Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

Role of Algorithm Awareness in Privacy Decision-Making Process: A Dual Calculus Lens

Sujun Tian *, Bin Zhang and Hongyang He

School of Economics and Management, Beijing University of Posts and Telecommunications, Beijing 100876, China; binzhang@bupt.edu.cn (B.Z.); hehongyang@bupt.edu.cn (H.H.)
* Correspondence: tiansujun@bupt.edu.cn

Abstract: In the context of AI, as algorithms rapidly penetrate e-commerce platforms, it is timely to investigate the role of algorithm awareness (AA) in privacy decisions because it can shape consumers' information-disclosure behaviors. Focusing on the role of AA in the privacy decision-making process, this study investigated consumers' personal information disclosures when using an e-commerce platform with personalized algorithms. By integrating the dual calculus model and the theory of planned behavior (TPB), we constructed a privacy decision-making model for consumers. Sample data from 581 online-shopping consumers were collected by a questionnaire survey, and SmartPLS 4.0 software was used to conduct a structural equation path analysis and a mediating effects test on the sample data. The findings suggest that AA is a potential antecedent to the privacy decision-making process through which consumers seek to evaluate privacy risks and make self-disclosure decisions. The privacy decision process goes through two interrelated trade-offs—that threat appraisals and coping appraisals weigh each other to determine the (net) perceived risk and, then, the (net) perceived risk and the perceived benefit weigh each other to decide privacy attitudes. By applying the TPB to the model, the findings further show that privacy attitudes and subjective norms jointly affect information-disclosure intention whereas perceived behavioral control has no significant impact on information-disclosure intention. The results of this study give actionable insights into how to utilize the privacy decision-making process to promote algorithm adoption and decisions regarding information disclosure, serving as a point of reference for the development of a human-centered algorithm based on AA in reference to FEAT.

Keywords: information disclosure; algorithm awareness; dual calculus model; theory of planned behavior

Citation: Tian, S.; Zhang, B.; He, H. Role of Algorithm Awareness in Privacy Decision-Making Process: A Dual Calculus Lens. *J. Theor. Appl. Electron. Commer. Res.* **2024**, *19*, 899–920. https://doi.org/10.3390/jtaer19020047

Academic Editors: Jiaming Fang, Chao Wen and Benjamin George

Received: 13 March 2024
Revised: 16 April 2024
Accepted: 17 April 2024
Published: 20 April 2024

1. Introduction

Given that big data and artificial intelligence (AI) become broadly penetrative in society, data-driven algorithms are gradually penetrating into all aspects of our lives and increasingly becoming an indispensable part of it [1]. Indeed, the success of e-commerce platforms, like Amazon and Alibaba, hinges heavily on consumer data and personalized algorithms that enable platforms (and the firms behind them) to tailor services and products more accurately, with advantages for both firms (such as increased recall and more purchases) and their customers (such as better preference matches and conveniences). However, despite these obvious benefits to both, the integration of personalized algorithms also raises ethical and privacy concerns [2]. That is, algorithms operate behind the interface, tracking consumer online behaviors and regulating what becomes available to consumers without themselves knowing what the algorithms are or their functions [1], which gives rise to what we refer to as the algorithm black-box-like problem. On the one hand, this issue is likely to cause consumer privacy concerns about their personal information possibly being inappropriately collected, utilized, or processed by algorithmic platforms without their consent. Thus, consumers would take protective actions—such as refusing to provide

information to a platform, providing inaccurate information, or removing information from a platform [3]—to reduce the privacy risk, which will not be conducive to healthy platform growth in the long run. On the other hand, in view of the increasing realization that consumers deserve to know what algorithms are, how algorithms work, where algorithms are deployed, and the intent and goals of those developing algorithms and taking control of consumer data and privacy [4], the black-box issue related to algorithms has thus garnered vast public attention that is paid to algorithm awareness (AA), which refers to common individuals' general knowledge about the existence and functioning of algorithms based on their practice and experience in interaction with algorithmic platforms [5], including transparency, accountability, fairness [6], and more recently, explainability [4] (i.e., the key concepts of FEAT).

Indeed, previous studies have indicated that most consumers lack an understanding of how these algorithmic platforms automate recommendations for them, despite the widespread utilization of personalized algorithms on various platforms [7]. Put simply, general consumers often remain unaware of how their personal information is collected and processed, as well as how such algorithms work, let alone taking the initiative to manage their privacy on such platforms. Accordingly, the concern regarding how to improve consumer awareness and understanding of algorithms has been a topic of debate over the last few years. Eslami et al. [8] propose that consumers develop a perception of algorithms resulting from active interaction with personalized algorithms. Zarouali et al. [9] argue that the key to cultivating AA is to realize how consumers make sense of an algorithm's attributes, capability, recommendations, and quality of personalization. Furthermore, the cognition that individuals develop about fairness, transparency, and accountability of personalized algorithms is necessary for them to accept personalized algorithms [10] and helps them assess and decide the ways of interacting with algorithmic platforms because educated judgments result in informed decisions [9]. Recent studies have consistently emphasized the effects of AA on consumers' subsequent behaviors, such as those related to privacy decisions and interactions with algorithms. For example, Gran et al. [7] point out the importance of consumer awareness because it shapes behaviors. Zarouali et al. [9] propose that AA might influence consumers and their information-disclosure behaviors. That is, once consumers become aware of how personalized algorithms work and the potential harms associated with algorithmic platforms accessing their personal information, they may need to make an informed decision regarding whether and when to disclose such information. Therefore, making an awareness evaluation of algorithms can be a key initial step to ensuring that users can make informed privacy evaluations and decisions [11,12]. In light of the backdrop of increasing concerns for privacy, examining the relationship between AA and privacy by focusing on how consumers evaluate privacy in the context of algorithms based on AA in reference to FEAT represents a theoretically intriguing and practically important research effort.

While the effect of individual factors (such as personal privacy experiences/awareness and personality/demographic differences) and external factors (such as personalization approaches—covert or overt—and privacy policies) on consumer information-disclosure behavior has already been elaborated on in the existing research, very few studies have examined the role of AA as an explanatory factor in consumer privacy decision-making process, which indicates a clear research gap. Consequently, this study explicitly considers the role of AA in consumer personal information disclosure towards platforms with personalized algorithms. This is important because it enables us to extend not only the knowledge of AA and privacy but also the relationship between both [13]. On this basis, our study sets forth to examine the following research questions:

RQ1: What roles does AA play in privacy decisions related to personal information disclosure, especially in the context of AI-driven personalized recommendations?

RQ2: What is the underlying mechanism of action between AA and consumer intentions to disclose personal information?

To address our research questions (RQ), we draw on the integration framework of the dual calculus model and the theory of planned behavior to construct a privacy decision-making model, which not only highlights two interrelated trade-offs that influence an individual's information-disclosure behavior—including the risk calculus (i.e., weighing between privacy threat and coping mechanisms) along with the privacy calculus (i.e., weighing between perceived benefits and privacy risks)—but also combines these two trade-offs together with the theory of planned behavior to predict the consumer intention of online self-disclosure. Moreover, this study conducted a randomized online survey with 581 participants from Chinese e-commerce-platform consumers. Based on our theoretical model and empirical research, we empirically examine how consumers perceive personalized algorithms through FEAT, how AA influences consumers' threat appraisals and coping appraisals regarding algorithms, and how these perceptions come together to establish consumers' privacy concerns (i.e., the risk calculus). Then, we weigh privacy concerns against perceived benefits to develop their privacy attitude (i.e., the privacy calculus) and, ultimately, see how those factors along with the constructs from the theory of planned behavior jointly influence their intention to disclose personal information while using an e-commerce platform with personalized algorithms.

