frontiers | Frontiers in Psychology

ORIGINAL RESEARCH
published: 13 June 2022
doi: 10.3389/fpsyg.2022.880261

On Students' Willingness to Use Online Learning: A Privacy Calculus Theory Approach

*Xinyu Jiang[1], Tiong-Thye Goh[2] and Mengjun Liu[1]**

[1] School of Education, Hubei University, Wuhan, China, [2] School of Information Management, Victoria University of Wellington, Wellington, New Zealand

Online learning platforms frequently collect and store learners' data to personalize content and improve learning analytics, but this also increases the likelihood of privacy breaches which may reduce learners' willingness to use online learning. This study aims to examine how perceptions of benefits, privacy, risk, and trust affect students' willingness to use online learning. We used the Privacy Calculus Theory as a theoretical framework for this study. To test the model, we surveyed 203 undergraduate students who used online learning. The results of the AMOS analysis revealed that students' risk perception has a significant negative effect on their willingness to use online learning, while their benefit perception and trust perception have positive effects. Furthermore, the study found that improved trust can reduce perceived risk and improve willingness to use online learning. Interestingly, privacy perception is not a significant predictor of students' willingness to use online learning, although it is a high concern factor. Discussion and conclusion are discussed at the end.

Keywords: online learning, privacy calculus theory, benefit perception, risk perception, trust perception

OPEN ACCESS

Edited by:
Mohamed Rafik Qureshi,
King Khalid University, Saudi Arabia

Reviewed by:
Kuang-Ming Kuo,
National United University, Taiwan
Caroll Hermann,
University of Zululand, South Africa

****Correspondence:***
Mengjun Liu
lmj_whu@163.com

Specialty section:
This article was submitted to Educational Psychology, a section of the journal Frontiers in Psychology

Received: *01 March 2022*
Accepted: *18 May 2022*
Published: *13 June 2022*

Citation:
Jiang X, Goh T-T and Liu M (2022) On Students' Willingness to Use Online Learning: A Privacy Calculus Theory Approach. Front. Psychol. 13:880261. doi: 10.3389/fpsyg.2022.880261

INTRODUCTION

Since the COVID-19 pandemic started, online learning has largely replaced face-to-face instruction and has developed into a viable alternative to delivering instruction at all levels of education. Online learning platforms are advantageous in delivering rich, comprehensive, and personalized content to individuals by profiling learners' personal and behavioral data. While personalization can improve adoption, passive or active collection and storage of personal data increase the risk of data breaches. Because large amounts of confidential data are more attractive to hackers. Studies conducted by Bongiovanni (2019) and Osterman (2021) suggested that universities were not adequately protecting their computer assets. For instance, in May 2018, the security vulnerability of NetID, an online service system of the University of Vermont, compromised the personal data security of 37,000 current and former faculty members and students (Bongiovanni, 2019). In May 2019, the internal database of the Georgia Institute of Technology was attacked, resulting in the breach of 1.3 million data (Chapman, 2019). Most recently, a Spanish e-learning platform discovered a data breach affecting 150,000 users across the globe. In addition to personally identifiable data, students' account details including the courses they have taken, account user IDs, their evaluation scores, and certificates of completion were compromised (DataBreach, 2020). In March 2020, Zoom,

an application for online videoconferencing which was widely used as a "cloud classroom" amid the COVID-19 pandemic, suffered frequent VTC hijacks (also known as "Zoom-bombing"). Intruders gained access to online classrooms by stealing information from online conferences, posing a threat to the security of students' data and learning information (Setera, 2020). While the pandemic has brought opportunities for online learning, it has also brought challenges. Increasing the security requirements for online learning is necessary and should continue after the pandemic.

Online learning is defined as a learning experience through the internet in a synchronous or asynchronous environment where students engage with instructors and fellow students at a time of their convenience (Singh and Thurman, 2019). In the online learning process, data is generated through the interaction between users and tools or platforms. Data can provide insight into behavior patterns and facilitate behavioral improvement. If effectively utilized, online learning providers can tailor personalized learning services to meet student's educational needs; students, and educators can get the information they need to make decisions and create opportunities for student success. These are important reasons for students to engage in online learning. Increasingly, there is more data being collected and exchanged due to the widespread use of personal networks and devices accessing online learning. However, many educational institutions have not been adequately prepared to deal with sophisticated cybersecurity threats (Osterman, 2021). In addition to lacking sufficient human resources and financial resources to manage network security, online learning providers also lack sufficient knowledge of network security principles and defenses. Due to the COVID-19 pandemic, many institutions have accelerated the transformation of the person learning to online learning. Online learning environments are therefore subject to unprecedented security risks (EDUCAUSE, 2021).

Increasing privacy issues limit users' trust in the online learning environment and the degree of information disclosure (Anwar, 2021). Students' perception and awareness of security and how they respond to vulnerability will affect their motivation to learn, which in turn affects the effectiveness of online learning and hence their adoption behavior (Ali and Zafar, 2017). Therefore, the present study developed a conceptual model that considers how issues of data security and privacy, compared with the benefits of online learning, will affect students' willingness to use online learning.

The term privacy calculus refers to the calculus of "human behavior." Calculus refers to the cognitive trade-off among situational constraints which govern the decision-making process of individuals to decide whether to disclose personal information (Laufer and Wolfe, 1977). The principal components in privacy calculus are the perceived benefits and perceived risks. The privacy calculus theory implies that human agents act in a way to maximize benefits and minimize risks. Using the framework of privacy calculus can explain the joint influence of perceived benefits and risks on the concept of privacy and privacy protection behavior. Perceived benefits refer to the value acquisition that users perceive when information is disclosed, and perceived risks refer to potential losses that users perceive when information is disclosed. Hence the stronger the perceived benefits, the higher the possibility of information disclosure; when people worry about the potential risks, the less likely they disclose private information. Perceived benefits include social support, enjoyment, customized information, time and cost-saving, or monetary rewards. Perceived risks generally refer to the privacy and security concerns of online users, including identity theft, damaged reputation, or loss of control. Although the specific benefits and risks factors differ from study to study, overall findings supported the central point of privacy calculus theory (Smith et al., 2011). For example, in the environment of e-commerce and social networking, benefits such as personalization and money had a positive impact on information disclosure (Sun et al., 2019; Koh et al., 2020). Concerns about privacy issues have been found to have a negative relationship with users' willingness to provide information and adoption of online services (Kim et al., 2019). The users may even choose to abandon the use and conduct personal privacy protection. In addition, users who are more concerned about privacy had stricter privacy settings for their data (Jozani et al., 2020).

