THE EFFECT OF PRIVACY CONCERNS ON CHILDREN'S BEHAVIOR ON THE INTERNET: AN EMPIRICAL STUDY FROM THE PARENTS' PERSPECTIVE

Ali Alkhalifah, College of Computer, Qassim University
Aseel Alghafis, College of Computer, Qassim University

ABSTRACT

With the development of the Internet, the number of children online is rapidly increasing worldwide. Many children go online for various activities such as gaming, chatting, and browsing social networking sites. These activities come with different risks and privacy concerns. This study aims to investigate children's behavior in relation to their information privacy on the Internet from their parents' perspective. The study explores different factors that could impact on privacy concerns and examines their effects on children's behavior. It develops a model based on coping theory and the theory of planned behavior (TPB). The study employs the structural equation modeling (SEM) approach to test the proposed hypotheses and presents high-quality research analysis. The results indicate that factors such as parental control, information disclosure, privacy risk, and subjective norms have effects on privacy concerns. Also confirmed in the study's findings is the effect of privacy concerns on children's behavior on the Internet. However, the hypothesized path relationship between privacy concerns and content on the Internet is not statistically significant. This study has theoretical and practical implications. It is hoped that the study's findings will contribute to society with respect to children's behavior on the Internet.

Keywords: Children's behavior; Privacy; Information disclosure; Parents.

INTRODUCTION

With rapid progress in the development of the Internet, some websites, especially those involved with social networking, require users to provide personal information, including their name, date of birth, etc. This technological advancement is a shift from the traditional concept of information giving which has served to facilitate interactions and social services. Users, and specifically those who are children, need to find ways to protect the privacy of their information on social networking sites that require sensitive information. This would prevent users from losing information and avoid the disclosure of their privacy. The number of children online is rapidly increasing worldwide, with Internet usage rates among children surpassing usage rates among adults. On a normal day, seven out of 10 children go online (Lwin et al., 2012). Many studies have shown that the Internet poses a high level of security risk that targets behavioral threats to children (Livingstone & Brake, 2010; Andrews et al., 2020). These threats remain present, with the need to effectively study children's behavior on the Internet now increasingly

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

important. The current study attempts to address this problem by determining and explaining factors that affect children's behavior on the Internet.

Among those using the Internet weekly, the "Children in UK Go Online" survey of those aged 9-19 years found that 11% had viewed racist content and 31% had seen violent content. Furthermore, 8% had gone to physically meet someone they had just met online (Lwin et al., 2012). While younger teens and boys were more likely to post fake information, a United States (US) survey found that older teenagers were more likely to provide identity information: overall, 29% had included their email addresses and 49% had included their school addresses (Lwin et al., 2012). While 49% in that study provided their dates of birth, an Irish survey of those aged 10–20 years found that only 12% gave out their mobile phone numbers and 8% their home addresses. These personal disclosures are not surprising, as social networking sites are designed in such a way that children need to provide at least their photograph and name, in addition to their date of birth (Livingstone & Brake, 2010).

A new risk has arisen for adolescents due to the emergence of online games. One study of students between 13 and 16 years old from Dutch secondary schools found that approximately 3% were addicted to online video games (Kim et al., 2017). The National Information Society also reported that, in one of the largest online gaming sites in the South Korea market, 14.3% of adolescent respondents played online games for an average of 7.9 hours per day. The violent content of the games causes problems, in addition to the significant amount of time spent (Kim et al., 2017). Some applications require users to focus on the screen for a long time, thus possibly affecting their thinking and behavior: they are also required to disclose their personal details when engaging in games.

To address these issues, the current study attempts to provide measures to protect children's privacy. This arises from concerns about the use of many separate online applications, by studying factors affecting children's behavior while using the Internet. The study also seeks to provide a supportive methodology that increases security and reduces the risk related to using the World Wide Web/Internet.

Despite the interest in children's behavior on the Internet, it is surprising that little research has been conducted on these topics compared to other topics, although children's behavior and information privacy today is viewed as important (Kokolakis, 2017; Andrews et al., 2020). Studies focused on children's behavior on the Internet are lacking. Furthermore, few studies have investigated privacy concerns and their effect on children's behavior on the Internet. Privacy concerns users of all ages. Therefore, future research should focus on specific group as representative as possible (Kokolakis, 2017).

To address these issues and fill the existing gaps, this study seeks to answer the question: "what factors affect children's behavior on the Internet?" Therefore, the study's objectives are:

- To review previous studies and develop a model based on theory to test children's behavior while they are engaged with the Internet by using the theory of planned behavior (TPB).
- To provide a comprehensive explanation about how to evaluate factors that have an effect on the privacy of users, specifically children, to help to protect them by using effective privacy levels to address their involvement on multiple online networks.

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

- To develop and describe a way to measure privacy concern scores that is related to these factors by applying effective quantitative research.

LITERATURE REVIEW

The study reviews previous studies on privacy concepts and information disclosure related to children's online behavior. An important aspect concerning children's behavior on the Internet relates to the relevant theories and models. This study identifies and highlights some of these models and their constructs that could affect children's behavior on the Internet.

Privacy

Information privacy refers to the collection of information, unauthorized use, errors, and improper access beyond an individual's control in which personal information is released (Buchanan et al., 2007). In the legal context, the right to be left alone is considered to be largely synonymous with privacy (Li et al., 2015). However, others have since argued that privacy is solely the right to prevent the disclosure of personal information to others (Buchanan et al., 2007). Shin and Ismail (2014) considered privacy as a due enabling user to have control of disclosures, control of personal data, and the right to be left alone. Privacy is also defined as the "interest individuals have in sustaining personal space free from interference by other people and organizations" (De Souza & Dick, 2008). Information privacy is regarded as an individual's desire to control or influence one's personal information (Lankton et al., 2017). In most cases, personal information is considered to be information that, without proper control, may expose users to unauthorized access or to people with malicious intent, with this referring to shared content (e.g., photos, one's location, and videos) (Silva et al., 2017). For this reason, privacy is a critical issue (Silva et al., 2017). Teenagers and children are a particularly vulnerable user group in relation to privacy violation, as they usually share personal data publicly and can be duped by malicious users or more easily induced by them to share such data (Silva et al., 2017).

Many authors have highlighted privacy risk, with this referring to privacy disclosure associated with online users' expectations of losses arising from the abuse of personal information and opportunistic behavior. The largest risk perceived by users would be due to losses caused by the disclosure of personal information (Xu et al., 2016). The existence of the relationship between privacy concern and privacy risk has been confirmed by many scholars. Xu et al. (2016), without mentioning the causation relationship, provided evidence of a positive relationship between privacy risk and the abuse of personal information. Evidence has also been provided of the positive effect on privacy risk at the level of privacy concerns of Internet users (Xu et al., 2016).

A relationship was found between privacy risk and privacy concerns in (Jordaan & Van Heerden, 2017), in exploring a process to protect individuals' personal information from unwanted viewers through altering individuals' online privacy behavior. In their study on the privacy of children's information, Lwin et al. (2012) found that reduced perceived risks increased the likelihood of risky behaviors, while personal information disclosed in a manner consistent with the level of children's privacy concerns was likely as privacy concerns promoted risk-reducing behaviors. Children's willingness to disclose personal information decreased as their privacy concerns increased (Lwin et al., 2012).

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Information Disclosure

Information disclosure refers to the degree and quantity of sensitive information released by individual users about themselves (De Souza & Dick, 2009). In other words, a composite variable based on the sensitivity and amount of information disclosed by users is called information disclosure (De Souza & Dick, 2009). For making online purchases or personalizing these services (e.g., through recommendations or "one-click" purchasing) or for accessing online services (e.g., via the ubiquitous registration form), a prerequisite disclosure is often requested (Joinson et al., 2010).