This study seeks to make three main contributions. First, our study contributes to the literature on algorithm awareness (AA) and privacy decisions by providing empirical evidence on the role of AA in the privacy decision-making process. The endeavor represents a response to calls for more empirical explorations regarding the interactions between humans and algorithms so as to design and develop responsible AI. Second, our study synthesizes the dual calculus model and the theory of planned behavior to analyze the mechanisms of action between AA and intentions to disclose personal information, which thus sheds light on the internal utility mechanism behind AA. Third, from a managerial viewpoint, we offer algorithmic platforms (and the firms behind them) actionable guidance on how to develop human-centered AI against the dehumanizing trends of algorithmic designs and operations, how to optimize consumers' algorithm experience, and how to promote informed privacy decisions, ultimately promoting healthy platform growth.

2. Literature Review and Theoretical Background

2.1. Algorithm Awareness

Explaining the interaction between humans and algorithms from the perspective of consumers has become a new research trend. Studies have consistently shown that when users are aware of algorithms and their functionality, this awareness influences how they behave online [5]. For instance, Gutierrez et al. [14] argue that how consumers make sense of algorithms shapes the behavioral ways through which they interact and engage with algorithms. In particular, within the field of information systems, consumer sensemaking can influence their information behaviors, such as sharing, giving a like, and commenting. However, a significant challenge lies in the fact that algorithm systems are proprietary and remain inaccessible to end-consumers, which makes it challenging to establish an objective notion or evaluation of AA, and they differ considerably among people [5]. Despite such restrictions, it is possible and meaningful to investigate how consumers develop AA and how to cultivate an algorithmic culture [15], which will have a significant impact on interactive relationships between humans and algorithms, and help in promoting algorithmic platforms to embed consumer awareness of algorithm as an intrinsic requirement of algorithm development and operations.

In the review of the literature on AA, it can be found that the early research examining AA was mainly through the ways of algorithmic imagery and folk theories. These approaches have limited effectiveness for investigating the interaction between humans and algorithms though. In recent years, scholars have increasingly linked AA with the FEAT issues in the field of AI [16] and explored the connotation and denotation of AA by constructing relevant measurement scales. For example, Swart [17] relates AA to concepts such as fairness, transparency, and trust. Zarouali et al. [9] argue for fairness, accountability,

and transparency as sub-components of AA. In addition, explainability has been discussed as yet another component of AA [4]. As such, Shin et al. [5] measured the AA of consumers from the four dimensions of fairness, explainability, accountability, and transparency, that is, what we refer to as FEAT, and developed a scale to measure AA, laying the foundation for this study. The conceptualization of AA based on FEAT gives significant implications that go beyond "know-what" and is instead the pursuit of recognizing the context, acquiring self-efficacy to assess quality and potential threat of algorithms, and meaningfully controlling human interaction with algorithms by evaluating and managing privacy on algorithmic platforms.

2.2. Information Disclosure

The concern regarding consumer privacy behaviors in the context of AI-driven personalized e-commerce platforms has increased over the last few years. For example, Xu et al. [18] explored the impact of personalized methods (overt/covert) and consumer individual characteristics on their willingness to disclose location information. Liu et al. [19] studied the influence of consumer cognitive factors (such as perceived ownership, perceived surveillance, privacy value orientation, and perceived effectiveness of privacy policies) on cognitive trade-offs and disclosure decisions. As personalized algorithms continue to play an increasingly important role in the development of platforms, scholars have increasingly believed that how to handle the relationship between algorithms and consumer privacy concerns has become a crucial factor in influencing consumer information-disclosure behaviors and the sustainable development of platforms [20]. Zhang et al. [21] proposed that it is necessary to find the right balance between personalization and privacy so as to achieve a win-win situation for both businesses and consumers.

Therefore, the research on the relationship between AA and privacy concerns has gradually received attention. Existing studies have found that, when consumers have a positive attitude toward platform algorithms, they often engage in efficiency-enhancing behaviors to improve the quality of matching (such as consciously disclosing preference information to "train the algorithm") [22]; conversely, they are more likely to engage in privacy risk-avoidance behaviors or even abandon usage (such as refusing to provide personal information, providing incorrect information, or deleting browsing history) [3]. It can be inferred that the shaping process of algorithm awareness on consumer self-disclosure behaviors is a manifestation of individual consciousness driving behavior. Each individual understands algorithms in his or her own cognitive processes and further generates their own privacy attitudes and information-disclosure intention based on AA, though there may be technological barriers of algorithms toward individuals. Therefore, in the era of AI with algorithms as the core driving force, it is crucial to consider consumer AA as an antecedent variable and investigate deeply its influence as well as mechanism of action on privacy decisions. Taken together, the related studies have shown the importance of AA and the gaps in understanding the relationship between AA and privacy [9]. Yet, our knowledge about the role of AA in consumer information-disclosure behaviors is still limited, especially the knowledge of the internal utility mechanisms behind AA, though AA is a potentially key predictor or antecedent for predicting privacy and information-disclosure decisions.

2.3. Dual Calculus Model

Much research has been conducted from various theoretical perspectives on consumers' concerns about online information privacy in the e-commerce environment, in which the privacy calculus is a common approach to studying the joint effect of opposing forces on privacy perception and behavior [23]. Privacy calculus theory (PCT) suggests that an individual's intention to disclose personal information is based on a calculus of behavior in which consumers perform the risk–benefit analysis and decide whether to disclose information based on the net outcomes [24]. Consumers' intentions to disclose information in various contexts have been studied in the literatures which were through the privacy calculus theory, such as in the context of e-commerce [25], social media [26], and IT-enabled

ride-sharing [27]. With further research, some scholars have found that privacy decision-making could also be affected by the effectiveness of risk response, and only a privacy calculus cannot accurately reflect the level of individual perception of privacy risks [23]. Accordingly, Li [23] developed an integrated framework that highlights two interrelated trade-offs that influence an individual's information-disclosure behavior: the privacy calculus (i.e., the trade-off between expected benefits and privacy risks that measures an individual's perceived net privacy risks) and the risk calculus (i.e., the trade-off between privacy risks and the efficacy of coping mechanisms). These two trade-offs that together predict an individual's intention to provide information in online transactions are called the dual calculus model, which reveals the internal process of individual information-disclosure decisions in a more comprehensive way. However, current research based on this theory is limited and is especially lacking in empirical tests of the theory.

2.4. Theory of Planned Behavior (TPB)

The theory of planned behavior has also been used to analyze individual privacy disclosure behavior, which suggested that an individual's volitional behavior depends jointly on motivation (i.e., intention) and ability (i.e., perceived behavioral control), and motivation is, then, determined by attitude, subjective norm, and perceived behavioral control [28]. The perceived behavioral control refers to an individual's perceived controllability of behavior based on past experience (such as privacy protection and invasion) and the anticipated abilities to carry out the behavior. The theory further suggests that attitude, subjective norm, and perceived behavioral control are each the summative index of the strengths of some salient beliefs multiplied by the subjective evaluations of the beliefs. For example, attitude toward information disclosure is determined by perceived benefits and perceived risks of the disclosure behavior, whereas the relative strengths of the two beliefs in a given context determine the individuals' overall attitude within that context. Studies built upon TPB emphasize the direct impact of privacy attitude on intention, whereas other antecedents such as subjective norm and perceived behavioral control are less frequently analyzed. Although empirical studies provided almost unanimous support for the direct impact of privacy belief on intention, the other two predictors, subjective norm and perceived behavioral control, should not be ignored [23].

