Soft Computing
https://doi.org/10.1007/s00500-022-07369-1

The online website privacy disclosure behavior of users based on concerns-outcomes model

X. I. E. Weihong[1,2] · Zhang Qian[1]

Accepted: 29 June 2022

Abstract
Reducing users' online privacy concerns and encouraging users' privacy disclosure behaviors are the important prerequisite for online websites to use data to obtain economic value. Based on the theory of clue utilization and privacy calculation theory, this paper uses the APCO model to intermediate online privacy concerns and adjust privacy calculations to explore the influence mechanism of online website users' privacy disclosure behaviors in China. Using the questionnaire survey method, SPSS 20.0 and AMOS 23.0 were used to conduct structural equation path analysis on the collected 966 valid data to verify the proposed research hypothesis. Research results show that website reputation and website trust have a significant positive impact on privacy disclosure; users' online privacy concerns will play a mediating role in website reputation, website trust, and privacy disclosure; when users with online privacy concerns are doing privacy calculations of perceived risks and perceived benefits are carried out during privacy disclosure. However, privacy calculations are contextual. On the premise of website trust, the benefits of information disclosure can reduce users' online privacy concerns and increase users' privacy disclosure behaviors. This article exposes that users will adopt privacy disclosure decisions with different levels of cognitive effort based on the degree of online privacy concerns, enriches research on privacy disclosure behavior, and exposes the contextual nature of privacy calculus, which further enriches and expands the theory of privacy calculus. Promote online websites to obtain user data and provide relevant countermeasures and suggestions.

Keywords Online websites · Online privacy concerns · Privacy disclosure behaviors · Privacy calculations · APCO model

1 Introduction

In the era of big data, users' data information has become an important strategic resource for enterprises and the key to improve their competitive advantages (Johnson et al. 2020). As the main medium of personal data circulation, online websites can effectively identify users' behaviors and preferences by correctly collecting, storing and processing user data and information, so as to provide personalized services and products to meet their demands (Erevelles et al. 2016). Users' information disclosure is of great significance to the survival and development of online websites. However, since relevant policies and regulations are still imperfect in China, information leakage often occurs, which aggravates users' privacy concerns. As a result, they begin to reduce or refuse information disclosure, such as closing or canceling accounts, reducing online shopping times (Hong et al. 2021) and share false information online to uphold their privacy needs (Thompson and Brindley 2021). The development of online network platforms is seriously hindered. Therefore, reducing users' privacy concerns and encouraging privacy disclosure have become important prerequisites for online websites to realize economic values through data.

✉ Zhang Qian
zhangqian198317@163.com

X. I. E. Weihong
xwh@gdut.edu.cn

[1] School of Management, Guangdong University of Technology, Guangzhou 510520, China

[2] School of Economics and Trade, Guangdong University of Technology, Guangzhou 510520, China

Published online: 28 July 2022

According to the clue utilization theory, users judge the value of using a product, and then make decisions based on some clues. In view of the importance of clues, a company will provide users with a series of clues to its quality. For example, many websites show their popularity and reputation to users to gain their trust, and enhance users' positive perception through internal and external clues, expecting users to make quick disclosure decisions. However, privacy is a multi-dimensional, flexible and dynamic concept which changes with different contexts. Also, it is influenced by various factors such as personal thinking, perception and cognition (Smith et al. 2011). Internet privacy concern is personal subjective feeling for the corresponding privacy context (Xie et al. 2019), while privacy disclosure behavior is users' subjective reaction of active disclosure according to specific privacy context. Users make privacy decisions with different cognitive efforts according to internal and external stimuli such as websites, individuals and environment. This study aims to investigate whether websites can reduce users' privacy concerns and promote their disclosure behavior by showing reputation and trust, and explore the corresponding influencing mechanism.

From the perspective of antecedents-privacy concerns-outcomes (hereinafter referred to as APCO) of information privacy, this study analyzes the influencing mechanism of privacy concerns and privacy disclosure behavior. First, APCO model reveals that privacy disclosure behavior is a decision-making process influenced by different cognitive efforts. For example, Dinev et al. (2015) pointed out that users' privacy cognition and decision-making were processed by high-effort and low-effort cognition. High-effort cognition involves thoughtful cognitive efforts and rational thinking and analysis. However, low-effort cognition involves relatively little cognitive effort or consciousness, and does not need laborious analysis of complex logic and detailed reasoning. Second, APCO model deeply analyzes the influence of privacy concerns on the decision-making process of privacy disclosure, and can be appropriately modified according to different study backgrounds and purposes. Therefore, APCO model can provide a suitable theoretical framework for this study.

According to the clue utilization theory and the privacy calculus theory, this study constructs a study framework of website reputation, website trust, network privacy concerns and privacy disclosure behavior based on APCO model, and explores the influencing mechanism of Chinese users' privacy disclosure behavior through empirical analysis. The contributions of this study are as follows: First, the existing studies generally believe that privacy disclosure behavior is a risk benefit trade-off (for instance, in exchange for items, services, discounts, or personalization) (Kolotylo-Kulkarni et al. 2021). This is because users do not understand the purpose of data collection or the sharing target, which induces users' privacy concerns and attention to personal information data. Therefore, privacy disclosure behavior is a process that needs careful consideration. It is affected by many factors, and involves the analysis and processing process of rational thinking. However, under the influence of information overload, time constraints and cognitive bias, privacy disclosure behavior may also be a simple, heuristic or spontaneous response, may not be totally determined by a rational calculus (Fernandes and Pereira 2021). This study deeply analyzes the relationship among clues provided by websites, privacy concerns and privacy disclosure behaviors, expecting to understand the influencing factors of users' privacy disclosure behaviors with different cognitive efforts, which is conductive to expanding the study of privacy disclosure behaviors. In addition, a model of "antecedents of information privacy-privacy concerns-results" of online websites with mediating and moderating effects is established, which can help online websites to understand the driving factors and hindering factors of users' privacy disclosure behavior, so as to provide relevant countermeasures and suggestions for online websites to obtain user data, realize economic value and enhance competitive advantages. Thirdly, the existing empirical research on privacy is mainly based on western samples, but due to the national conditions and cultural differences between Western countries and China, there are many differences between them (Hong et al. 2021). The study of Chinese context is conducive to expanding the research on users' privacy attitudes and behaviors.

The structure of this study is as follows: Sect. 2 reviews previous studies of Internet privacy concerns, privacy disclosure behavior and APCO model; Sect. 3 proposes six study hypotheses; Sect. 4 introduces the sample selection, data collection, and variable measurement. In Sect. 5, the empirical results are analyzed. Finally, Sect. 6 draws the conclusion, and discusses the theoretical significance, practical enlightenment, deficiencies and prospects of this study.

2 Literature review

2.1 Internet privacy concerns

Internet privacy concerns refer to the degree of Internet users' concern about the collection and use of their personal information on websites, which reflects individuals' willingness to expect websites to provide adequate protection for their personal information and the difference perception with the actual behavior of websites (Hong and Thong 2013). As a multidimensional, dynamic and contextualized concept, it is individuals' subjective feeling for

the corresponding privacy context. The studies of privacy concerns in China and foreign countries involve the measurement and influencing factors of users' privacy concerns.