Privacy, in terms of the disclosure of personal information, is another aspect to consider, as discussed above. This involves the self-disclosure of personal information (Li et al., 2016), defined as communication by people about themselves with other people (Li et al., 2016). Intimacy and sensitivity are two features of information which appear to be critical to information disclosure, with privacy disclosure related to the level and type of information that an individual is willing to divulge to another (Li et al., 2016).

In communication theory, the connection between attitudes towards privacy and information disclosure has been widely explored (Stutzman et al., 2011). Stutzman et al. (2011) in his original theorization of privacy postulated that individuals attempt to strike a balance between disclosures necessary for communication and individual privacy control mechanisms, with this being a general optimization function. As such disclosures are innately linked to practical mechanisms that adjust our disclosures with respect to our goals, privacy attitudes, and knowledge, the social individual must disclose this information (Stutzman et al., 2011).

A developing body of research has examined the consequent outcomes of the preponderance of involvement by users in these behaviors (Bryce & Fraser, 2014). For example, a recent study found that 29% of those aged 11–16 years in the United Kingdom (UK) had interacted with someone online with whom they had no prior contact. In addition, 36% had accepted friend requests from someone they had never met face to face, while 14% had disclosed personal information (e.g., address or phone number) to someone they had met online. Other studies have reported prevalence rates of 28% for cyber bullying (Bryce & Fraser, 2014). Evidence has revealed that to reduce anonymity and to establish the identities of young people and adults, they are required to reveal personal information on their online profiles as proof of inclusion (Bryce & Fraser, 2014). A recent study found that in the UK only 7% of those aged 9–16 years had been deceptive with regard to their online information (Bryce & Fraser, 2014). What this suggests is that most young people communicate personal information on their online profiles to set up their identity, rather than exploiting the anonymity provided by the online environment to engage in deceptive behavior (Bryce & Fraser, 2014).

Children's Behavior on the Internet

A complete revolution has occurred in technology during the past two decades, in this new move towards a digital age. What we are now witnessing is a new era of childhood, one which takes place in the digital world (Annansingh & Veli, 2016). The effect of the use of the Internet has been of great interest, as is evident in the recent literature (Bannon et al., 2015). This includes inquiries into its potential benefits from emotional and psychosocial points of view (Bannon et al., 2015). However, what still remains a concern is the negative psychological effect

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

of the Internet on young people and their online risk (Bannon et al., 2015). Findings of Bannon et al. (2015) indicated that 93% of US children aged from 12-17 years were using the Internet in 2009, while 60% of a pan-European sample of young people (aged 9-16 years) were shown to be online almost every day. Concerns regarding the susceptibility of young consumers with regard to their privacy and safety have also increased as a result of the increase in the number of youth and children engaged in online activities (Lwin et al., 2012).

Annansingh and Veli (2016) provided statistics showing that, while 75% of those aged 9–19 years had domestic Internet access, 37% of those aged 5–6 years, 64% of those aged 7–8 years, and 67% of those aged 8–10 years had never been unaccompanied to the shop or the local town. Overall, 92% had access through schools and at least 84% were Internet users as a matter of custom (Annansingh & Veli, 2016). Indeed, while society has made efforts to provide protection to children from external physical risks, less attention has been focused on their interactions through technology (Annansingh & Veli, 2016), even though the number of children using the Internet has been increasing (Bryce & Fraser, 2014; Annansingh & Veli, 2016; Kim et al., 2017; Andrews et al., 2020). As observed by Bremer (2005), a renowned expert in the field of computers and artificial intelligence (AI) stated that: "[t]here is a passionate love affair between children and computers across the world ... they seem to know that in a deep way it [computer technology] already belongs to them. They know they are the computer generation" (Bremer, 2005).

The techniques and tactics used to collect information through acquisition systems and advanced data mining have become easier to employ (Andrews et al., 2020). With regard to children, evidence has shown that data collection is carried out when interaction occurs between children and fictitious marketing characters when children provide personal data for social networking sites and register for websites or contests (Andrews et al., 2020). A study found that 25% of children's websites offer memberships for children under the age of 12, while 73% of such websites use online games (Andrews et al., 2020). As they are often naive, children become easy targets for information gatherers (Andrews et al., 2020).

Technology Adoption Theories and Models

This section provides and reviews two behavior theories that were applied in the current study. These theories have been used to study users' behavior in terms of their use of Internet services and other technologies.

Coping theory

Coping theory describes the processes through which individuals frame and respond to disruptive events in their environment (Bhattacherjee et al., 2018). This process describes which individuals frame their understanding and how they use this frame to respond to disruptive events in their external world (Bhattacherjee et al., 2018). Coping can be defined as "cognitive and behavioral strategies used by people in an effort to manage specific external and/or internal pressures that are known to be distressing, because they exceed the resources and the capacity of the person to cope" (Bhattacherjee et al., 2018). The idea of coping has been with us for many decades, becoming a prominent concept in the 1960s and 1970s through the growing interest in the effect of stress (Lazarus, 1993). If we think of coping as a broad concept including ego-

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

survival mechanisms and focused on threats to one's psychological nature, then the psychoanalytic concern about defense could be perceived as its historical forerunner (Lazarus, 1993).

Internal demands refer to the personal domain and involve matters such as obligations and a need to achieve fame or to face challenges, while external demands refer to those demands that come from the external world, and concern matters such as job requirements, expectations of parents, and even social pressures (Bhattacherjee et al., 2018). These demands on a person can be termed "disruptive events" especially if they go beyond that person's resources and ability to manage them (Bhattacherjee et al., 2018). Coping theory explains how people can respond to, or cope with, the excessive stress of disruptive events (i.e., their coping responses), and considers a person's ethical, cognitive, financial, social, and physical resources that he/she has at their disposal (Bhattacherjee et al., 2018). It must be borne in mind that these resources are not distributed uniformly among people and, in a given population; different individuals may have different and unique ways to cope with a stressful event (Bhattacherjee et al., 2018).

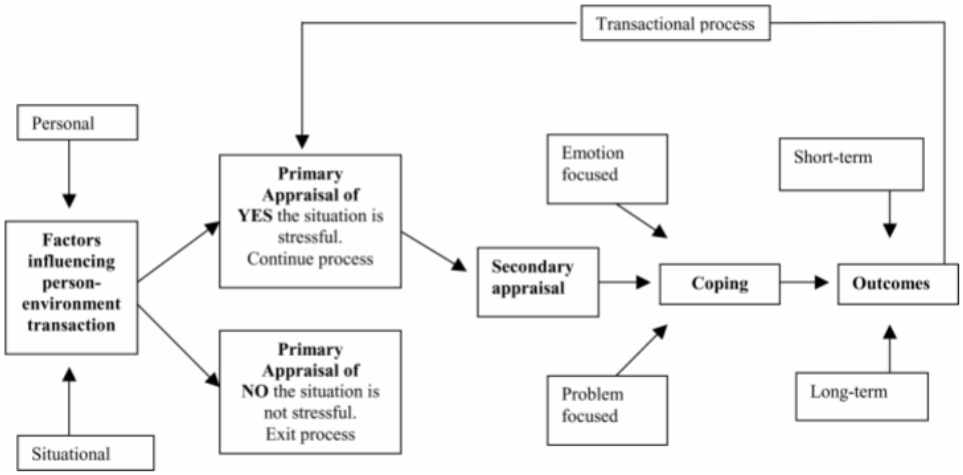

FIGURE 1

TRANSACTIONAL STRESS/COPING MODEL USED TO GUIDE CURRENT RESEARCH

Source: Theory developed by Lazarus and Folkman (1984)

Lazarus and Folkman's model, as shown in Figure 1, constitutes a specific type of coping mechanism identified by coping theory (Krohne, 2022). This theory may be identified and subsumed under two broad independent parameters: (a) strategies that are trait-oriented versus those that are state-oriented, and (b) approaches that are microanalytic versus those that are macroanalytic (Krohne, 2022).