Based on the privacy calculus theory, this manuscript proposes that students assess the perceived benefits and perceived risks of online learning to determine their adoption. Specifically, the greater the perceived benefits in online learning are more likely to induce learners to disclose personal information and use, while greater concern to information privacy and the perceived risks of privacy breaches will negatively impact learners' willingness to use online learning. According to information system theories, money, convenience (Hann et al., 2007), efficiency (Krasnova et al., 2010), personalized functions (Zhu et al., 2016), and other factors will motivate individuals to use online services. Likewise, the benefits of online learning have been identified as a convenience, choice, of course, hedonic learning, ease of learning, customization, and personalization (Truong et al., 2017). While learners are aware of the advantages of online learning, they are equally aware of the risks of privacy that are associated with it (Schaik et al., 2017; Gogus and Saygn, 2019). Privacy protection is essential for learners because it fosters the intellectual development of society by providing an environment in which ideas can be nurtured and developed (Hughes, 2015). Online learning poses a greater privacy risk due to its ability to capture, store, and disseminate information at scale through technological means, as learners leave behind more personal details detailing their behavior and preferences during the online learning process. Consequently, online environments have become prospective targets of data breach attacks (Anwar, 2021). Studies have found that users' perceptions of privacy risks and expectations of privacy protection are directly related to the continuity of courses, learning activities, and learning performance (May and George, 2011; Jim, 2021). Besides benefits and risks, studies showed that there was a significant correlation between the trust level of online services and disclosure intentions (Metzger and Flanagin, 2013; Fletcher and Park, 2017). Users tend to share personal information for the benefit of the overall process as long as they trust the shared environment and remain in control of their data. Moreover, security breaches that compromised the credibility of

the system adversely affected students' willingness to use online learning (Nurkhin, 2020). Thus, this study utilized the Privacy Calculus framework to examine the impact of online learning from three perspectives: perceived benefits, perceived risks, and perceived trust.

Prior research has provided useful evidence in explaining the success factors that influence learners' willingness to use and adopt behavior in online learning from the benefit perspective. Extensive research has been conducted in the learning environment, social environment, learner's perception experience, and learner's characteristics (Alshurafat et al., 2021; Jiang et al., 2021; Li et al., 2021; Maheshwari, 2021; Punjani and Mahadevan, 2021).

In addition to the benefit perspective, some researchers have paid attention to the negative factors that cause learners to worry and hesitate in online learning and studying the impact assessment of online learning adoption willingness from the perspective of privacy. Through thematic analysis, Khlaif et al. (2021) revealed that infrastructure factors, cultural factors, digital inequality, and digital privacy threats influence student engagement in online learning. Zhai et al. (2020) conducted an investigation using the stimulus-organism-response (SOR) paradigm to examine how privacy concerns influence learners' perceptions of knowledge hiding, thereby affecting their online collaboration. The results showed that two types of privacy concerns (abuse and unauthorized access to private data) affected students' perceptions of knowledge hiding and negatively influenced their participation in collaborative learning online. Kim (2021) has conducted an insightful study examining the factors that motivate and hinder Reserve Officers' Training Corps (ROTC) students from participating in online courses. Their results indicated that perceived usefulness and peer behavior directly affect participation intentions. Privacy and security concerns had a negative impact on perceived ease of participation, which is mediated by perceived usefulness and peer behavior. However, empirical research focusing on both benefits and privacy perspectives is still quite limited in the online education domain.

From the trust perspective, researchers mainly focused on collaborative learning and group interaction in online learning (Nam, 2014; Du et al., 2018). Researchers also quantified the perceived experience between privacy and trust to test the effectiveness of e-learning security mechanisms (Anwar and Greer, 2012). While some researchers have constructed theoretical frameworks for online learning related to benefits, privacy, and trust, most of the studies did not combine benefits and privacy. For example, Wang (2014) focused on a social-technical framework that includes credibility, design, instructor socio-communicative style, and privacy and security for the trustworthiness of an online course without considering its benefit. Therefore, this study intends to fill the gap by studying the relationships between learning benefit, privacy, and trust in online learning based on the privacy calculus theory. This will provide evidence to assist institutional decision-making to place emphasis on the services of online learning, promote a safe and trustworthy online learning environment, and enhance learners' overall online learning experience.

Benefit Perception

Benefit perception is a subjective evaluation of potential gains or favorable outcomes. According to Chen and Dubinsky (2003), benefit perception is the net gain obtained by consumers over the perceived cost to obtain certain expected benefits. Benefit perception can also be linked to the expectancy of success and task value in the expectancy-value theory (Loh, 2019; Poort et al., 2019). The expectancy-value theory holds that people's motivation to choose a certain task is determined by their expectation of the possibility of success of the task and the value they attach to the task (Wigfield and Eccles, 2000). Eccles et al. (1983) identified the three main components associated with the theory: achievement value, intrinsic value, and utility value. Achievement value refers to the importance of doing a task well in terms of personal values, intrinsic value refers to the intrinsic enjoyment a person experiences from completing a task, and utility value refer to the usefulness of a task in helping people achieve other short-term or long-term goals. Chiu and Wang (2008) found that achievement value, utility value, and intrinsic value related to benefits are important predictors of individuals' intention to continue using online learning. In the online learning environment, benefits include the convenience of acquiring knowledge, money and time savings provided by services, as well as the satisfaction and enjoyment obtained by students through online learning and interaction, including both material benefits and well-being benefits. Therefore, this study posits that the higher the students perceive the benefits brought by online learning, the higher their intention to learn from an online learning platform. The following hypothesis is proposed:

> **H_1**: Benefit perception (BP) is positively related to students' willingness to use online learning.

Privacy Perception

Privacy is defined as "the right of an individual, group, or organization to demand that they decide when, how, and to what extent information about them is communicated to others" (Westin, 1968). Privacy perception is the degree to which an individual perceives their right to control personal information. Privacy is violated when individuals do not have adequate control over the collection, storage, use, and disclosure of their personal information (Woodman et al., 1982). Privacy concern induces fears that information disclosure may cause undesired consequences (Xu et al., 2011a). Lwin et al. (2007) found that due to concerns about online privacy, users would use tools and techniques to protect the privacy and conceal information, such as using false information to disguise their identities. The stronger the user's privacy perception, the more likely they are to realize the importance of information privacy, pay more attention to the security and protection of information privacy, and be more cautious when carrying out online activities. Therefore, the following hypothesis is proposed:

> **H_2**: Privacy perception (PP) is negatively related to students' willingness to use online learning.