The measurement of privacy concerns has always been concerned with by scholars, and it constantly changes with context development. Based on the differences of study contexts, the studies of privacy concern measurement can be divided into different stages: privacy concern measurement in general context, represented by CFIP (Concerns for Information Privacy) scale established by Smith et al. (1996), includes four dimensions: collection, secondary use, improper access and errors; privacy concern measurement in the traditional Internet context represented by the IUIPC (Internet Users' Information Privacy Concerns) scale proposed by Malhotra et al. (2004), includes three dimensions: collection, control and awareness; privacy concern measurement in Web2.0 context, represented by an integrated measurement model from the perspective of interpersonal interaction in multidimensional development theory proposed by Hong et al. (2013), considers that internet privacy concerns include six dimensions: collection, secondary use, improper access, errors, control and awareness. Xie et al. (2019) summarized the representative privacy concern measurement scale, and verified the composition dimensions of internet privacy concerns in China, including five key dimensions: control, collection, secondary use, errors, improper access and remedy, as shown in Table 1.

Some scholars have discussed the influencing factors of internet privacy concerns from different perspectives. Smith et al. (2011) summarized interdisciplinary studies of privacy, and studied the influencing factors of internet privacy concerns, including individual factors that influence privacy concerns, such as users' privacy experience, privacy awareness, personality tendency and cultural differences, as well as some external factors, like privacy statement, government, industry privacy norm, etc. The model shows that users' actual behaviors depend on the comprehensive influence of all factors, which is of great importance to identify the factors leading to privacy concerns in further study (Ioannou et al. 2020). Hong et al. (2021) investigated the driving factors and restraining factors of internet privacy concerns, finding that familiarity with government legislation, internet knowledge, benefits of information disclosure, privacy protection and social existence can reduce users' internet privacy concerns. Personal privacy invasion experience, risk aversion personality and sensitivity of information required by websites can increase their internet privacy concerns.

However, compared to Western countries, Chinese Internet users have cultural differences in their attitudes and behaviors towards privacy. On the one hand, based on the study results in western countries, it is necessary to expand the studies of privacy concerns in China; on the other hand, because of the differences between Western culture and Asian culture, Asian users have a lower level of perception of privacy concerns (Westin 2010). Therefore, it is not enough to study only the privacy concerns of Chinese users, and the behavior results of privacy concerns should be thoroughly analyzed.

2.2 Privacy disclosure behavior

Users' privacy disclosure behavior refers to that an individual voluntarily and actively displays and shares information to others, which is a construct and phenomenon is highly complex, with multiple factors coming into play (Kolotylo-Kulkarni et al. 2021). Scholars usually interpret privacy disclosure behavior based on the privacy calculus theory, and believe that users use a risk–benefit trade-off or privacy calculus when they decide for or against self-disclosure (Choi et al. 2018). Privacy disclosure is determined by the comparison between benefits and risks, even when both return and risk are high, high disclosure results when expected return is greater than expected risk; and low

Table 1 Privacy concerns measure dimensions

The general context		The traditional Internet context	Web 2.0 context	The Chinese context
Author	Smith et al. (1996)	Malhotra et al. (2004)	Hong et al. (2013)	Xie et al. (2019)
Measurement dimension	Collection	Collection	Collection	Control
	Secondary use	Control	Secondary use	Collection
	Improper access	Awareness	Errors	Secondary use
	Errors		Improper access Control	Errors
			Awareness	Improper access
				Remedy

disclosure occurs when expected return is less than expected risk (Sun et al. 2022). However, some scholars explain that users' privacy behavior is affected by incomplete information, limited rationality and psychological deviation from the perspective of privacy paradox (Acquisti and Grossklags 2005). From the perspective of behavioral economics and psychological theory, users' privacy decision is a heuristic low-effort cognitive response (Dinev et al. 2015).

Disclosure behavior is users' subjective reaction, which is malleable and influenced by the context (Bansal et al. 2016). Some scholars have studied the influencing factors of privacy disclosure behavior from different theoretical perspectives. For example, Hallam and Zanella (2017) analyzed the influence of privacy concerns and social benefits on users' psychological intentions and self-disclosure behaviors based on the interpretation theory. Urbonavicius et al. (2021) explores the willingness of users to disclose personal data when shopping online through social exchange theory. Some scholars have studied the influencing factors of privacy disclosure behavior in different contexts. For example, Melumad and Meyer (2020) compared smart phones with personal computers and found that users were more willing to disclose information on smart phones. Combined with the framework of communication privacy management and social penetration theory, Osatuyi et al. (2018) studied the determinants of personal information disclosure in social networks. Some scholars also studied privacy disclosure behaviors of different groups of people. For example, Desimpelaere et al. (2020) studied children's online privacy disclosure behavior, and pointed out the importance of strengthening privacy literacy training for children's privacy protection. Disclosure is a complex and subjective decision-making behavior, which is influenced by personal factors (Kai et al. 2015; Benamati et al. 2017), external factors (Shane-Simpson et al. 2018), and environmental factors (Ilhan and Fietkiewicz 2020).

To sum up, privacy disclosure behavior is a subjective response made by users in different contexts. Influenced by many factors, users make disclosure decisions with different cognitive efforts. Sometimes, users will make thoughtful analysis because of the responses to external stimuli, which leads to attitudes and behaviors with high cognitive level (Dinev et al. 2015). However, sometimes users have limited rationality, and generated relatively automatic cognitive heuristics and thought shortcuts based on simple clues such as past experience, habits and conventions to evaluate behavior results (Fernandes and Pereira 2021). Therefore, it is particularly important to determine the factors leading to users' privacy disclosure with different cognitive efforts and the mechanism of privacy decision-making behavior.

2.3 APCO model

Internet privacy concerns and privacy disclosure behaviors have always been the focus of attention of digital enterprises and academic circles. Smith et al. (2011) put forward the antecedents-privacy concerns-outcomes model of information privacy (hereinafter referred to as APCO model), which studies not only individual factors that affect privacy concerns, such as users' privacy experience, privacy awareness, personality tendency and cultural differences, but also external factors such as corporate privacy statements, government or industry privacy norms. It is shown in Fig. 1. Dinev et al. (2015) added several factors to the original model, such as individuals' cognitive effort level, prejudice and wrong attribution, and established an enhanced APCO model, which considered both high-effort cognitive response of careful and rational thinking (the original APCO model), and the low-effort cognitive response influenced by the framework and theory of behavioral economics and psychology.