The trait-oriented (otherwise referred to as dispositional) strategy for coping seeks to make early identification of those people whose coping capacity and behavioral inclinations are inadequate to address the demands of a specific stressful situation (Krohne, 2022). The state-oriented approach examines the relationships between coping mechanisms used by people and

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

the related outcome variables (Krohne, 2022). These outcome variables, such as self-reported or objectively evaluated efficiency in emotional reactions, accompany and result from certain coping efforts, coping, or variables stemming from a capacity to adapt to situations (e.g., health status or test performance) (Krohne, 2022). This type of research seeks to lay the foundation for a general program to improve coping efficiency (Krohne, 2022).

The microanalytic approach focuses on a range of many different coping strategies, whereas the macroanalytic approach, invariably concentrating on more important constructs, functions at a higher level of abstraction (Krohne, 2022). More recently, two new theoretical models were identified and explained, with the literature referring to these models published in 2014 (Brand, 2017). The first model was introduced by Brand (2017). Shortly afterwards, Dong and Potenza published their research on another model, based on the concept of Internet gaming disorder (Dong & Potenza, 2014). A conceptual model with cognitive–behavioral elements was formulated to describe Internet gaming disorder, based on an analysis of the relevant extant literature (Dong & Potenza, 2014). The model referred to the following three domains and their contributions to addictive behaviors (Dong & Potenza, 2014): (1) motivational drivers linked to stress reduction and reward seeking; (2) behavioral control as it related to executive inhibition; and (3) decision-making strategies that involved the assessment of merits and demerits for people with motivated behaviors (Dong & Potenza, 2014). The model (Dong & Potenza, 2014) could be used in behavioral therapies to influence these domains in the clinical treatment of Internet gaming disorder (Dong & Potenza, 2014).

The model recommended by Brand et al. (2017) distinguished between a generalized addiction to the Internet and a more specific type of Internet addiction. This distinction was inspired by the differentiation between types of Internet addiction. In reference to this context, a situation describing multidimensional misuse of the Internet refers to generalized Internet addiction, which is usually accompanied by time-wasting and non-directed use of a variety of Internet applications, such as YouTube, social networking sites (SNSs), music sites, and information-searching sites, etc. (Brand et al., 2017). Primary difference between the generalized versus the specific types of Internet addiction is that people subject to generalized Internet addiction would not have developed these problematic behaviors without the attraction of the Internet itself. In contrast, individuals blighted by the specific type of Internet addiction would have developed similar unwanted behaviors in another setting (e.g., shopping offline, gambling offline, etc.) (Brand et al., 2017). The reference to the specific type of Internet addiction refers to an addictive misuse of one specific area of online applications, such as game sites, gambling sites, shopping sites, or social networking and communication sites (Brand et al., 2017).

Theory of planned behavior (TPB)

The theory of planned behavior (TBP) Ajzen (1991) describes a model that seeks to explain how human action is guided (Figure 2) by predicting the occurrence of a specific behavior, given the condition that this behavior is intentional. This model appears within three variables, claimed by the theory to predict the intention which will result in a behavior. Intentions are known to be the forerunners of behavior (Ajzen, 1991). This theory is true to its goal of not simply predicting human behavior, but also explaining it. At a basic level of explanation, the TPB states that behavior is the outcome of beliefs, salient information, past experiences, and memories relevant to a particular behavior (Ajzen, 1991). People can have a

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

variety of beliefs that influence a given behavior, but they are only able to hold a relatively small number of beliefs at any given moment (Ajzen, 1991). Behavioral beliefs are assumed to affect attitudes toward a particular behavior, while normative beliefs comprise the underlying aspects of subjective norms, and control beliefs form the basis for perceptions related to behavioral control (Ajzen, 1991). All three kinds are types of salient beliefs (Ajzen, 1991). Attitudes towards a behavior are based on behavioral beliefs, described as the beliefs that a person holds about the likely effects from performing a specific behavior (De Leeuw et al., 2015). The expression, subjective norms, refers to the perceived social pressure experienced by people to perform or not to perform a particular behavior (Ajzen, 1991). Finally, perceived control refers to the outcome related to control beliefs, which involves perceptions, about the presence of elements which will facilitate or obstruct the adoption of a given behavior (De Leeuw et al., 2015).

The TPB model is applied in the current study to explain the behavior of children who use the Internet (Lankton et al., 2017). The deductive approach, when applied against the backdrop of the characteristics of social networks, enables the TPB model to be used to explain how the process of the self-disclosure of personal information by users of online social networking sites can happen (Lankton et al., 2017).

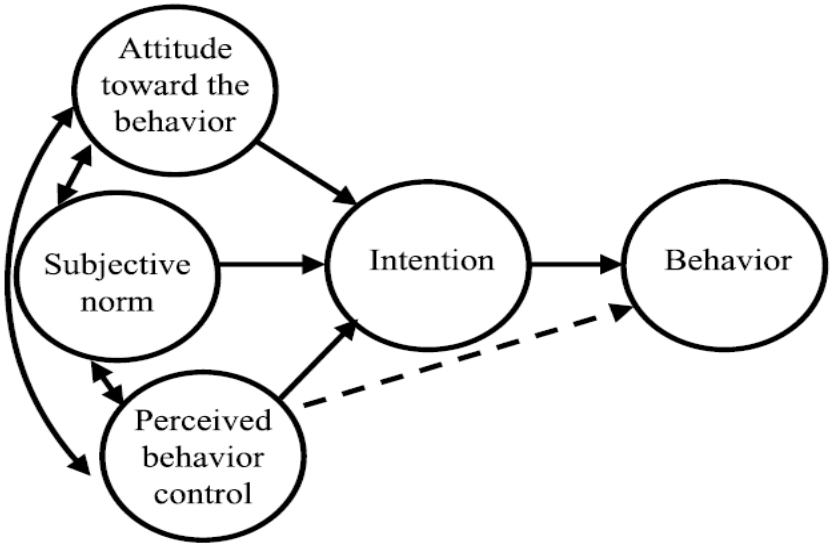

FIGURE 2

THEORY OF PLANNED BEHAVIOR (TPB)

Source: Xu et al., 2016

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

CONCEPTUAL MODEL AND HYPOTHESES DEVELOPMENT

Proposed Model

Based on the theory of planned behavior (TPB), coping theory, and the different factors related to children's behavior on the Internet, the study developed the model described below. As shown in Figure 3, this study leveraged privacy concerns and children's behavior to understand the effect of positive beliefs (parental control, content on the Internet), negative beliefs (information disclosure and privacy risk), and the role of social influence (subjective norms). Table 1 presents the explanation of the definitions of each construct in the model.