Risk Perception

The concept of perceived risk was introduced by Bauer (1960) as the unexpected and uncertain outcomes that are typically unpleasant. Perceived risk has evolved from a two-dimensional construct of uncertainty and negative consequences (Brindley, 2005) to a multidimensional construct that includes financial, performance, physical, psychological, social, technological, communication, and time risks (Bertea and Bertea, 2011). In this study, risk perception is the students' expected judgment of the worst possible outcome of personal information being excessively disclosed or subjected to cyber-attacks in the online learning platform. As online learning environments are exposed to constant security threats, risks, and attacks (Chen and He, 2013), it is necessary to assess how students perceive online learning risk. Mohamed et al. (2011) developed a scale to measure students' risk perception of online education and found that performance risk, time-loss risk, psychological, and source risks were strong predictors of online learning intentions. A study by Lim and Zailani (2012) showed that perceived risks affect students' intention to enroll in the online MBA program. In mobile learning, perceived risk had a significantly negative moderating effect on the relationship between performance expectancy and behavioral intention (Chao, 2019). Hence, when the students' perceived risk exceeds its acceptable threshold, they may have concerns about continuing to use online learning. Therefore, the following hypothesis is proposed:

> **H_3**: Risk perception (RP) is negatively related to students' willingness to use online learning.

Trust Perception

Trust is defined as a mental state comprising of expectancy of a specific behavior from a trustee, belief that the expected behavior occurs, and willingness to take the risk for that belief (Anwar, 2021). Trust Perception is defined as "students' perceptions about the reliability and trustworthiness of the system" (Arpaci, 2016). When users were faced with unfamiliar information systems, trust affected their decision whether to adopt (Gefen and Straub, 2003). Trust was found to be a significant predictor of behavioral intention in online learning (Harja et al., 2019). For instance, in online learning, trust must exceed a threshold level to accept assessment and recognition practices (Tereseviciene et al., 2020). Any security risk in online learning greatly affected students' perception of the reliability and credibility of learning through the Internet. The attractiveness of online learning decreased, and the development of online learning was hindered (Adams and Blandford, 2003). Furthermore, trust was a precondition for self-disclosure that reduced the perceived risks involved in the disclosure of sensitive information (Anwar, 2021). Learners' trust perception toward online learning is affected by data policy such as how sensitive data are shared and protected. For an instant, Kayali et al. (2019) investigated the adoption of cloud-based e-learning for delivering lectures and utilizing a learning management system and office application to facilitate the daily communication between students and lecturers, finding that trust in the cloud service providers affected user intention to adopt online learning. Therefore, this study believes that the stronger the students' trust perception, the stronger their willingness to use online learning. Moreover, trust has an indirect effect on willingness to online learning through the mediating effect of risk perception. Therefore, the following hypotheses are proposed:

> **H_4:** Trust perception (TP) is positively related to students' willingness to use online learning.

> **H_5:** Trust perception (TP) is negatively related to risk perception (RP).

The research model is shown in **Figure 1**.

MATERIALS AND METHODS

Participants

To test our proposed model, having learning experiences in online learning was the main requirement of the respondent. University students already have experience in using online learning and thus are ideal participants for this study. In this study, from March 9 to 11, 2020, data on the use of online learning were collected anonymously from undergraduates in a university in Hubei Province, China. A questionnaire was used as the primary data collection instrument, and copies were distributed online through QQ, WeChat, and Weibo. In a survey, 215 questionnaires were returned, and questionnaires with incomplete responses, straightening responses, or response time less than 40 s were removed. A total of 203 valid questionnaires were obtained, with a response rate of 94.4%. The respondents' profile is presented in **Table 1**. The sample contained 45.32% males and 54.68% females.

Instruments

The questionnaire survey intends to investigate the relationship between variables and to test the proposed hypotheses. The questionnaire was divided into two parts. The first part consisted of demographic information such as gender, major, year of study, online learning experience, and perceived frequency of privacy breaches. The second part of the questionnaire consisted of five dimensions measuring benefit perception, privacy perception, risk perception, trust perception, and willingness to use online learning.

As shown in **Table 2**, benefit perception adopted the learners' perceived usefulness of the online learning platform developed by Lin and Wang (2012) and the perceived benefits of the intention to mobile applications by Wang et al. (2016). Privacy perception adopted the privacy perception security by Workman et al. (2008) and perceived ability to control information in privacy concerns with the use of the Internet by Dinev and Hart (2004). Risk perception adopted the risk perception from Pavlou (2003) consumption tendency and perceived risk of information disclosure of the location-aware marketing by Xu et al. (2011b). Trust perception adopted the consumers' trust in online platforms from Grazioli and Jarvenpaa (2000). The willingness to use online learning adopted the Continued to Use Intention by Lin and Wang (2012). Overall, the five

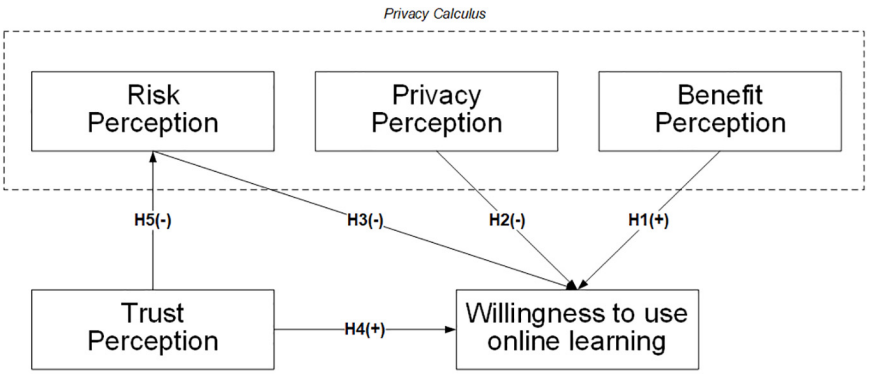

FIGURE 1 | Privacy calculus and trust research model. +: positive effect, –: negative effect.

factors in the research model were measured with 15 closed-ended questions. A five-point Likert scale was used to measure respondents' opinions, with five representing "strongly agree" and one representing "strongly disagree."

RESULTS

A structural equation model (SEM) was used to analyze the research model and the correlation between the factors. Because structural equation modeling helps reveal linear relationships between observed and latent variables (MacCallum and Austin, 2000). In this section, factor analysis, reliability, and validity analysis were conducted to test the consistency of the measurement. AMOS software was then used to test the research hypotheses.

TABLE 1 | Respondents profile (n = 203).