3. Hypotheses Development and Research Model

3.1. Understanding the Algorithm Awareness through Threat Appraisals and Coping Appraisals

Given that FEAT is regarded as describing different aspects of individual algorithmic awareness, this study considers algorithmic awareness as a second-order formative variable encompassing four variables, reflecting consumers' perception of platform algorithms. Specifically, algorithmic fairness refers to the absence of any bias in algorithmic decisions towards the inherent or acquired characteristics of individuals or groups [29]. Although algorithmic automated decisions can, to some extent, escape human control, they may also incorporate human biases, leading to biased and discriminatory decision outcomes and thereby causing public concern about algorithmic fairness [30]. Once such a perception of unfairness is formed, it can erode consumers' trust and trigger negative emotions and threat perceptions. Additionally, as algorithmic decisions increasingly permeate into people's daily lives and social operations, the risk of harm caused by unfair decision outcomes is also increasing. Secondly, algorithmic explainability refers to the ability to explain why a product or content is recommended. As one of the indicators for evaluating the performance of recommendation systems, explainability is as equally important as recommendation accuracy [4]. Explanations provided by algorithms can help dispel public concerns about the loss of decision-making autonomy and alleviate aversion to algorithms, thereby increasing consumer trust. On the other hand, algorithms lacking effective explanation mechanisms can lead to a black-box effect, which not only reduces consumer satisfaction with recommendation results but also easily triggers negative emotions, such as anxiety, fear, and threat [31]. Furthermore, algorithmic accountability emphasizes the

attribution and allocation of responsibilities for the social impacts caused by algorithms, determining the share of responsibility borne by algorithm platforms and establishing remedial mechanisms for the harms caused by algorithmic decisions [32]. This ensures that damages can be assessed, controlled, and remedied. The frequent occurrence of algorithmic misconduct and the lack of social responsibility easily erode consumers' confidence in platform algorithms. The establishment of an algorithm accountability mechanism can help trace and correct decision-making errors or adverse consequences of platform algorithms, thereby promoting consumers to establish positive confidence and enhancing their perception of coping effectiveness. Finally, algorithmic transparency refers to the degree of explanation regarding why and how an algorithm is used, emphasizing the reasonable openness of data usage and the algorithm's inherent logic [6]. As an information regulatory mechanism, algorithmic transparency is considered the fundamental force driving algorithm governance, serving as a tool to aid algorithm accountability and improve algorithm design [33]. Reasonable transparency of algorithms is crucial for maintaining trust between platform enterprises and data subjects, helping to unlock the black box of algorithms and alleviate consumers' concerns about the loss of control over the decision-making process of algorithms [34].

The process of obtaining information and completing transactions for consumers on e-commerce platforms is also a process of interaction with the algorithm of platforms. During this interaction, they form algorithmic awareness, which refers to their cognition and evaluation of the fairness, explainability, accountability, and transparency of the algorithms. Based on this awareness, they make judgments about threat appraisals of privacy and the effectiveness of their coping mechanisms. According to the protection motivation theory, threat appraisal refers to the cognitive judgment of risk susceptibility (i.e., the probability of a threatening event occurring) and risk severity (i.e., the severity of adverse consequences caused by the threatening event) when an individual faces a threat. The coping appraisal refers to the cognitive judgment of individuals' response effectiveness (i.e., the effectiveness of protective behaviors that can be taken) and self-efficacy (i.e., confidence in one's ability to perform protective behaviors) when responding to threats [35]. The more negative consumers' perceptions and evaluations of platform algorithms are, the stronger their perception of the likelihood and severity of privacy risks will be. And, the weaker their perception of the effectiveness of the protective behaviors they can take, their self-efficacy will be simultaneously [5]. Therefore, we hypothesize that:

H1. *Algorithm awareness is negatively related to perceived vulnerability;*

H2. *Algorithm awareness is negatively related to perceived severity;*

H3. *Algorithm awareness is positively related to response efficacy;*

H4. *Algorithm awareness is positively related to self-efficacy.*

3.2. Understanding the Outcomes of Risk Calculus

3.2.1. Threat Appraisals and Privacy Concerns

Risk calculation measures the perceived net risk of consumers' self-disclosure by weighing between threat appraisals and coping appraisals, enabling an accurate portrayal of the consumers' privacy risk level [23]. Li's research [23] indicates that, in the field of information privacy, threat appraisals have a positive impact on the perception of privacy risk, while coping appraisals have a negative impact on the perception of privacy risk. In the context of e-commerce, consumers' clickstream data, purchase data, and self-disclosed data, such as likes, forwards, and comments on the shopping platform, will all leave digital traces. Enterprises use information technologies such as data mining to collect, process, and screen consumers' fragmented data, constructing precise consumer profiles to help enterprises achieve precise matching between people and products. While this enables

personalized services, it also opens the door to privacy breaches, thus posing potential threats to consumers' privacy and security. Obviously, when individuals realize that such privacy threats are highly likely to occur or will cause serious consequences, their perceived privacy risks will be higher. Therefore, we hypothesize that:

H5. *Perceived vulnerability is positively related to perceived risks;*

H6. *Perceived severity is positively related to perceived risks.*

3.2.2. Coping Appraisals and Privacy Concerns

Platforms and consumers can also take protective measures to mitigate the negative effects of information disclosure. For example, platforms can provide privacy policies to help consumers understand how their personal information is collected and processed, as well as the potential privacy-protection measures that may be taken. Consumers, on the other hand, can manage their personal information by mastering certain privacy settings, or reduce the risk of privacy breaches by providing incorrect information or deleting browsing history, thereby reducing privacy concerns to a certain extent. Generally speaking, consumers tend to have a higher perception of privacy risk when facing privacy threats that are more severe, have a higher probability of occurrence, or when individuals lack effective preventive measures and confidence in their protective abilities. Conversely, when the negative effects of information disclosure are minor or individuals are confident in their ability to cope with the privacy threat, consumers' perception of privacy risk is relatively lower [36]. Therefore, we hypothesize that:

H7. *Response efficacy is negatively related to perceived risks;*

H8. *Self-efficacy is negatively related to perceived risks.*

3.3. Understanding the Outcomes of Privacy Calculus

Privacy calculus serves as an important prerequisite for a privacy decision, referring to the process where individuals weigh risks against benefits to maximize perceived benefits and minimize the risks associated with information disclosure. Perceived benefits and perceived risks are the cores of the privacy calculus [37]. In the context of e-commerce, the perceived benefits of information disclosure include accurate recommendations, personalized services, and economic rewards [38]. Especially in the era of information overload, consumers often suffer from decision fatigue when faced with the vast array of products on the market. Accurate recommendations and personalized services based on consumer profiles can effectively reduce the cost of information search and have become the primary motivation for individuals to disclose their information [39]. On the other hand, the perceived risks of information disclosure include a series of adverse consequences and potential losses caused by the loss of data control, such as the illegal acquisition and use of personal information, price discrimination based on personal data, identity theft, or advertising harassment [37]. Previous studies have shown that consumers' perceived benefits from information disclosure positively influence their privacy attitudes, while perceived risks negatively affect their privacy attitudes [18]. Therefore, we hypothesize that:

H9. *Perceived benefit is positively related to privacy attitude;*

H10. *Perceived risk is negatively related to privacy attitude.*

3.4. Understanding the Information-Disclosure Intention through the Theory of TPB

3.4.1. Privacy Attitude and Information-Disclosure Intention

The Theory of Planned Behavior, originally proposed by Ajzen and extensively utilized to predict and interpret diverse behavioral decisions among individuals, suggests

that behavioral intention is shaped by three primary factors, that is, behavioral attitude, subjective norms, and perceived behavioral control. Behavioral attitude refers to an individual's evaluative tendency towards a particular behavior within a given context, and a more favorable evaluation correlates with a stronger behavioral intention [23]. In the realm of information-disclosure decisions, an individual's attitude towards disclosing information is primarily driven by external compensatory factors. Smith et al. [38] have pointed out that personalized services, financial rewards, access to functional privileges, and various social benefits serve as incentives for individuals to disclose personal information. For instance, Xu et al.'s research [18] has suggested that users disclose their location information to access nearby resources and receive tailored push notifications. Consequently, individuals with a positive attitude tend to believe that disclosing personal information can bring them external compensatory benefits, thus generating a positive willingness to disclose. Therefore, we hypothesize that:

H11. *Privacy attitude is positively related to information-disclosure intention.*