In recent years, scholars have used APCO model to study privacy according to different contexts. Some scholars studied the privacy of mobile commerce. For example, Benamati et al. (2017) based on social networking platforms, applied the enhanced APCO model to examine the influences of privacy awareness (PA) and demographic variables (age, gender) on concern for information privacy (CFIP). Shen et al. (2019) have used APCO model to study patients' privacy, such as patients' privacy concerns, antecedents and results from the perspective of health information exchange. Menard and Bott (2020) applied the enhanced APCO model to explore users' actual disclosure behavior when using Internet of Things applications by carrying out experiments. APCO model is widely used to study privacy issues, and it can be modified appropriately according to different study backgrounds and purposes. Based on the clue utilization theory, in order to examine whether the clues provided by online websites to users are effective, that is, whether website reputation and website trust have significant influence on privacy disclosure behavior, this study applies the macro APCO model to the specific context of users' cognition of websites. First, the influence of website reputation and website trust, as antecedents, on the result variable-privacy behavior is analyzed. Second, the internet privacy concern, as a mediating variable, is introduced to discuss its influence on privacy disclosure behavior. Third, by introducing privacy calculus as a moderating variable to internet privacy concerns and privacy disclosure behavior, the influence mechanism of users' privacy disclosure behavior is analyzed.

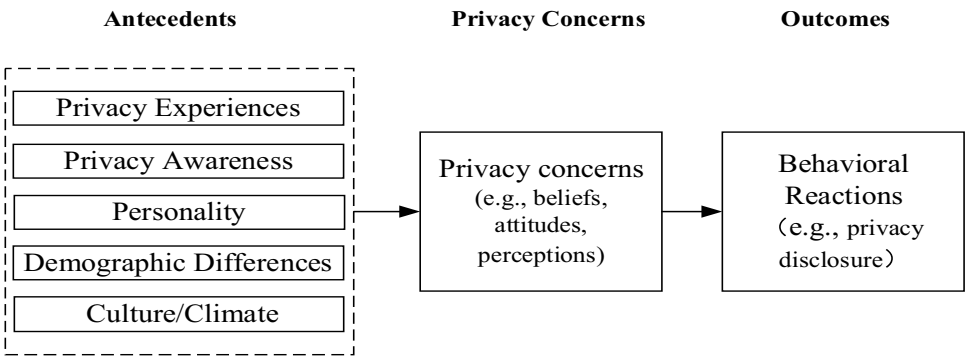

Fig. 1 APCO model

3 Study hypothesis

3.1 Direct effects of website reputation and website trust on privacy disclosure behavior

With different website perceptions, users have different degrees of privacy concerns and different purposes of privacy disclosure, which will lead to different self-disclosure results. Due to information asymmetry, it is difficult for users to objectively evaluate websites, and they can only measure the quality of companies or products according to heuristic clues (Dawar and Parker 1994). Previous study results demonstrate that websites can achieve the potential influence on users' information disclosure by enhancing social image (enhancing website reputation) (Aljukhadar et al. 2010) or establishing a good social response (building website trust) (Proudfoot et al. 2018).

As the "business card" of a network enterprise, website reputation refers to the public's general evaluation of product quality or service quality and reflection of use experience. Website reputation is regarded as an external clue to users' evaluation under asymmetric information (Jin and Kato 2006). The higher the website reputation, the lower the privacy concerns of users (Wirtz and Lwin 2009). Because users think that platforms with good reputation have higher moral and commercial standards and media pressure, and they are more willing to believe that these websites will care about the vital interests and have stronger ability and binding force to protect privacy, thus reducing the privacy concerns (Milne and Boza 1999). In addition, users predict that websites may continue the previous privacy protection behavior in future transactions according to the website reputation. In this case, the higher the website reputation, the more users will believe that they will not take actions that harm users' interests. As a result, users will reduce their concerns about disclosing information on the websites and increase their disclosure behaviors. In this basis, Hypothesis 1 is put forward:

H_1 Website reputation has positive influence on users' privacy disclosure behavior.

Trust refers to the degree to which one party is willing to rely on the other party with a relative sense of security in specific context, even if negative consequences may occur (Mcknight and Chervany 2001). This definition emphasizes the relationship between risk and trust. Only when there is risk, uncertainty or interdependence will trust become crucial (Roghanizad and Neufeld 2015). Online activities can lead to users' uncertainty and sense of risk (Gefen et al. 2003). Therefore, website trust indicates the degree of trust perceived by network users, and it is a standard for evaluating the ability of websites to protect users' personal information (Williams 2003). It is generally believed that website trust can affect users' selection and use of websites and the generation of digital footprints (Muhammad 2018). The previous studies of website trust and privacy issues demonstrate that website trust will affect users' privacy concerns and disclosure decisions through positive psychological expectations and reducing perceived risks. As argued by Martin and Murphy (2017), when there are obvious privacy issues, trust will promote users' disclosure willingness, purchase behavior, advertising acceptance and other positive marketing results. Urbonavicius et al. (2021) found that trust is an antecedent that affects privacy disclosure, especially in the context of interaction with online sites and assurances from regulatory systems. Hypothesis 2 is put forward:

H_2 Website trust has positive influence on users' privacy disclosure behavior.

3.2 Mediating role of internet privacy concerns

Privacy concerns as a major deterrent of consumers' willingness to disclose personal data (Fernandes and Pereira 2021). Because the understanding of privacy is relatively

subjective, privacy concern is generally taken as the core alternative variable in empirical studies. According to the enhanced APCO model proposed by Dinev et al. (2015), users will adopt different methods when making decisions on privacy disclosure behavior under the influence of many factors. If users directly disclose their privacy only by website clues and leave their digital footprints on network platforms, the decision-making method is a heuristic process with low effort cognition. However, users do not know how and to what extent the data collected by online websites will be used (Alkire et al. 2019), which leads to users' concerns about privacy and personal information data. Therefore, privacy disclosure is a process that needs careful consideration, and it is affected by different factors, involving users' adoption of more rational analysis and processing. Users will not simply judge self-disclosure according to website clues. Some studies demonstrate that privacy attitude and privacy behavior are inseparable from the specific perceived context of network users. That is, users' privacy concerns can directly affect their privacy disclosure behavior. In order to explain whether users with privacy concerns play a role in the mechanism of privacy disclosure behavior in different website clue situations, this study takes network privacy concerns as a mediating variable of website reputation, website trust and privacy disclosure behavior, and puts forward Hypothesis 3 and Hypothesis 4:

H_3 Internet privacy concerns play a mediating role between website reputation and user privacy disclosure behavior.

H_4 Internet privacy concerns a mediating role between website trust and users' privacy disclosure behavior.

3.3 Moderating effect of privacy calculus

Privacy calculus theory is a classical theory to analyze users' privacy disclosure behavior. It considers that individuals weigh the anticipated benefits of the action against perceived privacy risks or costs when giving out personal information (Li et al. 2019). Users will treat private information as a resource with exchange value. They will calculate between the expected risks of privacy and the potential benefits of disclosure, and then decide whether to disclose or not based on the result of the privacy trade-off (Cho et al. 2018). When the benefits of privacy disclosure are greater than the risks of privacy disclosure, users will tend to privacy disclosure.

As far as privacy behavior is concerned, the benefit of information disclosure refers to the benefit obtained by individuals from information disclosure, which is the result of the user's information disclosure that is beneficial to themself (Stone and Stone 1990). The benefits of privacy disclosure can vary in different contexts, including financial rewards, social rewards, perceived usefulness, personalization, self-representation, and enjoyment (Zhang et al. 2018). It positively and significantly affects users' disclosure behavior (Sun et al. 2021).