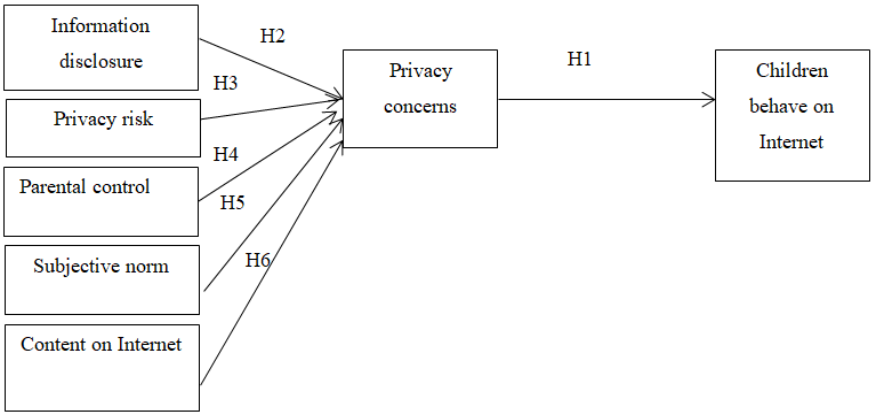

FIGURE 3

PROPOSED MODEL

TABLE 1
DEFINITIONS OF MODEL'S CONSTRUCTS

Concept	Definition
Information disclosure	"A complex variable based on the volume of information released and the sensitivity of the information shared and disclosed by the users" (Lwin et al., 2012).
Privacy risk	"The process of users' expectation of losses associated with the disclosure of private information online, and this is usually caused by opportunistic behavior and the abuse of personal information" (Xu et al., 2016).
Parental control	"When children are of an age to be able to give consent, online services have to supply comprehensive information to minors and also have parental permission to ensure that children are of the necessary age" (De Souza & Dick, 2009).
Subjective norms	This concept is derived from the field of sociology and psychology, with "subjective norms" a term popularly used in studies which have explored factors about certain **behaviors** which bears on people's attitudes (Xu et al., 2016).
Content on Internet	This relates to the content of the pages of the Internet which may have a detrimental effect on children, such as news feeds and games with questionable or dangerous content (Krasnova et al., 2010). Such content

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

	includes the content of social networking sites such as Facebook, which is used by children to exchange images, videos, and personal information about themselves or of others and to keep in touch with their friends (De Souza & Dick, 2009).
Privacy concerns	The users' serious concerns about risks to their privacy online (Xu et al., 2016).
Children's behavior on Internet	Parent's perceptions when the influence of the Internet appears in a child's behavior which depends partly on the nature of the content (benefits or dangers) (Bremer, 2005).

Proposed Hypotheses

Privacy concerns

An individual's level of privacy concerns acts as a motivation for that individual to protect himself/herself from risks to his/her privacy (Xu et al., 2016). Researchers have indicated their belief that the increase in consumers' concerns with respect to marketers' data collection and sharing practices is likely to lead to the adoption of privacy protection behaviors (Xu et al., 2016; Lankton et al., 2017). Privacy concerns act as a motivator for users to take steps in reaction to the security of their privacy, in addition to taking care of their personal information (Xu et al., 2016).

With privacy concerns leading to the promotion of risk-reducing behaviors, the possibility exists that children will reveal information in a manner consistent with their level of privacy concerns as reduced perceived risk increases the possibility of behaviors that are risky (Xu et al., 2016).

H1: Privacy concerns will have an effect on children's behavior on the Internet.

Information disclosure

Information disclosure involves the opportunity for you to present yourself in the way that you want others to see you (Shin & Ismail, 2014). The misuse of personal information is an issue that is of concern (Shin & Ismail, 2014). The reason is that online Internet connections are much more relaxed than offline connections (Shin & Ismail, 2014). Information that is personal and sensitive is frequently given to a range of nodes in the network that are not friends of the individual (Shin & Ismail, 2014). Many children provide their name and clear demographic information on the Internet, such as their age and geographic location (Xu et al., 2016).

H2: Information disclosure will have an effect on the level of privacy concerns.

Privacy risk

Privacy risk is attributed to users' expectations with regard to losses associated with privacy disclosure online, with such losses being the result of misuse of personal information and opportunistic behavior (Li et al., 2015). The higher the losses from the disclosure of personal information, the higher the risk perceived by users and the more factors affecting the privacy of children. One study has provided the expected outcomes as influenced by external variables (Xu

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

et al., 2016). It is also assumed that the level of privacy concerns is the result of perceived risk and the perceived influence of website features and the networked environment.

H3: Privacy risk will have an effect on privacy concerns.

Parental control

As depicted in the media and as supported by evidence in the literature, parents may possibly to be unaware of the activities of their children (Shin & Ismail, 2014): "[p]arents [are] shouldering the major responsibility for controlling their children's access to the Internet and this feature most public [;] however, initiatives still rely on it" (Shin & Ismail, 2014).

On average, a child spends five hours on the computer, watching television, or doing homework while, for 76% of the day, the child is relatively inactive (Bremer, 2005). Concerns have been expressed about the additional risks affecting children as computer users, with these including back strain, carpal tunnel syndrome, and eye strain leading to vision deterioration (Bremer, 2005). Parents have several possible reasons for not giving enough attention to what their children are doing online (Shin & Ismail, 2014). All too often the level of computer literacy of parents is less than that of their children, thus making them feel unable to monitor their children's online activities. Many parents are unaware of the risks faced by their children when they go online, permitting them access to the Internet without any limit and without any supervision (Shin & Ismail, 2014).

H4: Parental control will have an effect on the level of privacy concerns.

Subjective norms

The culture of a society has an important impact on the disclosure of information by people in social networks (Xu et al., 2016). Children are more likely to participate on social network sites where their classmates are already members. Also Xu et al. (2016) believed that when users voluntarily revealed their personal information, they related their behavior to the trust established with other users on the network. The tendency is for everyone to share real personal information with one another on a given social network site, with such behavior viewed as the subjective norms on that site (Li et al., 2015).

H5: Subjective norms will have an effect on privacy concerns.

Content

Content is an important factor affecting children's behavior (Lwin et al., 2012). Concerns have been expressed with respect to online predators, with policy makers also worried about the susceptibility of children to online marketers whose goal is to collect information regarding this important segment (Lwin et al., 2012). The collection of children's personal information by marketers has been the subject of criticism by privacy advocates who consider this to be an intrusion into children's privacy (Bremer, 2005; Lwin et al., 2012). The content on the Internet could possibly be beneficial or harmful (Lwin et al., 2012).

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Children may place their confidence in technologies without fully realizing the dangers and implications (Andrews et al., 2020). Some content is dangerous to children, such as exposure to potentially harmful content, encountering hate, racist, or violent material, exposure to illegal content, misinformation, challenging content (e.g., about anorexia, suicide, drugs, etc.), and (problematic) user-generated content (Tecson-Turano, 2017). Indeed, 85% of parents are of the opinion that the content of the Internet (e.g., photos, games, videos, etc.) presents the most risk for their children and is more dangerous than television (Lwin et al., 2012).

H6: The content of the Internet will have an effect on the level of privacy concerns.

METHODOLOGY

Type of Study

The current study applies a quantitative positivist methodology (Cresswel, 1994). With the study's focus being on exploring privacy concerns and effects on children's online behavior, the purpose of this type of study, which is to determine the objectives and examine the topic within the backdrop of social reality, is aligned with that of the current study. This study attempts to understand the phenomenon by measuring variables, testing theories, and making generalizations based on data from a sample of a fixed population to increase the predictive potential. This methodology has been selected as it has been proven reliable and has sound construct validity (Cresswel, 1994). Quantitative research methods include tools such as surveys, numerical techniques such as mathematical modeling, and laboratory experiments (Cresswel, 1994).

This study uses a survey method to gather data from individuals. Surveys can support a variety of research purposes and can be conducted in many different ways (Cresswel, 1994). The different types of data collected by surveys of a sample include information about attitudes, beliefs, resource possession, values, socio-economic status, use of time, characteristics of members of social networks, and self-reports of behavior (Cresswel, 1994). We used an online survey method with a questionnaire that was Web-based and accessed through an ULR link (Alkhalifah, 2017).

Data Collection

This section describes the study's data collection design process. The data collection procedure comprises the sampling technique, targeted population, and questionnaire development.

Target population

The target population is about 500 parents of children from Saudi Arabia. Table 2 presents the demographic statistics of participants. As this study uses structural equation modeling (SEM) and confirmatory factor analysis (CFA), this number is roughly suitable (Chin et al., 2003). According to Chin et al. (2003), a typical sample size in studies where SEM is used is generally 1:5 for each item and the CFA sample ratio (Chin et al., 2003). Another study ranked sample size as follows "100 as poor, 200 as fair, 300 as good, 500 as very good, and 1000 or

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

more as excellent" (Williams, 2010). We chose parents as prior research has suggested that parents are more likely to be concerned about the effect of the Internet on their children's behavior (Lwin et al., 2012; Andrews et al., 2020). In addition, they are generally aware of their children's behavior on the Internet and they provide easy access for the questionnaire's distribution. When we talk about their children, they care about this topic.