3.4.2. Subjective Norm and Information-Disclosure Intention

Subjective norms refer to the pressure that an individual perceives from society when making a decision about whether to engage in a particular behavior. It reflects the influence of significant others or groups around the individual on their behavioral decisions [40]. The more positive the perception of significant others around the individual towards their engagement in a certain behavior, the stronger their intention to engage in that behavior. In the context of information-disclosure decisions, when friends and family members actively recommend self-disclosure behaviors to other individuals after experiencing convenience, discounts, and other positive outcomes, the individual might generate a stronger motivation and willingness to disclose information influenced by demonstration effects and compliance motives. Previous studies have found that subjective norms positively affect an individual's willingness to disclose information on electronic health websites. It suggested that the greater the offline recommendation among website users, the greater the likelihood of users disclosing information [41]. Therefore, we hypothesize that:

H12. *Subjective norm is positively related to information-disclosure intention.*

3.4.3. Perceived Behavioral Control and Information-Disclosure Intention

Perceived behavioral control refers to the degree to which an individual perceives the ease or difficulty of performing a specific behavior, reflecting their awareness of the factors that either facilitate or hinder the enactment of that behavior [40]. If an individual's perceived behavioral control is low, it suggests that they perceive more uncontrollable factors, making it more difficult to carry out the behavior. Conversely, a high level of perceived behavioral control indicates that the individual perceives the behavior to be within their control and mastery, resulting in a strong behavioral intention [40]. In the context of e-commerce, the data-utilization behavior driven by algorithms is fraught with uncertainty and complexity. Accordingly, when consumers believe that they can control their privacy information and take protective measures to effectively counter the threat of privacy breaches, they will have a more positive willingness to disclose information. Conversely, they may perceive a higher privacy risk and suppress their willingness to disclose information. At the same time, when consumers possess a strong sense of perceived behavioral control, it also indicates that they have a strong belief in their ability to protect their privacy information based on their existing knowledge, their capabilities of risk identification and avoidance, and past experiences (such as the experience of privacy violations). That is, their sense of self-efficacy is strong. Therefore, we hypothesize that:

H13. *Perceived behavioral control is positively related to information-disclosure intention;*

H14. *Perceived behavioral control is positively related to self-efficacy.*

As shown in Figure 1, the dual calculus model integrated with the theory of planned behavior is used as a framework in this study. The model examines the role of algorithm awareness in the privacy decision-making process, which employs risk calculus and privacy calculus as the transmission mechanisms.

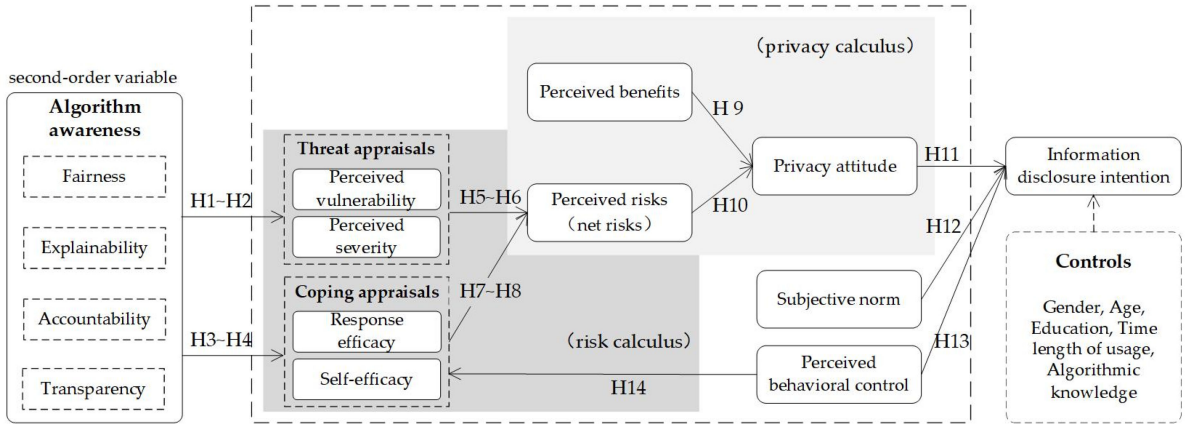

Figure 1. Research model.

4. Materials and Methods

4.1. Scale Development

To obtain the research instruments, we adapted constructs into the research model from measurement scales used in the existing literature to fit the e-commerce context (see Appendix A). All multi-item constructs were measured by a 7-point Likert scale that ranges from 1 (strongly disagree) to 7 (strongly agree), except for the demographic variables and control variables. First, we invited 95 Chinese e-commerce-platform users to participate in a pretest. After the pretest, we refine the language presentation of the questionnaire items. Additionally, we invited eight experts in the related field and Ph.D. candidates in management to verify the readability of the items.

In the questionnaire scale, algorithmic awareness is a second-order formative variable, including four first-order reflective variables, that is, fairness (Fai), explainability (Exp), accountability (Acc), and transparency (Tra), which were all measured with three items, respectively, taken from Shin et al. [5]. Perceived vulnerability (PV) and perceived severity (PS) were both assessed based on three items adapted from Zhang et al. [36]. Response efficacy (RE) and self-efficacy (SE) were both measured with three questions taken from Johnston et al. [42]. Perceived benefits (PB) and perceived risks (PR) were both assessed based on three items adapted from Xu et al. [43]. With regard to the constructs of the TPB, privacy attitude (PA) was measured with three questions derived and modified from Xu et al. [18], subjective norm (SN) was assessed based on three items adapted from Kaushik et al. [44], and perceived behavioral control (PBC) was measured with three questions taken from Xu et al. [45]. Finally, we used three items to measure the information-disclosure intention (INT) adapted from Xu et al. [43].

4.2. Sample and Data Collection

An online survey was employed to collect sample data via Credamo. The questionnaire comprised four parts. The first part described the purpose of the academic research and the condition of the participant's voluntary and anonymous involvement upon survey completion. The second part evidently stated that only users with online-shopping experience could participate. Additionally, participants were instructed to fill in the e-commerce platform they have used most frequently in the past three months and to recollect their us-

age experiences during that period. The third part included questions designed to measure the constructs in this research. The fourth part contained demographic questions.

The subjects of this study were limited to Chinese e-commerce users, with 620 questionnaires submitted. To ensure data quality, we removed questionnaires that were invalid or took less than 1 min to answer. Finally, 581 valid questionnaires were obtained. It is an acceptable level because a sample size ranging from 100 to 400 is suggested when engaging in complex structure modeling, though the PLS method can work with even smaller sample sizes [46]. In terms of demographic characteristics, the percentage of females was 53.528%, and 18~35 year olds made up the dominant group among the participants (74.355%). The percentage of users with a bachelor's degree was 78.830%. Moreover, 67.986% of the participants had been using e-commerce platforms for 2 years or more, indicating that most of them had a certain level of experience with, exposure to, awareness of, and attitudes toward personalized algorithmic e-commerce platforms, which helps ensure the quality of the questionnaire.

4.3. Common Method Variance

Because all sample data were collected from a single source and obtained from subject self-reports, common method variance (CMV) could exist. Three approaches were used to assess CMV in this study. First, according to existing research, Harman's one-factor test often works well in addressing CMV, which is commonly associated with the survey approach [47]. The results showed that the first factor explained approximately 34.22% of the total variances, which is less than the reference value of 40%. Second, the values of correlations among constructs should be less than 0.9 to indicate a lack of CMV [48]. The results showed that the maximum correlation coefficient between the variables is 0.732, which is less than 0.9. Third, following suggestions from Kock et al. [49], if the variance inflation factor (VIF) of all variables in the model is less than 3.3, it indicates that no bias exists in single-source data. The VIFs for all constructs in this study were 1.000~3.141. As a result, we consider that the CMV in this study was not a serious problem.