Profile	Frequency	Percent (%)
Gender		
Males	92	45.32%
Females	111	54.68%
Major		
Science	113	55.67%
Liberal arts	49	24.14%
Engineering	36	17.73%
Physical education	5	2.46%
Year of study		
Freshman	53	26.11%
Sophomore	41	20.20%
Junior	47	23.15%
Senior	62	30.54%
Online learning experience		
Less than 1 year	95	46.80%
1–2 years	50	24.60%
2–3 years	34	16.70%
More than 3 years	24	11.80%
Perceived frequency of privacy breaches		
Very frequently	10	4.90%
Often	28	13.80%
Generally	72	35.50%
Occasionally	66	32.50%
Never	27	13.30%

Measurement Analysis

Exploratory factor analysis is used to determine the underlying structure for each construct. Factor loadings for each item should be greater than 0.5, indicating that all constructs have been discovered (Campbell and Fiske, 1959). As shown in **Table 3**, all factor loadings were greater than 0.6 and met the conditions.

For reliability analysis, Cronbach's alpha and composite reliability were used to test the reliability of internal consistency. The measurement model is considered reliable when both Cronbach's alpha (Field, 2013) and Composite reliability (Hair et al., 1998) values are greater than 0.7. As shown in **Table 3**, both Cronbach's alpha and Composite reliability are greater than 0.7, indicating that each structure exhibits strong internal reliability.

For validity analysis, this study used convergent validity and discriminant validity for evaluation. To satisfy convergent validity, the Average Variance Extracted value should be 0.5 or higher (Hair et al., 1998). As shown in **Table 3**, the AVE values of the constructs were all greater than 0.5, meeting the condition of convergent validity. To demonstrate discriminant validity, the square root value of the AVE for each latent construct should be greater than the estimated correlation between these constructs (Fornell and Larcker, 1981). As shown in **Table 4**, the square root values of AVE for all constructs were higher than the correlation between these constructs, satisfying the discriminant validity condition.

Structural Model Analysis

This study used a goodness-of-fit analysis to assess how well the proposed model fits the collected data. Then, the hypotheses proposed in the research model were tested. As described in **Table 5**, the results showed that χ^2/df (2.592), AGFI (0.829), RMSEA (0.089), CFI (0.916), and IFI (0.917) were within the recommended range, and GFI (0.883), NFI (0.867), and TLI (0.871) were both greater than 0.85, which is acceptable. In

TABLE 2 | Measurement items.

Constructs	Items	Statements	Sources
Benefit Perception (BP)	BP1	I think the online learning platform is very convenient.	Lin and Wang, 2012; Wang et al., 2016
	BP2	I think online learning can save money.	
	BP3	I think the online learning platform can save time.	
Privacy Perception (PP)	PP1	I think of privacy as a right that I can control and use.	Dinev and Hart, 2004; Workman et al., 2008
	PP2	Controlling privacy is very important to me.	
	PP3	I think it's very important to know how my personal information is being used.	
	PP4	When an online learning platform asks me to provide personal information, I need to weigh the risk.	
Risk Perception (RP)	RP1	I think there are risks in using online learning.	Pavlou, 2003; Xu et al., 2011b
	RP2	I think the use of online learning increases the risk of personal privacy breaches.	
	RP3	I am concerned about privacy breaches due to an attack on the online learning platform.	
Trust Perception (TP)	TP1	I think the vast majority of online learning is trustworthy.	Grazioli and Jarvenpaa, 2000
	TP2	I believe that online learning will fulfill its promise to protect personal privacy.	
	TP3	I believe that the online learning platform will not arbitrarily use my personal privacy information.	
Willingness to use online learning (WTL)	WTL1	I am willing to use online learning to learn.	Lin and Wang, 2012
	WTL2	I would like to recommend the online learning platform to my relatives and friends.	

TABLE 3 | Factor analysis, construct reliability, and convergent validity.

Constructs	Items	Factor loading (>0.6)	Cronbach's alpha (>0.7)	Composite reliability (CR > 0.7)	Average variance extracted (AVE > 0.5)
Benefit Perception (BP)	BP1	0.676	0.785	0.787	0.556
	BP2	0.881			
	BP3	0.659			
Privacy Perception (PP)	PP1	0.799	0.855	0.883	0.654
	PP2	0.876			
	PP3	0.812			
	PP4	0.742			
Risk Perception (RP)	RP1	0.833	0.804	0.845	0.645
	RP2	0.784			
	RP3	0.792			
Trust Perception (TP)	TP1	0.806	0.874	0.860	0.672
	TP2	0.834			
	TP3	0.819			
Willingness to use online learning (WTL)	WTL1	0.781	0.800	0.703	0.543
	WTL2	0.690			

summary, the values of these model fit indices, as shown in **Table 6** confirm that the model has a reasonably good fit.

To test hypotheses, a path analysis was performed on the hypothetical model. **Figure 2** depicted the results of the analysis which showed that: (H1) benefit perception significantly affects willingness to use online learning ($\beta = 0.61$, $p < 0.01$); (H2) privacy perception's path to the willingness to use online learning is not significant at $p > 0.05$; (H3) risk perception significantly affects willingness to use online learning ($\beta = -0.15$, $p < 0.05$); (H4) trust perception significantly affects willingness to use online learning ($\beta = 0.34$, $p < 0.01$); and (H5) trust perception significantly affects risk perception ($\beta = -0.32$, $p < 0.01$). Overall, the structural model explained 10.4% of risk perception and 82.6% of willingness to use online learning.

To further examine the impact of risk perception in trust perception and willingness to use online learning, the meditation

TABLE 4 | Correlation matrices and discriminant validity.

Construct	BP	PP	RP	TP	WTL
Benefit Perception (BP)	**0.75**				
Privacy Perception (PP)	−0.122	**0.81**			
Risk Perception (RP)	0.062	0.461	**0.80**		
Trust Perception (TP)	0.500	−0.223	−0.267	**0.82**	
Willingness to use online learning (WTL)	0.641	−0.208	−0.222	0.636	**0.74**

Square roots of the AVE are presented as diagonal elements.

test for the indirect impact suggests that trust perception's effect on willingness to use online learning through risk perception (β = 0.05, 95% CI = 0.01–0.13) is significant. **Table 6** showed the results of the direct effects, indirect effects, and the total effects among the variables by performing bootstrapping.