TABLE 2
DEMOGRAPHIC PROFILE OF PARTICIPANTS

Item		Percentage (%)
Gender	Male	22.2
	Female	77.8
Age	20–30	27.7
	30–40	49.2
	40–50	19.2
	50–60	2
	60+	1
Education Level	Diploma	10.2
	Bachelor's degree	72.8
	Master's degree	5.3
	PhD	3
	Uneducated	1
	Other	0
How many children do you have?	1	21.7
	2	27.9
	3	19.5
	4	12.6
	5+	18.2
Children's average age (years)	0–5	34.8
	5–10	13.1
	10–12	25.2

Note: N=500.

Sampling techniques

As previously discussed, to collect data from parents concerned about their children's behavior on the Internet, we used a survey to gather information, focusing on an online survey method, with the questionnaire accessed through an UR link (URL). Two methods were used to disseminate information about the survey:

- Placing the link on Twitter (Retweet)
- Sending the link by email

The "snowball" sampling technique was used to identify parents with children aged from 6–12 (Alkhalifah, 2017). Snowball sampling is the process used to identify participants "through referrals made among people who share or know of others who possess some characteristics that

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

are of research interest" (Alkhalifah, 2017). This technique is suitable for the current study as it was difficult to obtain a list of targeted parents with children who would be willing to describe their perceptions and experiences (Alkhalifah, 2017). However, this method is not appropriate for collecting data that can be confidently generalized to larger populations; for example, the results show more female participants (77.8%) than male participants (22.2%) (Table 2). The reason is that mothers may focus more attention on their children, monitoring them more than their fathers. When we started collecting data from participants, we posed two questions to determine if the participant was a parent or not, asking them, firstly, "Are you a parent?" and, secondly, "Do you have a child?" If the participant answered "yes" to these two questions, he/she could continue answering the rest of the questions, and if their answer was "no", the participant was excluded from the survey. For this reason, about 105 participants were excluded.

Questionnaires

In this research, we adopted measures (items) and questionnaires that had already been developed and used in previous studies, with the current study also developing new measures (Table 3). Most adopted measures came from well-established literature sources with minor modifications made to ensure that they fit the context of our study, namely, children's behavior on the Internet. The study questionnaire comprised two sections. The first section sought participants' demographic information and comprised six questions: age, gender, education level, are you parents? do you have children? and how many children do you have? The second section comprised specific questions about children's behavior on the Internet, based on the factors identified earlier. The questionnaire was made available so participants could undertake the survey. The Likert scale was used to rate the responses on a scale of 1–5 as follows: 1. 'Strongly disagree;' 2. 'Disagree;' 3. 'Neither agree nor disagree;' 4. 'Agree;' and 5. 'Strongly agree'**.** The questionnaire was written in English and Arabic languages, as we wanted all parents to have the opportunity to participate. A pilot study was undertaken to further revise the scale items before collecting the data and analyzing the results. A total of 22 scale items were initially finalized, representing four items for each construct. Four scale items were subsequently dropped after pilot study feedback, leaving a total of 18 scale items (Table 3).

TABLE 3
ITEMS IN SURVEY QUESTIONNAIRE

Construct	Item code	Item in English	Source
Children's behavior on the Internet (CHB)	CHB1 CHB2 CHB3 CHB4	I will let my child use the Internet. Even if there is risk, I will let my child use the Internet. My child can use the Internet all the time. In the future, I will let my child share his/her information online.	Xu et al., 2016
Privacy (P)	P1 P2 P3	On the Internet, I feel my child's information is protected. I am concerned that unauthorized people may access my child's personal information. It is very important to be aware of why my child's information will be collected.	Xu et al., 2016

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Information disclosure (ID)	ID1 ID2 ID3	My child may disclose information more quickly. I don't care about my child's identity online. My child revealed her/his identity information to some of the Internet's websites threatening her/his safety.	Bryce & Fraser, 2014
Privacy risk (PR)	PR1 PR2 PR3	My child's information may be exploited online. Personal information of my child could be inappropriately used by websites. There would be high potential for unexpected problems when giving my children's personal information on websites.	Xu et al., 2016
Parental control (PC)	PC1 PC2 PC3	I have major responsibility for controlling my children's access to the Internet. I'm aware of the risks faced by my children online. I'm permitting my child access to the Internet with limits and with my supervision.	Xu et al., 2016
Subjective norms (SN)	SN1 SN2 SN3	My child tends to share his/her real personal information with their friends on the Internet. People who influence my behavior think that keeping personal information private is very important. My child's use of the Internet is affected by her/his friends' opinions.	Xu et al., 2016
Content (C)	C1 C2 C3	Online content affects the behavior of my children. I control every content that my child can see. I'm using programs for filtering inappropriate content.	De Souza & Dick, 2009; Nyst, 2017

DATA ANALYSIS AND RESULTS

This study used structural equation modeling (SEM) which is "a statistical method for testing and estimating causal relationships using a combination of statistical data and qualitative causal assumptions" (Chin, 1998). The SEM approach is often used in research with partial least squares (PLS) as it can test additive causal models and theoretically support linear regression (Chin, 1998). Research conducted using this method has produced high-quality statistical analysis (Chin, 1998). The SEM technique is carried out through the measurement of items, after which they are statistically tested (Chin, 1998).

The measurement model (Figure 4) was developed using SmartPLS 3.0 software <www.smartpls.de>. The stability of the scale was tested using confirmatory factor analysis (CFA). The pattern of loadings of the measurement items on the latent constructs is explicitly specified in the model (Chin, 1998). The fit of this pre-specified model is then examined to define both its discriminant validity and its convergent validity (Chin, 1998). This factorial validity deals with whether the theoretically anticipated factors and the pattern of loadings of the measurement items correspond to each other (Chin, 1998). These two elements of factorial validity can and must be examined in PLS, as must also be undertaken with latent variables in general (Chin et al., 2003). The two elements, convergent validity and discriminant validity (also

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

known as construct validity), are components of a larger scientific measurement concept (Chin, 1998). These two types of validity indicate how well the measurement items are captured in relation to the constructs as well as to some aspects of the measurement model's goodness of fit (Chin, 1998). Each measurement item correlates strongly with the one construct to which it is related, while it does not significantly correlate with all other constructs or correlates weakly with them (Chin, 1998). To test the adequacy of the first-order construct measures, reliability, convergent validity, and discriminant validity were examined based on the criteria suggested by Fornell and Larcker (1981 and Chin (1988) as illustrated in Table 4.