5. Result

This study employed partial least squares (PLS) to test and evaluate the research model. Compared with covariance-based structural equation modeling (CB-SEM), PLS is a variance-based SEM and is more liberal on sample size and data-distribution requirements than CB-SEM. In addition, PLS can handle complex structural models with multiple variables and is suitable for dealing with formative variables [50]. Due to the complex model under study, which incorporates mediating factors and second-order formative variables, we employed SmartPLS (version. 4.0) to evaluate and test the measurement model and structural model.

5.1. Validity and Reliability (Measurement Model)

Several assessments were conducted to examine the reliability and validity of the questionnaire in order to ensure both convergent validity and discriminant validity. As shown in Table 1, the Cronbach's alpha values and composite reliability (CR) of all variables are greater than 0.700, indicating that the scale has good internal consistency and a high level of reliability. Additionally, the average variance extracted (AVE) of each factor exceeds the threshold of 0.500, which demonstrates that the scale has good convergent validity.

Table 1. Reliability and validity of the scales.

Variables	Cronbach's α	CR	AVE
Fai	0.808	0.887	0.725
Exp	0.858	0.915	0.784
Acc	0.841	0.904	0.76
Tra	0.808	0.887	0.724
PV	0.858	0.914	0.779
PS	0.889	0.931	0.819
RE	0.892	0.933	0.822
SE	0.899	0.938	0.834
PB	0.846	0.907	0.766
PR	0.847	0.908	0.766
PA	0.813	0.889	0.728
SN	0.925	0.952	0.87
PBC	0.773	0.868	0.688
Int	0.859	0.914	0.779

Discriminant validity requires that the correlation between different constructs should be relatively low. This study examines the discriminant validity among constructs through three indicators, that is, the Fornell–Larcker criterion, the cross-loadings, and the heterotrait–monotrait ratio (HTMT). First, as shown in Appendix B, the square roots of the AVE values for each variable surpass the correlation coefficients between the variable and other variables, aligning with the recommendation of Fornell et al. [51]. Secondly, according to Appendix C, the primary loadings of each item exceed their respective cross-loadings. Finally, as indicated in Appendix D, all HTMT values fall below the reference value of 0.850 proposed by Kline [52]. These results suggest that each variable exhibited an acceptable discriminant validity.

Furthermore, algorithm awareness in the research model is conceptualized as a second-order formative variable whose validity can be assessed by examining the weights and variance inflation factors (VIF) [53]. According to Table 2, the weights of the four first-order dimensions of algorithm awareness are statistically significant at the 0.001 level, and all the VIF values are below 2.600, which satisfies the threshold criterion of being less than 3.3. These results indicate that this second-order formative variable demonstrates robust validity.

Table 2. Validity analysis of algorithm awareness (second-order formative variable).

Second-Order Variable	Second-Order Variable	Weight	t-Value	*p*-Value	VIF
algorithm awareness	Fairness	0.251	4.371	0.000	2.567
	Explainability	0.214	4.353	0.000	2.006
	Accountability	0.488	11.698	0.000	1.877
	Transparency	0.229	4.203	0.000	2.406

5.2. Evaluating the Structural Model

Prior to testing the research hypotheses, this study evaluated the validity of the structural model using the coefficient of determination (R^2) and the cross-validated correlation coefficient (Q^2). Among them, R^2 is an effective indicator to measure the explanatory power of the model, reflecting the extent to which the exogenous variables account for the total variation in endogenous variables. Concurrently, Q^2 is used to measure the predictive relevance of the model. According to the results, the R^2 values of all endogenous variables in the model range from 0.345 to 0.674, with adjusted R^2 values ranging from 0.344 to 0.672. Both are higher than the reference value of 0.19 proposed by Chin [54], indicating satisfactory explanatory power for the endogenous variables. Additionally, the Q^2 values of the endogenous variables range from 0.276 to 0.510, exceeding the threshold of zero proposed by Geisser [55], which suggests that the model has good predictive relevance.

We used SmartPLS (version. 4.0) to evaluate the structural model. The findings depicted in Figure 2 demonstrate that consumers' privacy decision-making processes in the context of e-commerce include three stages, that is, privacy antecedents, privacy trade-offs, and privacy decision-making.

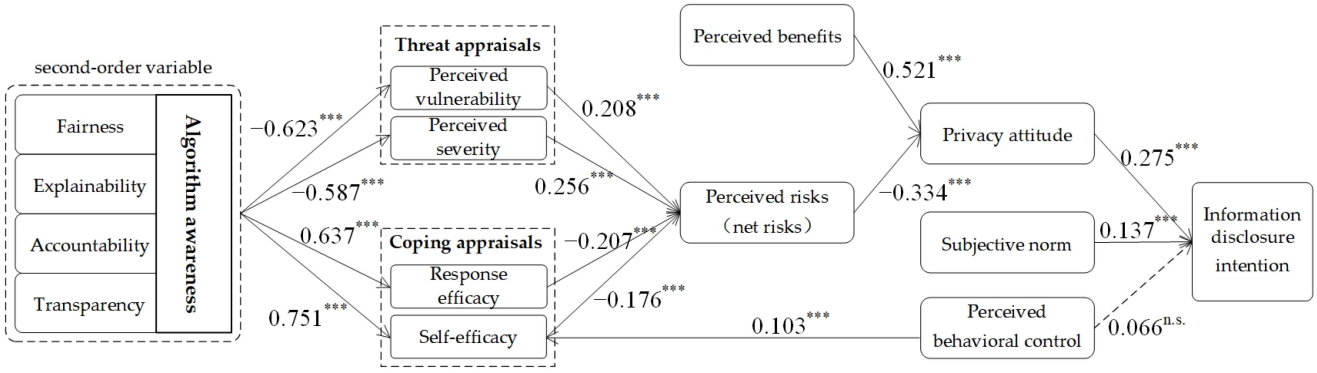

Figure 2. Hypotheses testing results for the research model. "***" denote $p < 0.001$ and "n.s." represents no significance.

First, in relation to privacy antecedents, this study specifically focuses on the critical antecedent of consumers' algorithm awareness. The evaluation results indicate that algorithm awareness has a significant negative impact on perceived vulnerability ($\beta = -0.623$, $p < 0.001$) and perceived severity ($\beta = -0.587$, $p < 0.001$), thus confirming our proposed H1 and H2. Simultaneously, it positively and significantly influences response efficacy ($\beta = 0.637$, $p < 0.001$) and self-efficacy ($\beta = 0.751$, $p < 0.001$), validating our proposed H3 and H4 accordingly.

Second, the privacy trade-off stage involves two interrelated calculations. In the risk calculation, both perceived vulnerability and perceived severity have a significant positive impact on perceived risk, as confirmed by the significance tests ($\beta = 0.208$, $p < 0.001$ and $\beta = 0.256$, $p < 0.001$), thus confirming our proposed H5 and H6. Concurrently, response efficacy and self-efficacy exert a significant negative influence on perceived risk ($\beta = -0.207$, $p < 0.001$ and $\beta = -0.176$, $p < 0.001$), confirming our proposed H7 and H8. Consequently, threat-appraisal variables increase the perception of privacy risk, while coping-appraisal variables offset part of this risk perception, resulting in a perceived net risk through the trade-off between the two. In the privacy calculation, the perceived net risk significantly and negatively affects privacy attitude ($\beta = -3.334$, $p < 0.001$), while perceived benefit significantly and positively influences privacy attitude ($\beta = 0.521$, $p < 0.001$), confirming our proposed H9 and H10. Notably, the impact of perceived benefit on privacy attitude is more than 1.5 times greater than that of perceived net risk, making it the dominant force influencing privacy attitude, which aligns with the findings of Chellappa and others [39].

Finally, in the privacy decision-making stage, both privacy attitude and subjective norms have a significant positive impact on information-disclosure intention, as confirmed by the significance tests ($\beta = 0.275$, $p < 0.001$ and $\beta = 0.137$, $p < 0.001$), thus supporting hypotheses H11 and H12. Additionally, consumers' perceived behavioral control has a significant positive influence on self-efficacy ($\beta = 0.103$, $p < 0.001$), validating hypothesis H14. However, the positive effect of perceived behavioral control on information-disclosure intention is insignificant, and thus, hypothesis H13 is not supported.