DISCUSSION

Based on the privacy calculus, this study develops a research model to understand the influence that benefit perception, privacy perception, risk perception, and trust perception have on the willingness to use online learning. We conducted a structural equation analysis to validate both the research model and the hypotheses. Results indicate that the benefit perception has a direct positive influence on students' willingness to use online learning whereas the risk perception has a negative influence on students' willingness to use online learning which is consistent with that of Chiu and Wang (2008). And the perceived benefits outweigh the perceived risks (Abduljawad et al., 2020). This result is consistent with the privacy calculus theory. When the perceived benefit outweighs the perceived risk, students are more likely to engage in online learning. Online learning provides students with the convenience of time and costs savings as well as learning modules that promote knowledge acquisition over potential risks. These results suggest that students may be motivated to use online learning if the perceived benefits are heightened.

The findings show that the risk perception negatively impacts students' willingness to online learning which is consistent with the findings of Mohamed et al. (2011) where the four aspects of perceived risk were significantly and negatively correlated with intention to enroll in online learning. To provide personalization, online learning requires students to provide personal information, which students perceived to make them vulnerable to privacy risks. When students perceive the risks are high, they will tend to protect their privacy and reduce the behavior of endangering their privacy, which hinders their willingness to learn online. Therefore, to motivate students to use online learning, it is recommended that institutions should better understand students' privacy fears and concerns. For example, they can promote certain security features of online learning to alleviate this concern, and publish and promote their data protection policy statements such as the General Data Protection Regulation (GDPR) and confidentiality options to reduce students' insecurities (EDUCAUSE, 2021; Osterman, 2021).

Trust perception is found to have a positive significant effect on students' willingness to use online learning which is consistent with the recommendation of Anwar and Greer (2012) and Anwar (2021) who advocated privacy-preserving reputation management (RM) to instill trust in online e-learning environments. The findings indicate that trust perception can positively influence students' willingness to use online learning by reducing perceived risk which is consistent with the study of Hung and Wu (2012). Therefore institutions must ensure their online learning maintains good data protection reputations and trust mechanisms by adopting privacy-preserving technology (PPT) such as blockchain (Ullah et al., 2021) which will reduce the risk perception of students and motivate them to use online learning (Chang, 2021).

Interestingly, it is found that privacy perception is not affecting students' willingness to use online learning. As indicated by this study, students are very concerned with privacy (M = 2.3), yet they are still open to using online learning (M = 2.5). This inconsistent behavior is often referred to as the "privacy paradox" (Barth and de Jong, 2017). There are various plausible explanations for such inconsistency. First, their trust in online learning and their need to obtain learning resources, student services, and social connections outweigh the privacy risks. Moreover, their use is motivated by the need to acquire knowledge in a timely and cost-effective manner to begin or continue learning. Additionally, although many students and teachers have expressed their appreciation for the importance of safety, the quality, and convenience of learning remain a significant part of what students and teachers expect (EDUCAUSE, 2021). Second, students may not be aware of the risks associated with the disclosure of information. The frequency with which students feel that their privacy has been leaked in the online learning platform (M = 3.35) is between

TABLE 5 | Results of model fit indices.

Indices	Observed values	Recommended values	Sources
χ^2/df	2.592	<5.00	Kline, 2011
GFI	0.883	>0.90	Bagozzi and Yi, 1988
AGFI	0.829	>0.80	Fornell and Larcker, 1981
RMSEA	0.089	<0.10	Hair et al., 1998
NFI	0.867	>0.90	Hair et al., 1998
TLI	0.871	>0.90	Bentler and Bonett, 1980
CFI	0.916	>0.90	Fornell and Larcker, 1981
IFI	0.917	>0.90	Keith and Jane, 2003

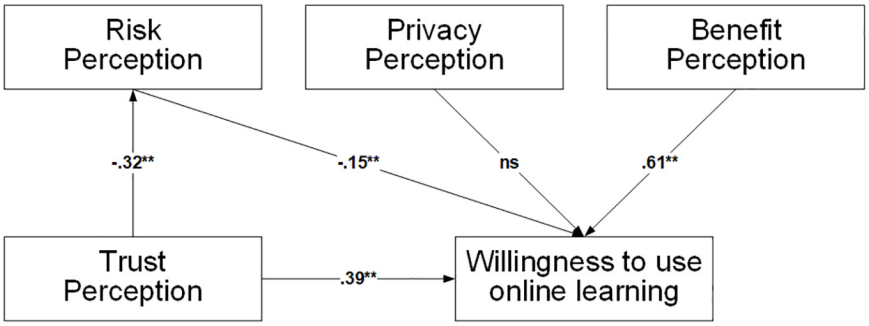

FIGURE 2 | Results of hypothesis tests (n = 203). *$p < 0.05$, **$p < 0.01$.

TABLE 6 | Results of hypothesis tests (n = 203).

		Standardized (β)			
Hypotheses		**Total effect**	**Direct effect**	**Indirect effect**	**Supported**
H1	BP→WTL	0.61**	0.61**	–	Yes
H2	PP→WTL	−0.02	−0.02	–	No
H3	RP→WTL	−0.15*	−0.15*	–	Yes
H4	TP→WTL	0.39**	0.34**	0.05**	Yes
H5	TP→RP	−0.32**	−0.32**	–	Yes

*The hypothesis was tested based on the direct effect results, *p < 0.05, **p < 0.01.*

"normal" and "occasionally." In the process of online learning, the threat of cyber-attacks is often neglected or downplayed. Although some students may express their concerns, research showed that most students have limited ability to deal with data privacy issues because they lack the necessary knowledge and skills to handle these issues (Sideri et al., 2019). Dinev et al. (2015) revealed that individuals with fewer cognitive resources or with a heavier cognitive burden tend to perform low-effort processing. Low-effort processing is characterized by spontaneous reactions that lead to irrational behaviors that contradict the beliefs of the individual. The lack of transparency in the use of data, or the fact that they cannot prevent data breaches, may lead to users abandoning the protection of their personal information, resulting in a low motivation for users to take steps to secure their data.

Research Implications

As one of the few studies to examine the impact of privacy security issues on online students, this study has a number of important implications. From a theoretical perspective, this study extends the privacy calculus theory into the area of online learning which enables us to develop a better understanding of how student perceptions of benefits, risks, and trust contribute to the willingness to use the online learning environment. The findings highlight the necessity for balancing personalization, privacy, and trust in the design of privacy and risk-aware online learning environments.