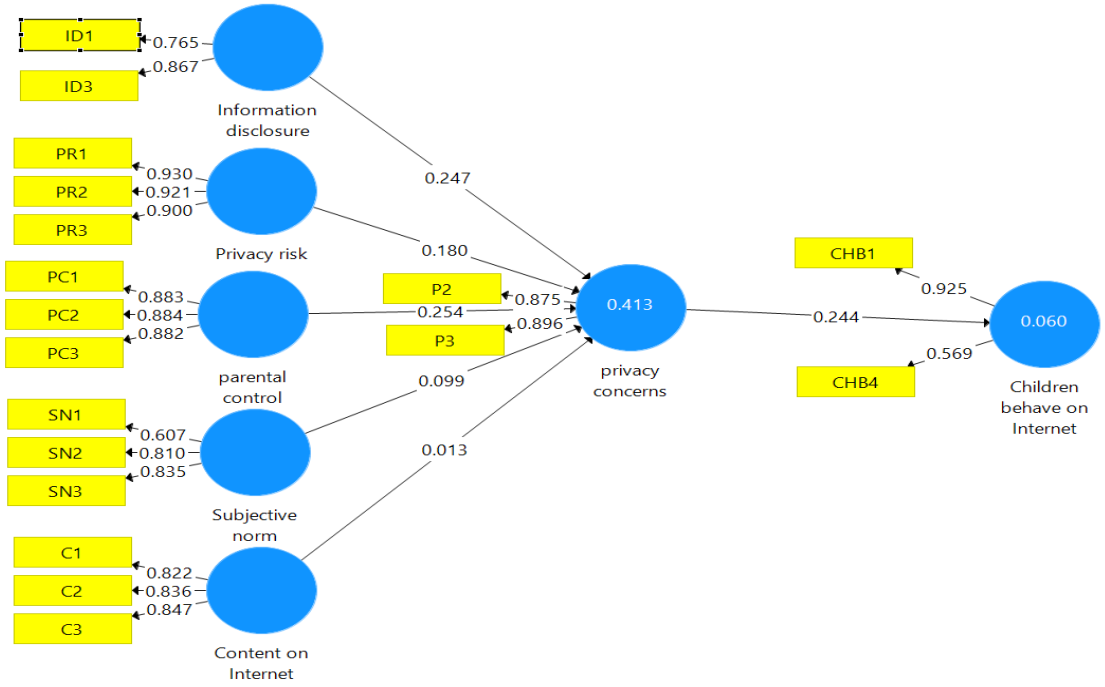

FIGURE 4

PLS MODEL RESULTS

TABLE 4
RELIABILITY AND VALIDITY

What to check?	What to look for in SmartPLS?	Where is it in the report?	Is it OK?
Reliability			
Indicator Reliability	"Outer loadings" numbers	PLS>Calculation Results>Outer Loadings	"Square each of the outer loadings to find the indicator reliability value." "0.70 or higher is preferred. If it is an exploratory research, 0.4 or higher is acceptable."
Internal Consistency Reliability	"Reliability" numbers	PLS>Quality Criteria>Overview	"Composite reliability should be 0.7 or higher. If it is an exploratory research, 0.6 or higher is acceptable."

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Validity			
Convergent Validity	"AVE" numbers	PLS>Quality Criteria>Overview	It should be 0.5 or higher (Fornell & Larcker, 1981)
Discriminant Validity	"AVE" numbers and Latent Variable Correlations	PLS>Quality Criteria>Overview (for the AVE number as shown above) PLS>Quality Criteria>Latent Variable Correlations	Fornell and Larcker (1981) suggest that "the square root of AVE of each latent variable should be greater than the correlations among the latent variables."

Source: adopted from (Chin, 1998) and (Fornell & Larcker, 1981)

Reliability is the word used to define the degree to which scale items are free from error and, therefore, the extent to which they yield consistent results (Chin, 1998). This study modeled all underlying constructs as reflective variables (Figure 4). As shown in Table 6, all item loadings exceeded the cut-off value of 0.6. Table 5 shows the results of the pilot study. Four items (ID2, P1, CHB2, CHB3) were deleted and not analyzed due to their low loading. Cronbach's alpha coefficient values were above 0.7 for all constructs except 'information disclosure' ($\alpha = 0.5$) and 'children's behavior on Internet' ($\alpha = 0.35$); although they had values less than 0.6, this was considered acceptable (Straub et al., 2004). Composite reliability (CR) was above the cut-off value of 0.7 for all constructs (Fornell & Larcker, 1981; Chin, 1998). The highest CR value was 0.941 for 'perceived risk', whereas the lowest CR was 0.732 for 'information disclosure' and 'children' behavior on Internet.' Therefore, the reliability was judged to be satisfactory.

TABLE 5
SUMMARY OF RESULTS FOR REFLECTIVE OUTER MODELS (PILOT STUDY)

	AVE	CR	Cronbach's alpha	Item loading	Mean	Loading
Information disclosure	0.442	0.594	0.324	ID1 ID2 ID3	3.01 1.88 3.64	0.756 -0.057 0.867
Privacy risk	0.841	0.941	0.905	PR1 PR2 PR3	3.25 3.35 3.56	0.930 0.921 0.900
Parental control	0.780	0.914	0.859	PC1 PC2 PC3	3.99 3.85 3.93	0.883 0.884 0.883
Subjective norms	0.574	0.799	0.641	SN1 SN2 SN3	2.55 3.18 3.21	0.612 0.807 0.835
Content on Internet	0.698	0.874	0.788	C1 C2 C3	3.80 3.37 3.55	0.819 0.838 0.849
Privacy concerns	0.537	0.740	0.546	P1 P2 P3	2.23 3.32 3.74	0.221 0.873 0.895

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Children's behavior on Internet	0.243	0.274	0.538	CHB1 CHB2 CHB3 CHB4	2.88 1.64 1.73 2.30	0.827 -0.194 -0.058 0.469

TABLE 6
SUMMARY OF RESULTS FOR REFLECTIVE OUTER MODELS

	AVE	CR	Cronbach's alpha	Item loading	Mean	Loading
Information disclosure	0.668	0.732	0.509	ID1 ID3	3.01 3.64	0.875 0.896
Privacy risk	0.841	0.941	0.905	PR1 PR2 PR3	3.25 3.35 3.56	0.930 0.921 0.900
Parental control	0.780	0.914	0.859	PC1 PC2 PC3	3.99 3.85 3.93	0.883 0.884 0.882
Subjective norms	0.574	0.799	0.641	SN1 SN2 SN3	2.55 3.18 3.21	0.607 0.810 0.835
Content on Internet	0.698	0.874	0.788	C1 C2 C3	3.80 3.37 3.55	0.822 0.836 0.847
Privacy concerns	0.784	0.879	0.725	P1 P3	3.32 3.74	0.875 0.896
Children's behavior on Internet	0.590	0.732	0.354	CHB1 CHB2	2.88 2.30	0.925 0.569

The study also calculated the average variance extracted (AVE) value to confirm convergent validity. As shown in Table 6, the AVE for each construct was greater than the cut-off value of 0.60, thus suggesting good convergent validity (Fornell & Larcker, 1981). We calculated the square root of the AVE values of the correlation matrix as shown in the diagonals in Table 7. These values were greater than the relationship of the construct with the other variables in the first-order model. This indicates that each item loaded more on its relevant construct than on other constructs. Therefore, discriminant validity was confirmed.

TABLE 7
CORRELATIONS OF THE FIRST-ORDER MODEL

	Children's behavior on Internet	Content on Internet	Information disclosure	Privacy concerns	Privacy risk	Subjective norms	Parental control
CHB	**0.768**						
CI	0.154	**0.835**					
ID	0.207	0.480	**0.817**				
P	0.244	0.459	0.545	**0.886**			

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

PR	0.104	0.551	0.653	0.534	**0.917**		
SN	0.312	0.498	0.486	0.432	0.515	**0.757**	
C	0.196	0.707	0.497	0.526	0.531	0.449	**0.883**

Hypotheses Testing

The study calculated the path coefficients (beta coefficients) between the latent constructs for all endogenous variables (Chin, 1998). An endogenous variable (or construct) is a dependent variable which has at least one causal relationship. In terms of a path diagram, the endogenous variable is based on the inputs of one or more other variables (i.e., a construct which has one or more arrows leading to it) (Straub et al., 2004). Furthermore, non-parametric bootstrapping was carried out using 500 cases and 1,000 samples to obtain the significance of each structural path (i.e., the *t*-value) between the constructs (Straub et al., 2004). Table 8 shows the results of the path analysis and hypotheses testing. Based on the inner model suggestion, 'parental control' has the strongest effect on privacy concerns (0.254), followed by 'information disclosure' (0.247), and 'privacy risk' (0.180), 'subjective norms' (0.099), while the weakest effect is that of 'content on Internet' (0.013). The effect of privacy concerns on children's behavior on the Internet at 0.244 is statistically significant (0.99). All loadings of the constructs were significant at $p < 0.001$ except 'content on Internet' (Fornell & Larcker, 1981; Chin, 1998). However, the hypothesized path relationship between 'content on Internet' and 'privacy concerns' is not statistically significant, as shown by its standardized path coefficients (0.013) being lower than 0.05 (Chin, 1998). Therefore, Hypotheses H1, H2, H3, H4, and H5 were supported, while H6 was not confirmed.