Information sensitivity has become the restraining factor of information disclosure behavior, and belongs to privacy risk. It refers to the degree of users' privacy concern about certain data under certain circumstances (Sheehan and Hoy 2000). Research points out that the costs or risks associated with decision-making will have a negative impact on the behavioral decision (Belanger et al. 2021), that is, privacy disclosure risks have a negative impact on privacy disclosure behavior (Yu et al. 2020).

Acquisti et al. (2015) pointed out that privacy calculus is related to context. In some cases, users are willing to share their personal information in exchange for certain benefits (such as discounts). In other cases, users will take extreme measures to protect their privacy. Therefore, this study regards information sensitivity and information disclosure benefits in privacy calculus as mediated adjustment, and proposes Hypothesis 5 and Hypothesis 6:

H_5 Information sensitivity plays a moderating role in the relationship between network privacy concerns and privacy disclosure behavior.

$H_{5\text{-}a}$ In the condition of website reputation, information sensitivity plays a moderating role in the relationship between internet privacy concerns and privacy disclosure behavior.

$H_{5\text{-}b}$ In the condition of website trust, information sensitivity plays a moderating role in the relationship between internet privacy concerns and privacy disclosure behavior.

H_6 Information disclosure benefits play a moderating role in the relationship between network privacy concerns and privacy disclosure behaviors.

$H_{6\text{-}a}$ In the condition of website reputation, information disclosure benefits play a moderating role in the relationship between Internet privacy concerns and privacy disclosure behavior.

$H_{6\text{-}b}$ In the condition of website trust, information disclosure benefits play a moderating role in the relationship between Internet privacy concerns and privacy disclosure behavior.

To sum up, the theoretical framework model is shown in Fig. 2.

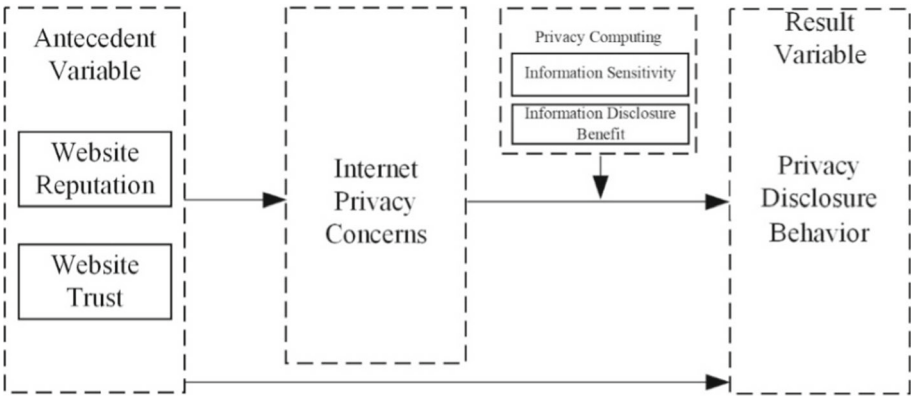

Fig. 2 Study model

4 Study design

4.1 Sample selection and data collection

With Chinese users who use online websites as the study objects, this study collected data by questionnaire and carried out empirical analysis. (1) The pre-investigation stages. First, in order to ensure the validity and reliability of the questionnaire, four experts were invited to discuss and revise the questions, so as to ensure that the statements were simple and clear. Second, 115 students and employees were randomly selected for pre-investigation, and the questionnaire questions were further revised and improved. (2) Formal investigation stage. The questionnaire survey data were collected and sorted by means of online distribution and offline distribution. The offline questionnaire was distributed through two channels: first, the special training course on talent cultivation, transformation and upgrading of small and medium-sized enterprises undertaken by the unit of the study group; second, the questionnaire was distributed to teachers and students in Guangzhou universities. Online questionnaire was distributed on Wenjuanxing website in China, and the survey objects included students and employees who did not fill out offline questionnaires. In this survey, 1,307 questionnaires were distributed from June to December, 2018, and 1,046 questionnaires were recovered. After removing 80 invalid questionnaires, 966 valid questionnaires were obtained, with the effective sample recovery rate of 73.9%. The descriptive statistical results of the samples are shown in Table 2.

4.2 Variable measurement

Combined with the specific study background, based on the mature scales used in Chinese and foreign literature, this study designed different scales for website reputation, website trust, internet privacy concerns, information disclosure benefits, information sensitivity and privacy disclosure behavior. Likert five-point scale was used for the main study variables, where "1" means "extremely inconsistent," "extremely disagreeable" and "very low," and "5" means "completely consistent," "very agreeable" or "very high." The measurement of each variable was completed. Website reputation was adapted from Gefen and Straub (2003), including three items. The website trust was adapted from Hong and Thong (2013), including four items. Internet privacy concern mainly refers to the study results of Xie et al. (2019), and it was divided into five sub-dimensions, including control, collection, errors, secondary use, improper access and remedy, with a total of 19 items; privacy disclosure benefit refers to the scales of Hui et al. (2007), Chellappa and Sin (2005), and Youn (2009), including three sub-dimensions: monetary incentive, personalized benefits and social benefits, with a total of nine items. According to the study design of Zhu et al. (2013) and Miline et al. (2017), the information sensitivity was mainly measured from six dimensions, including background information, consumption information, identity information, financial information, communication information and social relations information, with a total of 24 items. Combined with the measurement items of Melinda and Katherine (2008), Dienlin and Trepte (2015), privacy behavior involves six items. The details are given in Table 3. In addition, combined with the research purpose, this article sets up control variables, including the user's gender, online age, education level, and frequency of privacy concerns.

5 Empirical results and analysis

5.1 Reliability and validity

In this study, *Cronbach's Alpha* value in SPSS 20.0 analysis was used to test the reliability of variables, and AMOS 23.0 was employed to test the validity of variables by carrying out confirmatory factor analysis. The results show

Table 2 Descriptive statistical results of samples

Features	Category	Sample size	Proportion %	Features	Category	Sample size	Proportion %
Gender	Male	648	67.1	Age	18 years old and below	60	6.2
	Female	318	32.9		19–24 years old	438	45.3
Education level	Senior high school and below	27	2.8		25–34 years old	244	25.3
	College degree	149	15.4		35–44 years old	154	15.9
	Bachelor degree	647	67.0		45–54 years old	57	5.9
	Master degree	126	13.0		55 years old and above	13	1.3
	Doctoral degree and above	17	1.8	Frequency of privacy disturbance	Very frequent	458	47.7
Internet age	1 year and below	16	1.7		Relatively frequent	98	10.2
	2–5 years	156	16.1		Generally frequent	143	14.9
	6–10 years	407	42.1		Less frequent	81	8.4
	11–20 years	366	37.9		Never	122	12.7
	20 years and above	21	2.2				

Table 3 Variable measurement

Variable	Dimension	Number of items	Source
Website reputation	/	3	Gefen and Straub (2003)
Website trust	/	4	Hong and Thong (2013)
Internet privacy concern	Control, collection, reuse, errors, improper access and remedy	19	Xie et al. (2019)
Information disclosure benefit	Financial incentives, personalized service and social benefits	9	Hui et al. (2007)
			Chellappa and Sin (2005)
			Youn (2009)
Information sensitivity	Background information, consumption information, identity information, financial information, communication information and social relations information	24	Zhu Hui (2013)
			Miline et al. (2017)
Privacy disclosure behavior	/	6	Melinda and Katherine (2008)
			Dienlin and Trepte (2015)

that the *CITC* values of all items of website reputation and website trust are greater than 0.6, and the *Cronbach's Alpha* values are above 0.7. The *CITC* values of all items of internet privacy concerns are greater than 0.4, and the *Cronbach's Alpha* values are above 0.8. The *CITC* values of all items of information disclosure benefits are greater than 0.4, and the *Cronbach's Alpha* values are above 0.8. The *CITC* values of all items of information disclosure benefit are greater than 0.4, and the *Cronbach's Alpha* values are above 0.9. The *CITC* values of all items of privacy disclosure behavior are greater than 0.45, and the *Cronbach's Alpha* values are above 0.7, which indicates that the scale has good reliability.