From a practical perspective, the research provides evidence and guidance to help online providers improve the safety concerns of online learning. For instance, providers can improve students' and educators' awareness of cyber security threats and promote the sound development of online learning security mechanisms. Likewise, online learning system developers should place a more significant emphasis on the security of their systems, along with the quality of control of their offerings and the technical capabilities of their systems. Online education providers have not been adequately prepared to handle network security issues. Many information technology support teams lack adequate human and financial resources to effectively manage network security (Osterman, 2021). Therefore, online learning providers should invest more in network security, solve the problem of information security worker shortages, and develop mature security measures. Online learning providers should ensure the confidentiality, integrity, and availability of data. Thus, students' concerns regarding privacy and risk perceptions in relation to online learning systems are alleviated. The lack of transparency in what online learning is collected, how they are used, and how they benefit students, undermines trust in institutions' ability to protect students' data (EDUCAUSE, 2021). It is recommended that online learning providers implement a comprehensive data governance system to protect and manage student privacy so that students can have confidence in the security of their online learning environment and achieve a positive online learning experience.

Limitations and Future Work

This study has some limitations. First, the current samples consist of only students from a single university in China. Since different provinces and universities provide different online learning environments, the samples need to be expanded to encompass

different segments of the population to generalize the results. Second, the study was conducted which involved a completely online mode of learning rather than a blended learning approach. Thus, the results are relevant to this situation. Additional studies are needed to validate the different learning modes. Last, while the variance explaining students' willingness to use an online learning platform is high, it is still possible that other variables were not considered, such as individual traits or personalities that are susceptible to risk. It may be possible to include such variables as part of an extended model in the future.

In this study, privacy perception did not seem to affect students' willingness to engage in online learning, which may be explained by the privacy paradox. Additional research could clarify the extent to which privacy influences students' willingness to use online learning by taking into account all moderators and individual factors, such as gender, age, education, personality, and learning level to arrive at a comprehensive privacy calculus model operate in the online learning context.

CONCLUSION

Even though the use of online students' data offers several benefits to students, including improved functionality and enhanced services, privacy and data security remain concerns for students. A privacy calculus theory is presented in this study to examine the factors that will assist online learning providers in addressing privacy protection concerns. The model was empirically tested using 203 data samples from a university in Wuhan, Hubei, China. Benefit perception and trust perception are the two factors that have the greatest effect on students' willingness to learn online. It can be stated that the proposed model is useful for explaining students' willingness to use online learning. These findings allow us to better understand what factors contribute to increased willingness to participate in online learning. Additionally, the findings can assist online learning providers and educational institutions in developing guidelines and policies designed to enhance online learning capabilities and quality of service.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

ETHICS STATEMENT

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. The patients/participants provided their written informed consent to participate in this study.

AUTHOR CONTRIBUTIONS

XJ contributed to the study design, theoretical basis, data analysis, and discussion of the manuscript. T-TG contributed to the discussion and conclusions of the manuscript and critically revised the manuscript. ML was responsible for the conception, data collection, and analysis of the manuscript. All authors contributed to the article and approved the submitted version.

FUNDING

This study was supported by Open Fund of Hubei Research Center for Quality Education in Primary and Secondary Schools "Research on Emotional Development of Primary School Students in Hubei Based on Free Writing Big Data" (2020HBSZA08).

REFERENCES

Abduljawad, M., Ahmad, A., Jaber, K. M., Thunaibat, A. A., Maria, E. A., Khasawneh, A., et al. (2020). Evaluating and adopting E-learning systems in Al-Zaytoonah university of Jordan. *Int. J. Adv. Soft Comput. Appl.* 12, 82–100.

Adams, A., and Blandford, A. (2003). "Security and Online learning: to protect or prohibit," in *Usability Evaluation of Online Learning Programs*, ed. C. Ghaoui (London: IDEA Publishing), 331–359.

Ali, R., and Zafar, H. (2017). A security and privacy framework for e-learning. *Int. J. e-Learning Secur. (IJeLS)* 7, 556–566.

Alshurafat, H., Al Shbail, M. O., Masadeh, W. M., Dahmash, F., and Al-Msiedeen, J. M. (2021). Factors affecting online accounting education during the COVID-19 pandemic: an integrated perspective of social capital theory, the theory of reasoned action and the technology acceptance model. *Educ. Inf. Technol.* 26, 6995–7013. doi: 10.1007/s10639-021-10550-y

Anwar, M. (2021). Supporting privacy, trust, and personalization in online learning. *Int. J. Artif. Intell. Educ.* 31, 769–783. doi: 10.1007/s40593-020-00216-0

Anwar, M., and Greer, J. (2012). Facilitating trust in privacy-preserving E-learning environments. *IEEE Trans. Learn. Technol.* 5, 62–73. doi: 10.1109/TLT.2011.23

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Comput. Hum. Behav.* 58, 150–157. doi: 10.1016/j.chb.2015.12.067

Bagozzi, R. P., and Yi, Y. (1988). On the evaluation of structural equation models. *J. Acad. Mark. Sci.* 16, 74–94. doi: 10.1007/BF02723327

Barth, S., and de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telemat. Inform.* 34, 1038–1058. doi: 10.1016/j.tele.2017.04.013

Bauer, R. A. (1960). "Consumer behavior as risk taking," in *Proceedings of the 43rd National Conference of the American Marketing Assocation, June 15, 16, 17, 1960*, ed. R. S. Hancock (Chicago, IL: American Marketing Association).

Bentler, P. M., and Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychol. Bull.* 88, 588–606. doi: 10.1037/0033-2909.88.3.588

Bertea, A. F., and Bertea, P. E. (2011). "A scale to measure perceived risk in E-learning adoption," in *The Proceedings of the 2011 eLearning and Software for Education* (Bucharest: Editura Universitara), 223–228.

Bongiovanni, I. (2019). The least secure places in the universe? A Systematic Literature Review on Information Security Management in Higher Education. *Comput. Secur.* 86, 350–357. doi: 10.1016/j.cose.2019.07.003

Brindley, C. (2005). Barriers to women achieving their entrepreneurial potential: women and risk. *Int. J. Entrep. Behav. Res.* 11, 144–161. doi: 10.1108/13552550510590554

Campbell, D. T., and Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychol. Bull.* 56, 81–105. doi: 10.1037/h0046016

Chang, B. (2021). Student privacy issues in online learning environments. *Distance Educ.* 42, 55–69. doi: 10.1080/01587919.2020.1869527

Chao, C.-M. (2019). Factors determining the behavioral intention to use mobile learning: an application and extension of the UTAUT model. *Front. Psychol.* 10:1652. doi: 10.3389/fpsyg.2019.01652

Chapman, J. (2019). How safe is your data? Cyber-security in higher education. *HEPI Policy Note* 12, 1–6.