In addition, the control variable tests reveal that consumer gender, education level, and the duration of using the platform have significant positive impacts on information-disclosure intention, which is consistent with the findings of Liu et al. [19]. Furthermore, this study also finds that older consumers and those with a deeper understanding of algorithmic knowledge tend to have a more pronounced intention to disclose their personal information.

5.3. Testing the Mediating Effects

The mediation effects of the protection motivation mechanism on the paths from algorithm awareness (AA) to (net) perceived risks and the mediation effects of privacy attitude on the path from perceived benefits and (net) perceived risks to information-disclosure intention were tested using Preacher and Hayes (2008)'s bootstrapping methodology. A bootstrapping analysis with 5000 resamples was performed to test these mediation effects, running on the SmartPLS (version. 4.0) software tools. Detailed results of the mediation effect analysis are given in Table 3.

Table 3. Test results for mediation effects.

Paths	Indirect Effect	Bias Corrected 95%CI		Direct Effect	Bias Corrected 95%CI	
		UCL	LCL		UCL	LCL
AA→PV→PR	−0.130	−0.172	−0.089			
AA→PS→PR	−0.150	−0.194	−0.103	−0.105	−0.181	−0.010
AA→RE→PR	−0.132	−0.187	−0.084			
AA→SE→PR	−0.132	−0.205	−0.059			
PR→PA→INT	−0.092	−0.125	−0.063	−0.123	−0.198	−0.052
PB→PA→INT	0.143	0.105	0.183	0.156	0.093	0.215

The results show that the mediating paths between consumers' algorithm awareness and perceived risks include AA→PV→PR, AA→PS→PR, AA→RE→PR, and AA→SE→PR. The bias-corrected 95% CI for these four paths are [−0.172, −0.089], [−0.194, −0.103], [−0.187, −0.084], and [−0.205, −0.059], respectively, none of which includes zero, indicating that the mediating effects are all significant. Additionally, the direct-effect value of algorithm awareness on perceived risk is −0.105, with a bias-corrected 95% CI of [−0.181, −0.010], which excludes zero, indicating that the direct effect is also significant. Therefore, perceived vulnerability (PV), perceived severity (PS), response efficacy (RE), and self-efficacy (SE) partially mediate the relationship between consumers' algorithm awareness and perceived risk. It can be concluded that consumers' algorithm awareness indirectly affects privacy risk through the trade-off between threat-appraisal variables and coping-appraisal variables within the framework of the protection motivation mechanism. That is, the protection motivation mechanism plays a partial mediating role between algorithm awareness and perceived risk.

Furthermore, the mediating path between perceived risks and information-disclosure intention is PR→PA→INT, with a bias-corrected 95% CI of [−0.125, −0.063]. The confidence interval does not include zero, indicating a significant mediating effect. Additionally, the direct-effect value of perceived risk on information-disclosure intention is −0.123, with a bias-corrected 95% CI of [−0.198, −0.052]. Since the confidence interval excludes zero, the direct effect is also significant. Therefore, consumers' privacy attitude (PA) partially mediates the relationship between perceived risk and information-disclosure intention. On the other hand, the mediating path between perceived benefits and information-disclosure intention is PB→PA→INT, with a bias-corrected 95% CI of [0.105, 0.183]. The confidence interval does not include zero, indicating a significant mediating effect. In addition, the direct-effect value of perceived benefits on information-disclosure intention is 0.156, with a bias-corrected 95% CI of [0.093, 0.215]. Again, the confidence interval excludes zero, indicating a significant direct effect. Therefore, consumers' privacy attitude (PA) also partially mediates the impact of perceived benefits on information-disclosure intention. In conclusion, both perceived benefits and perceived risks influence their information-disclosure intention through the partial mediating role of privacy attitude.

Taken together, the results suggest that the effect of algorithm awareness (AA) on (net) perceived risks is partially mediated via perceived vulnerability, perceived severity, response efficacy, and self-efficacy, and then, the effect of perceived benefits and (net) perceived risks on information-disclosure intention is partially mediated via privacy attitude.

The role of these factors as mediators may help platforms in identifying and utilizing factors that may determine algorithm acceptance and use.

6. Conclusions and Discussion

6.1. Discussion of Findings

Based on an integrated framework of the dual calculus model and the theory of planned behavior, this study extends existing findings on privacy by clarifying how consumers make sense of algorithms based on FEAT, and how their perception of algorithm awareness (AA) influences privacy and leads to information disclosure. The findings of this study offer meaningful insights into the relationships among AA, (net) privacy risks, privacy attitude, and information-disclosure intention in the context of algorithmic e-commerce platforms. Put differently, this study shows the specific roles and processes of AA in consumers' privacy decisions related to personalized algorithms.

First, the findings proposed that the processes of interaction with algorithmic platforms cultivate individuals' AA, which indicates a consumer's own cognition of algorithm attributes and features—including fairness, explainability, accountability, and transparency (i.e., reference to FEAT). Just as it does in social systems, the issues of FEAT have been regarded as essential values in algorithm-based platforms, and consumers seek assurances on them during interaction with algorithms [5]. As the findings suggest, AA promotes the awareness evaluation of performance, attitude, and intention. Accordingly, AA can serve as a baseline to understand how consumers are empowered to find the right balance between personalization and privacy when using algorithmic platforms.

Second, the findings clarified that the development of AA is a psychological antecedent of the dual calculus process through which consumers seek to predict privacy risks and make the decision to disclose information. The role of AA in privacy decisions has remained largely unknown, particularly in the context of an AI-driven personalized algorithm [9]. As such, we approached AA as a key antecedent to assess the privacy and subsequent actions of informed self-disclosure. Specifically, the model showed that the level of AA influences consumers' threat appraisals and coping appraisals regarding algorithms and ultimately leads to subsequent evaluations toward (net) privacy risk through the risk calculus process. This argument is supported by the mediation role of the protection motivation mechanism—which emphasizes the combined effect of threat appraisal and coping appraisal—in the relationship between AA and (net) privacy risks. Accordingly, this finding highlighted the importance of AA as a facilitating mechanism, illustrating that consumers' awareness of algorithms should be translated into coping efficacy, which then facilitates subsequent positive attitudes toward privacy evaluation. That is, improving consumers' awareness of algorithms and capability helps them to activate the protection motivation mechanism, deal with privacy risks, and, thus, reduce privacy concerns. Subsequently, the model further suggested that a trade-off occurs between (net) perceived risk and perceived benefit, which determines privacy attitudes through the privacy calculus process. Moreover, the mediating effects of privacy attitude on the paths from perceived benefits or (net) perceived risks to information-disclosure intention implied that the outcomes of a risk–benefit analysis based on the privacy calculus process can lead to self-disclosure only when potential benefits outweigh risks.

Taken together, by focusing on consumers' privacy decision-making processes based on the dual calculus model, we elaborated how consumers interact with algorithms through their own cognitive processes of AA based on FEAT (H1, H2, H3, and H4), how these factors influence consumers' perceptions of (net) privacy risks through the risk calculus (H5, H6, H7, and H8), and how they seek to determine the privacy attitude through the privacy calculus (H9, H10) and ultimately assess information-disclosure intention (H11). The complex chain of action can become a key clue to understanding algorithm qualities, algorithm experiences, and interactions between consumers and algorithmic platforms.