In the test of validity, most variables in the questionnaire were measured by referring to the maturity scale used in Chinese and foreign studies. After being revised through interviews and expert consultation, the variables have higher content validity. In addition, the convergence validity and discrimination validity of the variables were tested. According to the division of dimensions, factor models are established for website reputation, website trust, network privacy concerns, information disclosure

benefits, information sensitivity and privacy disclosure behavior. The obtained indexes show that the fitting result is ideal, x^2 /*df* < 3, *RMR* = 0.42, *RMSEA* = 0.045, *CFI* = 0.918, *IFI* = 0.919, indicating that each variable has high discrimination validity. The normalized factor load of all items is between 0.550 and 0.957, and the *t* value shows high significance. In the meanwhile, the *CR* values of all variables are greater than 0.77, and the *AVE* values are basically above the threshold value of 0.49, which shows the good convergence validity.

5.2 Correlation analysis

The mean, standard deviation and correlation coefficient of the study variables are calculated by carrying out correlation analysis, and there is a certain correlation among the main variables, which are suitable for regression analysis. This lays an analytical foundation for testing the mediation effect and regulation effect, as shown in Table 4.

5.3 Hypothesis test

5.3.1 Test of main effect and mediation effect

Table 5 lists the regression results of the mediating effect of internet privacy concerns. Model 2 shows that website reputation and website trust have significant positive effects on privacy disclosure behavior ($\beta = 0.129$, $p < 0.001$; $\beta = 0.417$, $p < 0.001$). Therefore, H1 and H2 are supported. Model 4 is the model of the influence of mediating variables on privacy disclosure behavior. Internet privacy concerns play a partial mediating role in the relationship among website reputation, website trust and privacy disclosure ($\beta = -0.128$, $p < 0.001$). Therefore, H3 and H4 are supported.

5.3.2 Test of moderation effect of privacy calculus

Ye and Wen (2013) proposed a program to test the mediating regulatory effect after summarizing the methods of testing mediating regulatory models. The four steps are as below:

Step 1 Construct the regression equation of dependent variable (*Y*) to independent variable (*X*), regulating variable (*U*) and their interaction term (*UX*), and examine the regression coefficient. If it is significant, continue the following steps:

$$Y = c0 + c1X + c2U + c3UX + \varepsilon 1 \quad (1)$$

Step 2 Construct the regression equation of intermediate variable (*W*) to independent variable (*X*), regulating variable (*U*) and their interaction term (*UX*), and test the regression coefficients $a1$ and $a3$:

$$W = a0 + a1X + a2U + \mathrm{a}3UX + \varepsilon 2 \quad (2)$$

Step 3 Construct the regression equation of dependent variable (*Y*) to independent variable (*X*), intermediate variable (*W*), regulating variable (*U*), interaction term between independent variable and regulating variable (*UX*) and interaction term (*WU*) between intermediate variable and regulating variable (*WU*), and test whether regression coefficient $b1$ and $b2$, or $a3$ and $b1$, or $a3$ and $b2$ are significant or not, or calculate the confidence intervals of $a3b1$, $a3b2$ and $a1b2$.

$$Y = c'0 + c'1X + c'2U + c'3UX + b1W + b2UW + \varepsilon 3 \quad (3)$$

If any of the above regression coefficients are significant or the confidence interval does not contain 0, the influence of interaction term (*UX*) between independent variable and regulating variable on dependent variable (*Y*) is at least partly realized through mediating variable (*W*).

Step 4 Test coefficient $c'3$. If it is not significant, the regulatory effect has complete mediation. If it is significant, the regulatory effect has partial mediation.

Table 4 Mean, standard deviation and correlation coefficient of main variables

Variables	Mean	Standard deviation	1	2	3	4	5	6
Website reputation	3.716	0.748	1.00					
Website trust	3.008	0.805	0.086**	1.00				
Internet privacy concerns	4.262	0.483	0.290**	−0.137**	1.00			
Information disclosure benefits	3.536	0.676	0.428**	0.162**	0.326**	1.00		
Information sensitivity	2.639	0.697	−0.002	0.300**	−0.189**	0.069*	1.00	
Privacy disclosure behaviors	2.789	0.693	0.168**	0.415**	−0.136**	0.294**	0.411**	1.00

*represents $p < 0.05$; **represents $p < 0.01$; ***represents $p < 0.001$

Table 5 Test of mediation effects of internet privacy concerns

Variables	Privacy disclosure behaviors				Internet privacy concerns
	Model 1	Model 2	Model 3	Model 4	Model 5
Gender	−0.023	−0.005	−0.012	−0.005	0.081**
Internet age	−0.136***	−0.091**	−0.106**	−0.066*	0.190***
Education level	0.055	0.096**	0.046	0.084**	−0.094**
Frequency of privacy disturbance	−0.092**	−0.124***	−0.104**	−0.133***	−0.069*
Website reputation		0.129***		0.163***	0.266***
Website trust		0.417***		0.401***	−0.125***
Internet privacy concerns			−0.122***	−0.128***	
R^2	0.023	0.216	0.036	0.223	0.166
Adjusted R^2	0.018	0.211	0.031	0.218	0.161
F value	5.544***	118.550***	13.520***	17.084***	43.134***

*represents $p < 0.05$; **represents $p < 0.01$; ***represents $p < 0.001$

All tests were completed by using Bootstrap method, and realized by SPSS 20.0 and PROCESS. According to this procedure, this study carried out centralized processing for website trust, internet privacy concerns, information disclosure benefits and privacy disclosure behaviors. The analysis results are shown in Table 6.