Chen, Y., and He, W. (2013). Security risks and protection in online learning: a survey. *Int. Rev. Res. Open Distrib. Learn.* 14, 108–127. doi: 10.19173/irrodl.v14i5.1632

Chen, Z., and Dubinsky, A. J. (2003). A conceptual model of perceived customer value in e-commerce: a preliminary investigation. *Psychol. Mark.* 20, 323–347. doi: 10.1002/mar.10076

Chiu, C. M., and Wang, E. (2008). Understanding Web-based learning continuance intention: the role of subjective task value. *Inf. Manag.* 45, 194–201. doi: 10.1016/j.im.2008.02.003

DataBreach (2020). *150,000s of e-Learning Students Exposed in 8Belts Data Breach. Security Magazine* [Online]. Available online at: https://www.vpnmentor.com/blog/report-8belts-leak/ (accessed August 28, 2020).

Dinev, T., and Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behav. Inf. Technol.* 23, 413–422. doi: 10.1080/01449290410001715723

Dinev, T., McConnell, A. R., and Smith, H. J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Inf. Syst. Res.* 26, 639–655. doi: 10.1287/isre.2015.0600

Du, J., Wang, C., Zhou, M., Xu, J., Fan, X., and Lei, S. (2018). Group trust, communication media, and interactivity: toward an integrated model of online collaborative learning. *Interact. Learn. Environ.* 26, 273–286. doi: 10.1080/10494820.2017.1320565

Eccles, J. S., Adler, T. F., Futterman, R., Goff, S. B., and Midgley, C. (1983). "Expectations, values, and academic behaviors," in *Achievement and Achievement Motives: Psychological and Sociological Approaches*, ed. J. T. Spence (New York: Freeman), 75–146.

EDUCAUSE (2021). *2021 EDUCAUSE Horizon Report® | Information Security Edition*. Boulder, CO: EDUCAUSE Publications.

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics*. London: SAGE.

Fletcher, R., and Park, S. (2017). The impact of trust in the news media on online news consumption and participation. *Digit. Journal.* 5, 1281–1299.

Fornell, C., and Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: algebra and statistics. *J. Mark. Res.* 18, 382–388. doi: 10.2307/3150980

Gefen, D., and Straub, K. D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Q.* 27, 51–90. doi: 10.2307/30036519

Gogus, A., and Saygn, Y. (2019). Privacy perception and information technology utilization of high school students. *Heliyon* 5:e01614. doi: 10.1016/j.heliyon.2019.e01614

Grazioli, S., and Jarvenpaa, S. L. (2000). Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *IEEE Trans. Syst. Man Cybernet. Part A* 30, 395–410. doi: 10.1109/3468.852434

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. (1998). *Multivariate Data Analysis*, Vol. 5. Upper Saddle River, NJ: Prentice hall, 207–219.

Hann, I., Hui, K. L., Lee, S., and Png, I. P. L. (2007). Overcoming online information privacy concerns: an information-processing theory approach. *J. Manag. Inf. Syst.* 24, 13–42. doi: 10.2753/MIS0742-1222240202

Harja, Y. D., Irawan, M. I., and Ambarwati, R. (2019). Measure the significance of learning value and trust factors for online learning technology acceptance in Indonesia. *IPTEK J. Technol. Sci.* 31, 188–200.

Hughes, K. (2015). "The social value of privacy, the value of privacy to society and human rights discourse," in *Social Dimensions of Privacy: Interdisciplinary Perspectives*, eds B. Roessler and D. M. Mokrosinska (Cambridge: Cambridge University Press), 225–243.

Hung, S.-Y., and Wu, H.-L. (2012). Factors influencing user acceptance of web-based decision support systems. *J. Comput. Inf. Syst.* 52, 70–77. doi: 10.1080/08874417.2012.11645578

Jiang, H., Islam, A. Y. M. A., Gu, X., and Spector, J. M. (2021). Online learning satisfaction in higher education during the COVID-19 pandemic: a regional comparison between Eastern and Western Chinese universities. *Educ. Inf. Technol. (Dordr.)* 26, 6747–6769. doi: 10.1007/s10639-021-10519-x

Jim, R. (2021). L2 student engagement with automated feedback on writing: potential for learning and issues of trust. *J. Second Lang. Writ.* 52:100816. doi: 10.1016/j.jslw.2021.100816

Jozani, M. M., Ayaburi, E., Ko, M., and Choo, K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective. *Comput. Hum. Behav.* 107:106260. doi: 10.1016/j.chb.2020.106260

Kayali, M., Safie, N., and Mukhtar, M. (2019). The effect of individual factors mediated by trust and moderated by IT knowledge on students' adoption of cloud based E-learning. *Int. J. Innov. Technol. Explor. Eng* 9, 987–993.

Keith, F. W., and Jane, S. T. (2003). On specifying the null model for incremental fit indices in structural equation modeling. *Psychol. Methods* 1, 16–37. doi: 10.1037/1082-989X.8.1.16

Khlaif, Z. N., Salha, S., and Kouraichi, B. (2021). Emergency remote learning during COVID-19 crisis: students' engagement. *Educ. Inf. Technol.* 26, 7033–7055. doi: 10.1007/s10639-021-10566-4

Kim, D., Park, K., Park, Y., and Ahn, J.-H. (2019). Willingness to provide personal information: perspective of privacy calculus in IoT services. *Comput. Hum. Behav.* 92, 273–281. doi: 10.1016/j.chb.2018.11.022

Kim, S. S. (2021). Motivators and concerns for real-time online classes: focused on the security and privacy issues. *Interact. Learn. Environ.* 1–14. doi: 10.1080/10494820.2020.1863232

Kline, R. B. (2011). "Principles and practice of structural equation modeling," *Journal of the American Statistical Association* (New York, NY: Guilford Press) 101.

Koh, B., Raghunathan, S., and Nault, B. R. (2020). An empirical examination of voluntary profiling: privacy and quid pro quo. *Decis. Support Syst.* 132:113285. doi: 10.1016/j.dss.2020.113285

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: why we disclose. *J. Inf. Technol.* 25, 109–125. doi: 10.1057/jit.2010.6

Laufer, R. S., and Wolfe, M. (1977). Privacy as a concept and a social issue: a multidimensional developmental theory. *J. Soc. Issues* 33, 22–42. doi: 10.1111/J.1540-4560.1977.TB01880.X

Li, Y., Nishimura, N., Yagami, H., and Park, H.-S. (2021). An empirical study on online learners' continuance intentions in China. *Sustainability* 13:889. doi: 10.3390/su13020889

Lim, L. L., and Zailani, S. H. M. (2012). Determinants influencing intention to enrol on an online MBA programme. *Int. J. Bus. Inf. Syst.* 9:51.

