic Motivation:

IM1. Using web-based healthcare portals is fun.

IM2. Using web-based healthcare portals is enjoyable.

IM3. Using web-based healthcare portals is very entertaining.

Habit:

HT1. The use of web-based healthcare portals has become a habit for me.

HT2. I am addicted to using web-based healthcare portals.

HT3. I must use web-based healthcare portals.

HT4. Using web-based healthcare portals has become natural to me.

Intention to use WBHP:

BI1. I intend to continue using web-based healthcare portals in the future.

BI2. I will always try to use web-based healthcare portals in my daily life.

BI3. I plan to continue to use web-based healthcare portals frequently.

Collection:

COLL1: Providing personal health information through web-based healthcare portals usually bothers me.

COLL2: It bothers me to give my personal health information through so many web-based healthcare portals

COLL3: When I am asked for personal health information through web-based healthcare portals, I sometimes think twice before providing it

COLL4: I'm concerned that too much personal health information about me is collected through web-based healthcare portals

Secondary use:

SEC1: I am concerned that when I give personal health information through web-based healthcare portals, my information might be used for other reasons

SEC2: I am concerned that the personal health information that I provide through web-based healthcare portals could be sold to other healthcare entities or non-health-related organizations

SEC3: I am concerned that the personal health information that I provide through web-based healthcare portals could be shared with other entities without authorization

Improper access:

ACC1: I am concerned that enough time and effort are not devoted to preventing unauthorized access to the personal health information that I provide through web-based healthcare portals

ACC2: I am concerned that the personal health information that I provide through web-based healthcare portals are not protected from unauthorized access

ACC3: I am concerned enough steps are not taken to make sure that unauthorized people cannot access the personal health information that I provide through web-based healthcare portals

Errors:

ERR1: I am concerned that enough time and effort are not devoted to verifying the accuracy of the personal health information that I provide through web-based healthcare portals

ERR2: I am concerned that there are no adequate procedures available to correct errors in the personal health information that I provide through web-based healthcare portals

ERR3: I am concerned that enough steps are not taken to make sure that the personal health information that I provide through web-based healthcare portals are accurate

Control:

CON1: It usually bothers me when I do not have control of the personal health information that I provide through web-based healthcare portals

CON2: I am concerned when control is lost or unwillingly reduced as a result of providing my personal health information through web-based healthcare portals

CON3: It usually bothers me when I do not have control or autonomy over decisions about how the personal health information that I provide through web-based healthcare portals are used and shared

Awareness:

AWR1: It usually bothers me when I am not aware or knowledgeable about how the personal health information that I provide through web-based healthcare portals will be used

AWR2: It is very important to me that I am aware and knowledgeable about how the personal health information that I provide through web-based healthcare portals will be used

AWR3: It usually bothers me when my personal health information is requested through web-based healthcare portals without disclosing the way the data are processed and used