According to the study of Ye and Wen (2013), the adjustment steps with mediation are verified. Only when website trust is an independent variable, internet privacy concern as a mediating variable, information disclosure benefit and an adjustment variable, and privacy disclosure behavior as a dependent variable, the test results are passed, and $H_{5-a,}$ H_{5-b} and H_{6-a} are not supported. According to the results in Table 6, the regression equation of the interaction items of website trust, information disclosure benefit, privacy disclosure behavior, website trust and information disclosure benefit is constructed in model 6 ($\beta = -0.172$, $p < 0.01$). The regression coefficients of the interaction terms of website trust and information disclosure benefits are significant, and the 95% confidence interval of this effect is [0.087, 0.210]. In model 7, by constructing the regression equation of internet privacy concerns on website trust, information disclosure benefits, website trust and information disclosure benefits, it is found that the regression coefficient of website trust and information disclosure benefits is significant ($\beta = 0.066$, $p < 0.01$), and the 95% confidence interval of this effect is [0.020, 0.113]. Based on model 6, the interaction items of internet privacy concerns and information disclosure benefits are added in model 8. The effect of interaction items of internet privacy concerns and information disclosure benefits on privacy disclosure behavior is still significant ($\beta = -0.161$, $p < 0.01$), and the 95% confidence interval of this effect is [−0.269, −0.054]. The results show that the mediation model is established, which means that under the premise of website trust, the interaction between internet privacy concerns and information disclosure benefits can partially regulate users' privacy disclosure behavior. Therefore, H_{6-b} is supported.

In order to present the moderating effect of information disclosure benefits more intuitively, this study takes the average value of information disclosure behavior plus or minus one standard deviation as the grouping standard, and describes the relationship between internet privacy concerns and privacy disclosure behavior in the conditions of high information disclosure benefits and low information disclosure benefits. The details are given in Fig. 3. When users perceive low information disclosure benefit (M-1SD), the effect of internet privacy concerns on privacy disclosure behavior is 0. 162 ($p < 0.001$). When users perceive high information disclosure benefit (M + 1SD), the effect of internet privacy concerns on privacy disclosure behavior is 0. 362 ($p < 0.001$). The difference in the effect of internet privacy concerns on privacy disclosure behavior under the two benefit levels of information disclosure is 0. 20, and the confidence interval of 95% difference value is [0.092, 0.420], which reaches the significant level. To sum up, when users perceive the benefits of high information disclosure, website trust will reduce users' internet privacy concern, thus increasing their privacy disclosure behavior.

5.4 Analysis of control variable

Users' gender ($\beta = -0.005$, $p > 0.05$) does not have significantly negative control effect on privacy disclosure behavior. Users' education level ($\beta = 0.084$, $p < 0.001$) has significantly positive control effect on privacy disclosure behavior. Sheehan (2000) found that people with

Table 6 Test results of moderation effects

Variables	M_6: Privacy disclosure behaviors			M_7: Internet privacy concerns			M_8: Privacy disclosure behaviors		
	β	SE	95% CI	β	SE	95% CI	β	SE	95% CI
Website trust	0.287***	0.025		−0.127***	0.0184		0.262***	0.025	
Information disclosure benefits	0.335***	0.032		0.268***	0.022		0.364***	0.032	
Website trust × Information disclosure benefits	−0.172**	0.031	[0.087,0.210]	0.066**	0.024	[0.020,0.113]	0.148***	0.031	[0.087,0.210]
Internet privacy concerns							− 0.313***	0.044	
Internet privacy concerns × Information disclosure benefits							−0.161**	0.055	[−0.269, −0.054]
R^2	0.262			0.150			0.279		
F value	85.448***			56.676***			74.343***		

*represents $p < 0.05$; **represents $p < 0.01$; ***represents $p < 0.001$

higher education level are more concerned about their internet privacy than those with lower education level. Therefore, this study speculates that people with higher education level will continuously improve their awareness and knowledge of internet security through learning so as to enhance their ability to identify privacy risks. They are more likely to choose privacy disclosure than those with low education level. Users' internet age ($\beta = -0.066$, $p < 0.05$) has a significantly negative effect on privacy disclosure behavior, and the frequency of privacy disturbance ($\beta = -0.133$, $p < 0.001$) has a significantly negative effect on privacy disclosure behavior. Generally speaking, the longer the users' internet age, the higher the frequency of privacy disturbance, which proves the conclusion of Hong et al. (2021): individuals who have experienced privacy disturbance will be more cautious when providing personal information to websites.

6 Conclusions

This study carried out empirical analysis of 966 samples. From the perspectives of the clue utilization theory and the privacy calculus theory, based on APCO model with mediation, the influence of website reputation and website trust on privacy disclosure behavior was discussed. Moreover, the mediating effects of internet privacy concerns and privacy calculus were introduced. The study results are shown in Table 7.

First, the study results reflect that website reputation and website trust have direct influence on users' privacy disclosure behavior, that is, they can verify the influence of the clue utilization theory on online website users' information disclosure behavior. Users evaluate websites according to clues such as website popularity and website trust, thus forming initial website cognition and making privacy disclosure decisions. The results show that higher website reputation and website trust have significant influence on users' privacy disclosure behavior. Users make direct and rapid low-effort cognitive decisions in privacy disclosure, which can help them easily obtain the convenience of using websites and save time cost.

Second, the results show that website reputation has significantly positive influence on internet privacy concerns, while website trust has significantly negative influence on internet privacy concerns. Website reputation has significant positive influence on internet privacy concerns, which may be related to the internet privacy leakage incidents of many famous websites in recent years. For example, the Facebook "leakage door" incident in 2018 resulted in the data leakage of 87 million users, who began to question the information security level of well-known websites. The websites with high reputation are used most

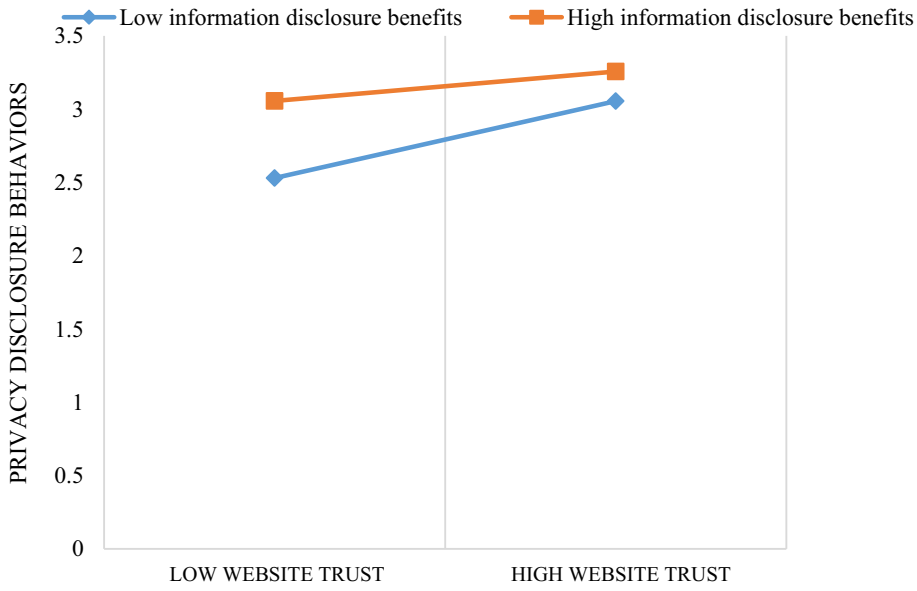

Fig. 3 Moderating effect of information disclosure benefits

frequently, the most personal information of users is disclosed. Once an information disclosure accident occurs, many important information of users will be disclosed, which aggravates users' concerns about privacy (Hong et al. 2021), thus leading to higher reputation of websites and concerns about network privacy. In addition, the influence of website trust on internet privacy concerns is consistent with the results of previous studies, that is, the higher the website trust, the lower the internet privacy concerns.