Third, by applying TPB to our model, we further found that subjective norms among consumers along with their own privacy attitude both have a positive influence on the

information-disclosure intention (H11, H12), except for perceived behavioral control, which is contrary to the assumptions of TPB (H13). The finding implied that informed self-disclosure while interacting with personalized algorithms depends on motivation (including privacy attitude and subjective norms). Thus, the consumer privacy decision-making process is not a singular activity and involves instead multiple paths and shapes [23]. Yet, from the unexpected results, the insignificant positive relation between perceived behavior control and information-disclosure intention, it can be inferred that the effect of perceived behavior control on self-disclosure is offset by the privacy attitude dominated by the perceived benefits (H9, H11) and subjective norms affected by the bandwagon effect (H12). This argument offers meaningful insights into the phenomenon that we refer to as the privacy paradox (i.e., ambivalent attitudes and behaviors on privacy issues, where saying is one thing and practical action is another) [18]. Indeed, because of privacy concerns, consumers desire to have some control over what personal data are gathered, how these data are utilized and analyzed, and to what extent their information is or would be processed [14]. In fact, however, they may perceive a limited sense of control over their privacy, primarily because engaging with AI represents a novel aspect, coupled with its inherent black-box nature [56]. With the increasing dependence on online shopping and personalization among consumers, they may surrender a certain level of control over privacy in exchange for personalized recommendations that are considered beneficial and worth the risks [5]. Accordingly, we suggest that, due to the rapid algorithmification of platforms and the lack of alternative functions or services, they have to cede some privacy control to get access, and the privacy paradox may thus be a reluctant choice for consumers.

6.2. Theoretical Implications

Our work advances contributions to the ongoing discussion on human–algorithm interactions [5]. The results make certain theoretical refinement in the following ways.

First, our study addresses a crucial yet underexplored question: how does consumers' awareness of algorithmic mechanisms influence their privacy decision-making process? This marks our initial attempt to bridge the gap between privacy concerns, information disclosure, and consumers' algorithmic awareness (AA). Given the growing concerns surrounding the adverse impacts of information technology in the realm of information systems, our research serves as a timely response to scholars in the information-privacy field who are calling for more inquiries into the internal mechanisms of consumers' AA in the era of AI, where algorithms play a pivotal role. By focusing on the core dimensions of AA—fairness, explainability, accountability, and transparency—and developing a privacy decision-making model to investigate its impact on consumer decisions regarding information disclosure, our study begins to unwrap the complex inner workings of AA. This, in turn, broadens the scope of existing research on information-disclosure behavior, offering valuable insights into the intricate relationship between consumers' algorithmic understanding and their privacy choices.

Second, our study introduces the concept of risk calculus to investigate information-disclosure behavior, marking a preliminary empirical attempt to test the dual calculus theory. Prior research has primarily examined information disclosure from the privacy calculus theory lens, leaving a gap in the exploration of this behavior through the dual calculus perspective, especially in terms of empirical validations. Therefore, our study empirically tests the transmission mechanism of both a risk and a privacy calculation, providing a comprehensive understanding of the internal processes that underlie the impact of AA on intention to disclose information. Furthermore, unlike previous studies that primarily focused on the relationship between privacy attitudes and information-disclosure intention, we integrate attitude, subjective norms, and perceived behavioral control—key constructs from the Theory of Planned Behavior (TPB)—within a unified framework of information disclosure. By combining the dual calculus model with TPB, we construct an integrated model that validates how these three variables jointly influence individuals' willingness to disclose information. This approach also offers novel insights

into understanding the privacy paradox, where individuals often express concern for privacy but still engage in disclosure behaviors.

6.3. Practical Implications

The significance of empowering consumers to make privacy decisions in an informed and principled way has increased. Compared to existing researchers who mainly propose their own solutions to the issue of how to enhance consumer information disclosure from two aspects—individual factors (such as personal privacy experiences/awareness and personality/demographic differences) [18] and external factors (such as personalization approaches and privacy policies) [19]—a meaningful practical implication of this study is that consumer sensemaking plays an active role in interaction with algorithmic platforms and provides a point of reference for the development of a human-centered algorithm. Certain features of the algorithm provide consumers with clues for performance evaluation and trust, and thus, consumers can actively control algorithmic curations by feelings of algorithm usefulness and credibility [14]. That is, consumers develop their own cognitive processes of AA based on FEAT [5], and in turn, AA affects the algorithm through informed actions [57] Thus, they are critical rudiments in the design and practice of the algorithm, given that what people perceive affects how they behave. As such, humans are considered both consumers and producers of algorithm systems because algorithms show what consumers want to see and what is relevant based on their own sensemaking results [5]. Therefore, consumer supervision based on AA becomes one of the necessary means that facilitates and ensures meaningful human-controllable algorithms by fulfilling essential values, namely fairness, transparency, accountability, and explainability, which are the key concepts of FEAT.

Another important practical contribution of this study is that it gives actionable insights into how to utilize the privacy decision-making process to promote algorithm adoption and decisions regarding information sharing. As the findings suggest, consumers make awareness valuations to make decisions about whether to share personal data with algorithms in exchange for personalized benefits through a process of dual calculus as well as TPB. Thus, drivers of information disclosure should be considered through the procedural view, and relevant strategies can be analyzed from the following aspects.

First, as AA significantly affects privacy risks through threat appraisals and coping appraisals, algorithmic platforms should proactively embed FEAT in algorithm design and operation to enhance the consumer's algorithm experience and increase interaction with algorithms. Therefore, platforms with personalized algorithms should have a strategy for how algorithm design and operation are fair, transparent, responsible, and in accordance with social norms. Specifically, the relevant measures may include these aspects—disclosing the fairness criteria of algorithms and related rationales during algorithm registration, which can reduce potential biases, errors, and discriminatory harms in the algorithm; disclosing the internal logic of algorithms and explaining why to recommend to consumers, which can improve the transparency and persuasiveness of the recommendation system; claiming and correcting errors or adverse consequences caused by the algorithm, which promotes improvement of the justice of the algorithm; and incorporating the algorithm assessment into enterprise development plans, establishing internal audit mechanisms algorithm, and actively cooperating with external algorithm audits, which all can facilitate algorithms being human-aware and help consumers to have meaningful control over algorithms.

Second, as perceived benefits significantly positively affect privacy attitudes and perceived risks have a significantly negative influence, the industry can benefit from exercising some measures to enhance consumers' perceived benefits and reduce their privacy concerns during online shopping. E-commerce platforms should improve the quality of products and services and meet consumers' personalized needs, which is the key to cultivating the satisfaction and loyalty of consumers. Meanwhile, a proactive approach towards a positive corporate brand, coupled with strict adherence to respecting and protecting consumers'

personal information, along with the implementation of cutting-edge privacy-protection technologies, can significantly bolster consumers' trust in platforms. These elevate their confidence in the privacy-protection measures taken and go some way to alleviate certain concerns they may have regarding the handling of their personal information.

Third, on the basis of the results of TPB in our model, privacy attitudes and subjective norms have significant positive impacts on information-disclosure intention whereas the positive impact of perceived behavioral control remains insignificant. A privacy paradox phenomenon may arise, trapping consumers in a situation where they have to weigh the personalized benefits against their privacy concerns. As consumers increasingly desire control over their personal information, it will be a disadvantage to healthy platform growth. Therefore, it is important to empower consumers to have control over their personal information.

In addition, policymakers and consumer advocacy groups also play an important role in supporting human-centered algorithms. To foster a positive algorithmic environment, policymakers can regulate algorithms through the enactment of relevant legislation similar to GDPR. For instance, legislating to require algorithm platforms to increase transparency and disclose the fundamental principles and operational methods of their algorithms can aid the public in better understanding how algorithms impact their daily lives. Simultaneously, they can establish a specialized algorithm audit institution to examine the fairness, transparency, and impartiality of algorithms, ensuring that algorithm platforms adhere to certain ethical and legal provisions when designing their algorithms. Policymakers should also establish an accountability mechanism, clarify the legal responsibilities of algorithm platforms in the event of issues, and set up effective complaint and appeal channels to protect consumer rights. Moreover, consumer advocacy groups can also become an important force in promoting human-controllable AI. For example, they can publish research reports that delve into various algorithmic platforms and uncover potential issues and biases, providing consumers with objective and comprehensive information. Furthermore, these groups can develop and promote algorithmic ethics guidelines, encouraging businesses to voluntarily adhere to these standards and thereby elevating the moral standards of the entire industry.