TABLE 8
RESULTS OF THE STRUCTURAL MODEL AND HYPOTHESES TESTING

Hypotheses	Associations	Path Coefficients	*t*-value	Supported
H1	Privacy concerns ⟶ Children's behavior on Internet	0.244	5.784	yes
H2	Information disclosure ⟶ Privacy concerns	0.247	4.89	yes
H3	Privacy risk ⟶ Privacy concerns	0.18	3.159	yes
H4	Parental control ⟶ Privacy concerns	0.254	4.493	yes
H5	Subjective norms ⟶ Privacy concerns	0.099	0.046	yes
H6	Content on Internet ⟶ Privacy concerns	0.013	0.234	No

DISCUSSION

This section discusses the results and compares the study's findings with those of previous studies on factors that influence children's behavior on the Internet. The main objective of this study was to investigate children's behavior in terms of information sharing via the Internet. The study explored different factors that could impact on privacy concerns and examined their effects on children's behavior. It then developed a model based on previous studies to test the proposed hypotheses.

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Privacy concerns affect children's behavior on the Internet

This study found that privacy concerns affect children's behavior on the Internet (β = 0.244) (H1). This finding is in contract with our hypothesis. The study's hypothesis proposed that privacy concerns will have an effect on children's behavior on the Internet as privacy concerns lead to the promotion of risk-reducing behaviors, and as perceived risk reduces the possibility of behaviors that are risky increases. One paper confirms that children will reveal information in a manner consistent with their level of privacy concerns (Xu et al., 2016).

Information Disclosure Affects Privacy Concerns

The study found that information disclosure has a positive effect on privacy concerns (β = 0.247) (H2). This finding confirms our hypothesis, implying that information disclosure, as perceived by users, remains the core determinant of, and lends further support to, previous planned behavior studies that came to similar conclusions. This also took into account that many of the children gave their names and clear demographic information on the Internet, such as age and geographic location (Xu et al., 2016). Based on the results of that study, this finding confirms H2 in the current study (Xu et al., 2016).

Privacy Risk Affects Privacy Concerns

The study found that privacy risk has a positive effect on privacy concerns (β = 0.180) (H3). This finding confirms the study's hypothesis. This indicates that the higher the losses from disclosing personal information, the higher the risk perceived by users (Shin & Ismail, 2014). One study provided evidence of the positive effect of perceived risk as these concerns made users unsure about the overall protection of their sensitive information (Xu et al., 2016). This finding is consistent with the argument that privacy concerns related to disclosing various types of personal information online have gained in importance (Xu et al., 2016).

Parental Control Affects Privacy Concerns

Hypothesis H4 hypothesized that parental control will have an effect on the level of privacy concerns. The results of the study confirmed this hypothesis (β = 0.254) (H4). The hypothesis proposed that parental control will have an influence on the level of privacy concerns as it is possible for parents to be aware of their children's activities (Shin & Ismail, 2014). This finding was confirmed: the reason could be that study participants had strict control over their children and that if the study were conducted in different societies, it may show different results.

Subjective Norms after Privacy Concerns

The study's results show that subjective norms will have a positive effect on privacy concerns (β = 0.099) (H5); thus, this hypothesis is supported. The reason could be that users who voluntarily reveal personal information relate their behavior to the confidence established with other users in the network (Xu et al., 2016). This result also confirms the results of previous studies that found subjective norms to be positively related to privacy concerns (Shin & Ismail, 2014; Xu et al., 2016).

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Content on the Internet Affects Privacy Concerns

Hypothesis H6 of the study was that the content of the Internet will have an effect on the level of privacy concerns. This hypothesis was not supported by the study's findings ($\beta = 0.013$) (H6). This finding could be due to parents seeing that their children may have placed their confidence in technologies without fully realizing the dangers and implications (Lwin et al., 2012). From the parents' perspective, content is more dangerous and poses the most risk for their children.

CONTRIBUTIONS AND IMPLICATIONS

The study has made the following contributions to, and has the following implications for, research, practice, and society.

Research Field

This study has developed a model by identifying the factors that have the potential to reduce risk on the Internet. Few researchers have been interested in children's behavior on the Internet (Bremer, 2005; Lwin et al., 2012; Bannon et al., 2015; Annansingh, & Veli, 2016; Wojniak & Majorek, 2016; Andrews et al., 2020). Some have identified factors such as privacy and information disclosure when seeking information aimed at studying children's privacy concerns. The current study empirically explored and measured different factors and their effects on privacy concerns leading to a better understanding of children's behavior on the Internet. The study provides a comprehensive explanation of how to evaluate factors with an impact on users' privacy concerns, specifically when these users are children.

Privacy concerns at the individual level focusing on consumers (Rath & Kumar, 2021), students (Xu et al., 2016), and citizens (Fox et al., 2021) have been widely addressed and explored in the research. Information privacy concerns in other contexts, such as among specific groups, ages, and societal levels need further research (Kokolakis, 2017; Rath & Kumar, 2021). Information privacy studies could address and explore data from a widely diverse range, such as gender, age, and income, instead of student-centric data (Rath & Kumar, 2021). This study has contributed to the literature by establishing the correlations between factors, addressed the gaps by applying SEM, and, specifically, the SmartPLS tool.

This study extends the theory of planned behavior (TBP) by integrating it with coping theory when considering the role of privacy concerns in relation to children's behavior on the Internet. Previous studies have employed and integrated the TPB to test privacy concerns in different contexts (Xu et al., 2016; Fox et al., 2021; Rath & Kumar, 2021). To the best of the authors' knowledge, no study has used the TBP to test children's behavior on the Internet and privacy. Examining privacy in the context of children is complex as it is difficult to measure their perceptions and beliefs. Therefore, the current study measured parents' beliefs as they are aware of and concerned about their children's behavior on the Internet (Andrews et al., 2020).

Practical Implications

Conceptual frameworks are lacking in relation to guiding parents on their children's behavior on the Internet. This study has developed a model by identifying constructs with the

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

potential to increase privacy and reduce risk on the Internet, and by specifying how these constructs could be combined with the theory of planned behavior (TPB). Although many researchers have examined factors such as content on the Internet (Andrews et al., 2020), information disclosure, etc. (Lwin et al., 2012) to aid in parents' general understanding and clarification on how to protect their children's privacy on the Internet, studies focusing on factors such as security, trust, and privacy have been limited. This study contributes to the literature by establishing the correlations between related factors such as privacy concerns, parental control, subjective norms, privacy risk, and children's behavior on the Internet, in addition to information disclosure, addressing this gap by examining parents' beliefs about these factors in the context of their children's behavior. The current study addresses this gap by applying SEM, and, specifically, the SmartPLS tool.

This study's findings are important for the design of privacy enhanced technologies (PETs) which are methods for protecting data in accordance with the law (Fox et al., 2021). Without losing the functionality of the information system (IS), PETs are important for online users as these technologies allow them to protect the privacy of personally identifiable information (PII) provided to and handled by services or applications (Van Blarkom et al., 2003). As Internet developments bring real or potential risks with regard to children's information disclosure and location disclosure in connection with data content transfer, linking data traffic with identity, children's profile disclosure, or information disclosure itself, PETs can contribute to an increase in parents' level of awareness of the need to protect their children's security and privacy (Van Blarkom et al., 2003). Also, PETs can help parents to control their children by preventing them from disclosing personal information on the Internet. In addition, PETs can help parents by address privacy risks, protecting their children's information and controlling their access to, and contribution to, content on the Internet. The adoption of PETs provides a solution to all privacy problems. This will help Web designers as application developers can take this into consideration, providing new designs.