Lin, W.-S., and Wang, C.-H. (2012). Antecedences to continued intentions of adopting e-learning system in blended learning instruction: a contingency framework based on models of information system success and task-technology fit. *Comput. Educ.* 58, 88–99. doi: 10.1016/j.compedu.2011.07.008

Loh, E. K. Y. (2019). What we know about expectancy-value theory, and how it helps to design a sustained motivating learning environment. *System* 86:102119. doi: 10.1016/j.system.2019.102119

Lwin, M., Wirtz, J., and Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *J. Acad. Mark. Sci.* 35, 572–585.

MacCallum, R. C., and Austin, J. T. (2000). Applications of structural equation modeling in psychological research. *Annu. Rev. Psychol.* 51, 201–226. doi: 10.1146/annurev.psych.51.1.201

Maheshwari, G. (2021). Factors affecting students' intentions to undertake online learning: an empirical study in Vietnam. *Educ. Inf. Technol.* 26, 6629–6649. doi: 10.1007/s10639-021-10465-8

May, M., and George, S. (2011). Privacy concerns in E-learning: is using tracking system a threat? *Int. J. Inf. Educ. Technol.* 1, 1–8. doi: 10.7763/IJIET.2011.V1.1

Metzger, M. J., and Flanagin, A. J. (2013). Credibility and trust of information in online environments: the use of cognitive heuristics. *J. Pragmat.* 59, 210–220. doi: 10.1016/j.pragma.2013.07.012

Mohamed, F., Hassan, A., and Spencer, B. (2011). Conceptualization and measurement of perceived risk of online education. *Acad. Educ. Leadersh. J.* 15, 1–16.

Nam, C. W. (2014). The effects of trust and constructive controversy on student achievement and attitude in online cooperative learning environments. *Comput. Hum. Behav.* 37, 237–248. doi: 10.1016/j.chb.2014.05.007

Nurkhin, R. A. (2020). Analysis of factors affecting behavioral intention to use E-learning uses the unified theory of acceptance and use of technology approach. *KnE Soc. Sci.* 4, 1005–1025. doi: 10.18502/kss.v4i6.6658

Osterman (2021). *Cybersecurity in Education – White Paper*. Osterman Research.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *Int. J. Electron. Commer.* 7, 101–134. doi: 10.1080/10864415.2003.11044275

Poort, I., Jansen, E., and Hofman, A. (2019). Intercultural group work in higher education: costs and benefits from an expectancy-value theory perspective. *Int. J. Educ. Res.* 93, 218–231. doi: 10.1016/j.ijer.2018.11.010

Punjani, K. K., and Mahadevan, K. (2021). Transitioning to online learning in higher education: influence of awareness of COVID-19 and self-efficacy on perceived net benefits and intention. *Educ. Inf. Technol.* 27, 1–30. doi: 10.1007/s10639-021-10665-2

Schaik, P.v., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Comput. Hum. Behav.* 75, 547–559. doi: 10.1016/j.chb.2017.05.038

Setera, K. (2020). *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*. Chelsea, MA: FBI Boston.

Sideri, M., Kitsiou, A., Tzortzaki, E., Kalloniatis, C., and Gritzalis, S. (2019). Enhancing University students privacy literacy through an educational intervention. A Greek case-study. *Int. J. Electron. Gov.* 11, 333–360. doi: 10.1504/IJEG.2019.10018628

Singh, V., and Thurman, A. (2019). How many ways can we define online learning? A systematic literature review of definitions of online learning (1988-2018). *Am. J. Distance Educ.* 33, 289–306. doi: 10.1080/08923647.2019.1663082

Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: an interdisciplinary review. *Soc. Electron. Publ.* 35, 989–1015. doi: 10.2307/41409970

Sun, Y., Fang, S. Y., and Hwang, Y. J. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability* 11:3311. doi: 10.3390/su11123311

Tereseviciene, M., Trepule, E., Dauksiene, E., Tamoliune, G., and Costa, N. (2020). Are universities ready to recognize open online learning? *Int. Educ. Stud.* 13, 21–32. doi: 10.3389/fpsyg.2020.02189

Truong, N. N., Hieu, V. M., and Quoc, T. H. A. (2017). An analysis of perceived student benefits in e-learning service case study on FPT University. *J. Educ. Soc. Sci.* 8, 71–82.

Ullah, N., Mugahed Al-Rahmi, W., Alzahrani, A. I., Alfarraj, O., and Alblehai, F. M. (2021). Blockchain technology adoption in smart learning environments. *Sustainability* 13:1801. doi: 10.3390/su13041801

Wang, T., Duonga, T. D., and Chen, C. C. (2016). Intention to disclose personal information via mobile applications: a privacy calculus perspective. *Int. J. Inf. Manag.* 36, 531–542. doi: 10.1016/j.ijinfomgt.2016.03.003

Wang, Y. D. (2014). Building student trust in online learning environments. *Distance Educ.* 35, 345–359. doi: 10.1080/01587919.2015.955267

Westin, A. F. (1968). Privacy and freedom. *Washington Lee Law Rev.* 25, 166–170.

Wigfield, A., and Eccles, J. S. (2000). Expectancy-value theory of achievement motivation. *Contemp. Educ. Psychol.* 25, 68–81. doi: 10.1006/ceps.1999.1015

Woodman, R. W., Ganster, D. C., Adams, J., McCuddy, M. K., Tolchinsky, P. D., and Fromkin, H. (1982). A survey of employee perceptions of information privacy in organizations. *Acad. Manag. J.* 25, 647–663.

Workman, M., Bommer, W. H., and Straub, D. W. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Comput. Hum. Behav.* 24, 2799–2816. doi: 10.1016/j.chb.2008.04.005

Xu, H., Dinev, T., Smith, H. J., and Hart, P. (2011a). Information privacy concerns: linking individual perceptions with institutional privacy assurances. *J. Assoc. Inf. Syst.* 12, 798–824. doi: 10.17705/1JAIS.00281

Xu, H., Luo, X., Carrolla, J. M., and Rossona, M. B. (2011b). The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decis. Support Syst.* 51, 42–52. doi: 10.1016/j.dss.2010.11.017

Zhai, X., Wang, M., and Ghani, U. (2020). The SOR (stimulus-organism-response) paradigm in online learning: an empirical study of students' knowledge hiding perceptions. *Interact. Learn. Environ.* 28, 586–601. doi: 10.1080/10494820.2019.1696841

Zhu, H., Ou, C. X. J., van den Heuvel, W. J. A. M., and Liu, H. (2016). Privacy calculus and its utility for personalization services in e-commerce: an analysis of consumer decision-making. *Inf. Manag.* 54, 427–437. doi: 10.1016/j.im.2016.10.001

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.