Third, the study results also prove that users' privacy disclosure behavior has complexity, which is not only positively influenced by website reputation and website trust, but also negatively influenced by internet privacy concerns. Once users have concerns about network privacy when using websites, they will make a series of prudent and rational high-effort cognitive decisions, instead of simple and quick low-effort cognitive decision. In addition, when users have privacy concerns, high-effort cognitive decision-making is manifested by weighing and calculating privacy risks and privacy benefits. According to the empirical results, when website trust is an independent variable, information disclosure benefit in privacy calculus has a moderating effect on the relationship between internet privacy concerns and privacy disclosure behavior.

6.1 Theoretical implications

First, based on the macro-APCO model, users' privacy disclosure behavior in the context of specific website clues was studied. This study used the measurement index system of privacy concerns suitable for Chinese context to make an empirical analysis of the influence mechanism of clues provided by websites (website reputation and website trust) and internet privacy concerns on users' privacy disclosure behavior. It is found that when users make privacy disclosure, they will make quick low-effort cognitive decisions directly based on clues such as website reputation and website trust. However, when users have internet privacy concerns, their privacy disclosure will become more cautious and complex. Users generally weigh the risks and benefits in privacy calculus before making privacy disclosure decision. In addition, the privacy issues in China were actively explored, which provided a new perspective for comprehensively understanding the mechanism of privacy disclosure.

Second, the study results demonstrate that privacy calculus plays a moderating role in the relationship between privacy concerns and privacy disclosure behavior only in specific context. Based on the clue utilization theory, clues such as website reputation and website trust have significant influence on online users' privacy disclosure behavior. However, when users have privacy concerns, the benefits of information disclosure only play a moderating role on the premise of website trust. It can be found that privacy calculus has the same moderating effect as internet privacy concerns and privacy disclosure behavior (Acquisti et al. 2015). The relationship among the antecedents of internet privacy concerns, internet privacy concerns and the results of internet privacy concerns are linked by privacy calculus, which further enriches and expands the privacy calculus theory and provides a basis for subsequent study.

Table 7 Study results

Theoretical assumptions	Support or not
H_1: Website reputation has positive influence on users' privacy disclosure behavior	Support
H_2: Website trust has positive influence on users' privacy disclosure behavior	Support
H_3: Internet privacy concerns play a mediating role between website reputation and user privacy disclosure behavior	Support
H_4: Internet privacy concerns play a mediating role between website trust and users' privacy disclosure behavior	Support
$H_{5\text{-}a}$: In the condition of website reputation, information sensitivity plays a moderating role in the relationship between internet privacy concerns and privacy disclosure behavior	Not supported
$H_{5\text{-}b}$: In the condition of website trust, information sensitivity plays a moderating role in the relationship between internet privacy concerns and privacy disclosure behavior	Not supported
$H_{6\text{-}a}$: In the condition of website reputation, information disclosure benefits play a moderating role in the relationship between Internet privacy concerns and privacy disclosure behavior	Not supported
$H_{6\text{-}b}$: In the condition of website trust, information disclosure benefits play a moderating role in the relationship between Internet privacy concerns and privacy disclosure behavior	Support

6.2 Practical implications

Empirical study results demonstrate that users generally decide privacy disclosure according to website reputation and website trust, which is the ideal result of cultivating website reputation and website trust. However, as users have more internet privacy concerns under the influence of different factors, they will no longer rely solely on their initial cognition of websites to decide their privacy disclosure behavior, which involves a more complex rational thinking process. In this case, websites will spend more money, time and manpower to reduce users' internet privacy concerns and encourage their' privacy disclosure behavior. Therefore, the following practical enlightenment can be obtained: First, as an important component of the era of big data, website platforms should cultivate users' positive perception of websites, and establish positive website reputation and cultivate website trust. Second, when users have internet privacy concerns, they will make thoughtful analysis because of external stimuli, which will lead to more complex privacy-related attitudes and behaviors. On the one hand, the government and industry should introduce relevant policies and regulations to create a positive network environment and atmosphere for users. On the other hand, empirical results show that website trust is more important than website reputation for online websites. Therefore, websites should not only give priority to how to build and enhance users' website trust, but also consider how to reduce users' privacy concerns, enhance the benefits of user privacy disclosure, and promote user privacy disclosure behavior from the user's perspective.

6.3 Limitations and future work

The limitations of this study and future study directions: First, this study obtained the cross-sectional data by issuing questionnaires, which cannot fully reflect the change of internet privacy concerns and privacy disclosure behavior with different contexts and time. In the future, the theoretical viewpoint should be further tested by collecting data and carrying out causality test based on the longitudinal study method. Second, the samples collected by the questionnaire survey are Chinese Internet users. In future study, the samples from different countries can be expanded. It will be more meaningful to conduct cross-border and cross-cultural privacy research. Third, it is urgent to analyze the influencing factors of users' privacy concerns and privacy disclosure behavior from the perspective of stakeholders. Some studies have pointed out that the participation of the government and enterprises is necessary in order to collect and share data in a sustainable way and reduce privacy and security issues (Ilhan and Fietkiewicz 2020). Similarly, the participation behaviors of the government and internet enterprises can also influence users' privacy concerns and privacy disclosure behaviors (Gong et al. 2019; Ilhan and Fietkiewicz 2020). Therefore, future study will take the privacy behaviors of the government and enterprises into account to verify whether and how they influence users' privacy concerns and privacy disclosure behaviors.

Authors contributions XIE Weihong is the supervisor of the paper and is responsible for questionnaire design, data collection, and paper revision. ZHANG Qian is responsible for the analysis of questionnaire data and the writing of the paper.

Funding General program of National Natural Science Foundation of China (No. 71672043) provided funding for this research.

Data availability Enquiries about data availability should be directed to the authors.

Declarations

Conflict of interest The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethics approval This article does not contain any research conducted by the author on human participants or animals.

Informed consent All authors agree to submit this edition and declare that no part of this manuscript has been published or submitted elsewhere.

References

Acquisti A, Grossklags J (2005) Privacy and rationality in individual decision making. IEEE Secur Priv 3(1):26–33

Acquisti A et al (2015) Privacy and human behavior in the age of information. Science 347(6221):509–514

Aljukhadar M et al (2010) Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environments. Int J Electron Commer 14(4):103–126

Alkire L et al (2019) Triggers and motivators of privacy protection behavior on Facebook. J Serv Mark 33(1):57–72

Bansal G et al (2016) Do context and personality matter? Trust and privacy concerns in disclosing private information online. Inf Manag 53(1):1–21

Belanger F et al (2021) Privacy maintenance in self-digitization: the effect of information disclosure on continuance intentions. Data Base Adv Inf Syst 52(2):7–24

Benamati JH et al (2017) An empirical test of an antecedents-privacy concerns-outcomes model. J Inf Sci 43(5):583–600

Chellappa RK, Sin RG (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inf Technol Manag 6(2–3):181–202

Cho JY et al (2018) Strategic approach to privacy calculus of wearable device user regarding information disclosure and continuance intention. KSII Trans Internet Inf Syst 12(7):3356–3374