Society

This study was designed to serve society by providing protection for children and their behavior on the Internet and connecting this aim with the technical domain through developing a model to measure perceptions of factors that could affect children's online behavior. The study has also contributed to parents' awareness, educating them about how they should protect their children's privacy on the Internet. This has been achieved by contacting parent study participants and obtaining their opinions about their children's behavior on the Internet. In addition, the study provides support to parents, helping to make the Internet more secure and trusted for their children.

CONCLUSION

The main objective of this study was to reduce the risk of the influences on children's behavior on the Internet by understanding and analyzing factors that affect privacy concerns and children's behavior. The study developed a model to achieve this objective, measuring the perceptions of children from their parents' perspectives. The study used SEM with Smart-PLS software to analyze the results. The study discussed the research hypotheses and the findings,

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

comparing them with those of previous studies. As this study has presented observations related to the protection of the privacy of children's information and has studied some factors that can have an effect on their behavior, these topics will be of interest to researchers and practitioners in the general area of information systems (IS) and technology.

Inevitably, this study confronted several limitations. These are now outlined with suggestions for further improvements for future research. This study's potential methodological limitation was related to the online survey method. The study was conducted within about 500 parents (both male [N=111] and female [N=389]) on social networks. Therefore, a threat to the external validity of the study could be that the study's targeted participants do not equally represent both genders of parents. Thus, future research may consider the involvement of more parents, expanding the number of participants in the survey. Another methodological limitation related to the use of constructs and simple item scales; for example, we measured both privacy and information disclosure with two item scales. Future studies should determine more factors and additional variable measures.

Depending on the limitations mentioned above, future work could consider the following:

- Future research could involve and test more factors, such as trust, trust in the Internet, and personal traits.
- The proposed model could be developed and enhanced with other models such as the technology acceptance model (TAM), task technology fit (TTF), and social exchange theory (SET).
- Future research could apply new methods and techniques to test the model, such as the machine learning technique.

REFERENCES

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

Alkhalifah, A. (2017). A research Methodology to Explore the Adoption of E-Government. *International Journal of Computer Engineering and Information Technology*, *9*(9), 216.

Andrews, J. C., Walker, K. L., & Kees, J. (2020). Children and online privacy protection: Empowerment from cognitive defense strategies. *Journal of Public Policy & Marketing*, *39*(2), 205-219.

Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: a study of Devon, UK. *Interactive Technology and Smart Education*, *13*(2), 147-165.

Bannon, S., McGlynn, T., McKenzie, K., & Quayle, E. (2015). The internet and young people with Additional Support Needs (ASN): Risk and safety. *Computers in Human Behavior*, *53*, 495-503.

Bhattacherjee, A., Davis, C. J., Connolly, A. J., & Hikmet, N. (2018). User response to mandatory IT use: A coping theory perspective. *European Journal of Information Systems*, *27*(4), 395-414.

Brand, M. (2017). Theoretical models of the development and maintenance of internet addiction. In *Internet Addiction* (pp. 19-34). Springer, Cham.

Bremer, J. (2005). The internet and children: advantages and disadvantages. *Child and Adolescent Psychiatric Clinics*, *14*(3), 405-428.

Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computers in Human Behavior*, *30*, 299-306.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology*, *58*(2), 157-165.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, *295*(2), 295-336.

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information systems research*, *14*(2), 189-217.

Cresswel, J. W. (1994). Research design: Qualitative and quantitative approaches. *Amerika: SAGE Publications*.

De Leeuw, A., Valois, P., Ajzen, I., & Schmidt, P. (2015). Using the theory of planned behavior to identify key beliefs underlying pro-environmental behavior in high-school students: Implications for educational interventions. *Journal of environmental psychology*, *42*, 128-138.

De Souza, Z., & Dick, G. N. (2008). Information disclosure on MySpace–the what, the why and the implications. *Pastoral Care in Education*, *26*(3), 143-157.

De Souza, Z., & Dick, G. N. (2009). Disclosure of information by children in social networking—Not just a case of "you show me yours and I'll show you mine". *International Journal of Information Management*, *29*(4), 255-261.

Dong, G., & Potenza, M. N. (2014). A cognitive-behavioral model of Internet gaming disorder: Theoretical underpinnings and clinical implications. *Journal of psychiatric research*, *58*, 7-11.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 106806.

Ji, Z., Lipton, Z. C., & Elkan, C. (2014). Differential privacy and machine learning: a survey and review. *arXiv preprint arXiv:1412.7584*.

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.

Jordaan, Y., & Van Heerden, G. (2017). Online privacy-related predictors of Facebook usage intensity. *Computers in Human Behavior*, *70*, 90-96.

Kim, J. Y., Lee, J. S., & Oh, S. (2017). A path model of school violence perpetration: introducing online game addiction as a new risk factor. *Journal of interpersonal violence*, *32*(21), 3205-3225.

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

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, *25*(2), 109-125.

Krohne, H. W. (2002). Stress and coping theories. *International Encyclopedia of the Social Behavioral Sceinces*, *22*, 15163-15170.

Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior*, *76*, 149-163.

Lazarus, R. S. & Folkman, S. (1984). Stress, appraisal, and coping. New York: Springer Publishing.

Lazarus R. S. (1993). Coping theory and research: past, present, and future. *Psychosomatic medicine*, *55*(3), 234–247.

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & management*, *52*(7), 882-891.

Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. *Nankai Business Review International*, *7*(3), 282-300.

Li, P., Li, T., Ye, H., Li, J., Chen, X., & Xiang, Y. (2018). Privacy-preserving machine learning with multiple data providers. *Future Generation Computer Systems*, *87*, 341-350.

Livingstone, S., & Brake, D. R. (2010). On the rapid rise of social networking sites: New findings and policy implications. *Children & society*, *24*(1), 75-83.

Lwin, M. O., Miyazaki, A. D., Stanaland, A. J., & Lee, E. (2012). Online usage motive and information disclosure for preteen children. *Young Consumers*,*13*(4), 345-356.

Nyst, C. (2017). Privacy, protection of personal information and reputation rights. *Children's Rights and Business in a Digital World Discussion Paper Series*, 15.

Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. (2016). Towards the science of security and privacy in machine learning. *arXiv preprint arXiv:1611.03814*.

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.

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.

Shin, W., & Ismail, N. (2014). Exploring the role of parents and peers in young adolescents' risk taking on social networking sites. *Cyberpsychology, Behavior, and Social Networking*, *17*(9), 578-583.

Silva, C. S., Barbosa, G. A., Silva, I. S., Silva, T. S., Mourão, F., & Coutinho, F. (2017, June). Privacy for children and teenagers on social networks from a usability perspective: a case study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference* (pp. 63-71).

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information systems*, *13*(1), 24.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*(1), 590-598.

Tecson-Turano, C. (2017). Social Media as a Communication Tool to Support University Student-Services: Affordances, Limitations and Opportunities for Innovations. *International Journal of Information and Communication Sciences*, *2*(5), 75.

Van Blarkom, G. W., Borking, J. J., & Olk, J. E. (2003). Handbook of privacy and privacy-enhancing technologies. *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, *198*, 14.

Williams, B., Onsman, A., & Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. *Australasian journal of paramedicine*, *8*(3), 990399.

Wojniak, J., & Majorek, M. (2016). Children in internet space–the European Union policies on children's safety online. In *SHS Web of Conferences* (Vol. 26, p. 01048). EDP Sciences.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, *13*(2), 151-168.

Citation Information: Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective. *Journal of Management Information and Decision Sciences, 25*(1), 1-24.