Choi B et al (2018) Love at first sight: the interplay between privacy dispositions and privacy calculus in online social connectivity management. J Assoc Inf Syst 19(3):124–151

Dawar N, Parker P (1994) Marketing universals: consumers' use of brand name, price, physical appearance, and retailer. J Mark 58(2):81–95

Desimpelaere L et al (2020) Knowledge as a strategy for privacy protection: how a privacy literacy training affects children's online disclosure behavior. Comput Hum Behav 110:1–12

Dienlin T, Trepte S (2015) Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur J Soc Psychol 45(3):285–297

Dinev T et al (2015) Informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Inf Syst Res 26(4):639–655

Erevelles S et al (2016) Big data consumer analytics and the transformation of marketing. J Bus Res 69(2):897–904

Fernandes T, Pereira N (2021) Revisiting the privacy calculus: why are consumers (really) willing to disclose personal data online. Telematics Inform 65:101717

Gefen D, Straub D (2003) Managing user trust in B2C e-services. E-Service 2(2):7–24

Gefen D et al (2003) Trust and TAM in online shopping: an integrated model. MIS Q 27(1):51–90

Gong X et al (2019) What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity. Inf Technol People 33(4):1174–1213

Hallam C, Zanella G (2017) Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput Hum Behav 68:217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hong WY, Thong JYL (2013) Internet privacy concerns: an integrated conceptualization and four empirical studies. MIS Q 37(1):275–298

Hong WY et al (2021) Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. J Bus Ethics 168(3):539–564

Hui KL et al (2007) The value of privacy assurance: an exploratory field experiment. MIS Q 31(1):19–33

Ilhan A, Fietkiewicz KJ (2020) Data privacy-related behavior and concerns of activity tracking technology users from Germany and the USA. Aslib J Inf Manag 73(2):180–200

Ioannou A et al (2020) Privacy concerns and disclosure of biometric and behavioral data for travel. Int J Inf Manag 54:102–122

Jin GZ, Kato A (2006) Price, quality, and reputation: evidence from an online field experiment. Rand J Econ 37(4):983–1004

Johnson GA et al (2020) Consumer privacy choice in online advertising: who opts out and at what cost to industry? Mark Sci 39(1):33–51

Kai L et al (2015) An empirical analysis of users' privacy disclosure behaviors on social network sites. Inf Manag 52(7):882–891

Kolotylo-Kulkarni M et al (2021) Information disclosure in e-commerce: a systematic review and agenda for future research. J Bus Res 126:221–238

Li P, Cho H, Goh ZH (2019) Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. Telemat Inf 41:114–125. https://doi.org/10.1016/j.tele.2019.04.006

Malhotra NK et al (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355

Martin KD, Murphy PE (2017) The role of data privacy in marketing. J Acad Mark Sci 45(2):135–155

Mcknight DH, Chervany NL (2001) What trust means in E-commerce customer relationships. Int J Electron Commer 6(2):35–59

Melinda LK, Katherine TB (2008) The influence of personality traits and information privacy concerns on behavioral intentions. J Comput Infor Syst 48(4):15–24

Melumad S, Meyer R (2020) Full disclosure: how smartphones enhance consumer self-disclosure. J Mark 84(3):28–45

Menard P, Bott GJ (2020) Analyzing IoT users' mobile device privacy concerns: extracting privacy permissions using a disclosure experiment. Comput Secur 95:1–14

Milne GR, Boza ME (1999) Trust and concern in consumers' perceptions of marketing information management practices. J Interact Mark 13(1):5–24

Milne GR et al (2017) Information sensitivity typology: mapping the degree and type of risk consumers perceive in personal data sharing. J Consum Aff 51(1):133–161

Muhammad S et al (2018) Analysis of factors that influence customers' willingness to leave big data digital footprints on social media: a systematic review of literature. Inf Syst Front 20(3):559–576

Osatuyi B et al (2018) " Fool me once, shame on you … then, I learn." an examination of information disclosure in social Networking Sites. Comput Hum Behav 83:73–86

Proudfoot JG et al (2018) Saving face on facebook: privacy concerns, social benefits, and impression management. Behav Inf Technol 37(1):16–37

Roghanizad M, Neufeld DJ (2015) Intuition, risk, and the formation of online trust. Comput Hum Behav 50:489–498

Shane-Simpson C, Manago A, Gaggi N, Gillespie-Lynch K (2018) Why do college students prefer facebook, twitter, or instagram? site affordances, tensions between privacy and self-expression, and implications for social capital. Comput Hum Behav 86:276–288. https://doi.org/10.1016/j.chb.2018.04.041

Sheehan K (2000) Toward a typology of internet users and online privacy concerns. Inf Soc 18(1):21–32

Sheehan KB, Hoy MG (2000) Dimensions of privacy concern among online consumers. J Public Policy Mark 19(1):62–73

Shen N, Bernier T, Sequeira L, Strauss J, Silver MP, Carter-Langford A, Wiljer D (2019) Understanding the patient privacy perspective on health information exchange: A systematic review. Int J Med Inf 125:1–12. https://doi.org/10.1016/j.ijmedinf.2019.01.014

Smith HJ et al (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Q 20(2):167–196

Smith HJ et al (2011) Information privacy research: an interdisciplinary review. MIS Q 35(4):989–1015

Stone EF, Stone DL (1990) Privacy in organizations: theoretical issues, research findings, and protection mechanisms. Res Pers Hum Resour Manag 8(3):349–411

Sun YQ et al (2021) Calculus interdependency, personality contingency, and causal asymmetry: toward a configurational privacy calculus model of information disclosure. Inf Manag 58(8):103556

Sun YQ et al (2022) Do individuals disclose or withhold information following the same logic: a configurational perspective of information disclosure in social media. Aslib J Inf Manag. https://doi.org/10.1108/AJIM-06-2021-0180

Thompson N, Brindley J (2021) Who are you talking about? contrasting determinants of online disclosure about self or others. Inf Technol People 34(3):999–1017

Urbonavicius S et al (2021) From social networking to willingness to disclose personal data when shopping online: modelling in the context of social exchange theory. J Bus Res 136:76–85

Westin AF (2010) Social and political dimensions of privacy. J Soc Issues 59(2):431–453

Williams LJD (2003) A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. Mark Lett 14(4):257–272

Wirtz J, Lwin MO (2009) Regulatory focus theory, trust and privacy concern. J Serv Res 12(2):190–207

Xie WH et al (2019) Construction and measurement of online privacy concerns based on multidimensional development theory (China). J Mod Inf 39(01):137–147

Ye BJ, Wen ZL (2013) A discussion on testing methods for mediated moderation models: discrimination and integration (China). Acta Psychol Sin 45(09):1050–1060

Youn S (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. J Consum Aff 43(3):389–418

Yu L et al (2020) A meta-analysis to explore privacy cognition and information disclosure of internet users. Int J Inf Manage 51:102015

Zhang X et al (2018) Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Inf Manag 55(4):482–493

Zhu H et al (2013) Research on information privacy boundaries and sensitivity of net users (China). J Guangdong Univ Technol 30(04):26–32