6.4. Limitations and Prospects

This study is applicable to exploring the interactive behaviors between humans and algorithmic platforms, particularly in investigating the impact of AA developed in human interaction with algorithms on information-disclosure behaviors. Yet, there are still certain limitations in this study that are worthy of further research. Given that the privacy decision-making process is a complex process influenced by multiple factors, appropriate moderator variables can be added to the model of this study in the future to explore the boundary conditions and how algorithm awareness affects privacy decision-making. Furthermore, this study collected sample data through questionnaire surveys. Due to certain inherent restrictions of the method, there may be deviations yet between consumers' actual privacy decision-making behaviors in the market and their disclosure intentions. Therefore, future studies can combine experimental methods, such as scenario experiments or event-related potentials (ERP), to investigate consumer behavioral data.

Author Contributions: Conceptualization, S.T., B.Z. and H.H.; methodology, S.T. and H.H.; software, S.T. and H.H.; investigation, S.T. and H.H.; resources, B.Z.; data curation, S.T. and H.H.; writing—original draft preparation, S.T. and H.H.; writing—review and editing, S.T. and B.Z.; supervision, B.Z.; funding acquisition, S.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Major project of the National Social Science Foundation of China (Grant No. 18VZL010) and the BUPT Excellent Ph.D. Students Foundation of the Beijing University of Posts and Telecommunications (Grant No. CX2023203).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Survey Instrument

Variables	Measures
Fairness (Fai)	1. An algorithmic platform does not discriminate against people and does now show favoritism (Nondiscrimination). 2. The source of data throughout an algorithmic process and its data analysis should be accurate and correct (Accuracy). 3. An algorithmic platform complies with the due process requirements of impartiality with no bias (Due process).
Explainability (Exp)	1. I found algorithmic platforms to be comprehensible. 2. The AI algorithmic services are understandable. 3. I can understand and make sense of the internal workings of personalization.
Accountability (Acc)	1. An algorithmic platform requires the person in charge to be accountable for its adverse individual or societal effects in a timely manner (Responsibility). 2. The platforms should be designed to enable third parties to audit and review the behavior of an algorithm (Auditability). 3. The platforms should have the autonomy to change the logic in their entire configuration using only simple manipulations (Controllability).
Transparency (Tra)	1. The assessment and the criteria of algorithms used should be publicly open and understandable to users (Understandability). 2. Any results generated by an algorithmic system should be interpretable to the users affected by those outputs (Interpretability). 3. Algorithms should let people know how well internal states of algorithms can be understood from knowledge of their external outputs (Observability).
Perceived Vulnerability (PV)	1. My information privacy is at risk of being invaded. 2. It is likely that my information privacy will be invaded. 3. It is possible that my information privacy will be invaded.
Perceived Severity (PS)	1. If my information privacy is invaded, it would be severe. 2. If my information privacy is invaded, it would be serious. 3. If my information privacy is invaded, it would be significant.
Response Efficacy (RE)	1. The privacy protection measures provided by this platform work for protecting my information. 2. The privacy protection measures provided by this platform can effectively protect my information. 3. When using privacy protection measures provided by this platform, my information is more likely to be protected.
Self-Efficacy (SE)	1. Protecting my information privacy is easy for me. 2. I have the capability to protect my information privacy. 3. I am able to protect my information privacy without much effort.
Perceived risks (PR)	1. Providing this platform with my personal information would involve many unexpected problems. 2. It would be risky to disclose my personal information to this platform. 3. There would be high potential for loss in disclosing my personal information to this platform.
Perceived benefits (PB)	1. This platform can provide me with personalized services tailored to my activity context. 2. This platform can provide me with more relevant information tailored to my preferences or personal interests. 3. This platform can provide me with the kind of information or service that I might like.
Privacy attitude (PA)	1. I think my benefits gained from the use of this platform can offset the risks of my information disclosure. 2. The value I gain from use of this platform is worth the information I give away. 3. Overall, I feel that providing this platform with my information is beneficial.

Variables	Measures
Subjective Norm (SN)	1. People who are important to me would think that I should disclose my information if needed by this platform. 2. People who influence my behavior would think that I should disclose my information if needed by this platform. 3. People who are family to me would think that I should disclose my information if needed by this platform.
Perceived Behavioral Control (PBC)	1. I believe I can control my personal information provided to this platform. 2. I believe I have control over how my personal information is used by this platform. 3. I belleve I have control over who can get access to my personal information collected by this platform.
Information Disclosure Intention (INT)	1. I am likely to provide my personal information on this platform. 2. I am willing to provide my personal information on this platform to access relevant services. 3. It is possible for me to provide personal information on this platform.

Appendix B. Correlation Coefficients and Square Root of AVE for Each Variable

Variables	Fai	Exp	Acc	Tra	PV	PS	RE	SE	PB	PS	PA	SN	PBC	Int
Fai	**0.851**													
Exp	0.636	**0.885**												
Acc	0.654	0.452	**0.872**											
Tra	0.685	0.661	0.591	**0.851**										
PV	−0.588	−0.479	−0.513	−0.513	**0.883**									
PS	−0.515	−0.422	−0.502	−0.492	0.732	**0.905**								
RE	0.489	0.465	0.579	0.542	−0.680	−0.710	**0.907**							
SE	0.632	0.638	0.675	0.621	−0.654	−0.614	0.699	**0.913**						
PB	−0.562	−0.421	−0.599	−0.519	0.717	0.725	−0.720	−0.695	**0.875**					
PS	0.069	0.113	0.104	0.059	0.117	0.014	0.050	0.069	−0.097	**0.875**				
PA	0.201	0.207	0.313	0.157	−0.107	−0.228	0.252	0.257	−0.384	0.553	**0.853**			
SN	0.097	0.156	0.151	0.138	−0.040	−0.125	0.170	0.148	−0.219	0.461	0.517	**0.933**		
PBC	0.149	0.182	0.205	0.166	−0.198	−0.194	0.234	0.262	−0.260	0.074	0.265	0.294	**0.829**	
Int	0.171	0.179	0.255	0.181	−0.098	−0.147	0.230	0.233	−0.329	0.484	0.599	0.503	0.269	**0.883**

Note: The bolded data on the diagonal are the square roots of the AVE values of each variable; the other data represent the correlation coefficients between each variable.

Appendix C. Test Results for Cross-Loadings

Variables	Fai	Exp	Acc	Tra	PV	PS	RE	SE	PB	PS	PA	SN	PBC	Int
Fai1	**0.802**	0.468	0.622	0.534	−0.576	−0.538	0.499	0.585	−0.659	0.044	0.224	0.090	0.110	0.174
Fai2	**0.832**	0.513	0.487	0.547	−0.454	−0.402	0.375	0.497	−0.424	0.052	0.134	0.076	0.115	0.139
Fai3	**0.916**	0.636	0.555	0.663	−0.471	−0.376	0.375	0.531	−0.354	0.079	0.152	0.080	0.153	0.124
Exp1	0.570	**0.774**	0.397	0.464	−0.440	−0.383	0.364	0.454	−0.312	0.037	0.142	0.108	0.117	0.092
Exp2	0.521	**0.920**	0.392	0.610	−0.399	−0.351	0.429	0.595	−0.391	0.124	0.208	0.149	0.183	0.187
Exp3	0.598	**0.952**	0.413	0.669	−0.435	−0.389	0.439	0.635	−0.410	0.132	0.197	0.155	0.178	0.190
Acc1	0.520	0.325	**0.862**	0.423	−0.416	−0.476	0.516	0.629	−0.518	0.117	0.305	0.117	0.132	0.226
Acc2	0.628	0.578	**0.821**	0.678	−0.472	−0.387	0.484	0.569	−0.479	0.077	0.240	0.131	0.215	0.224
Acc3	0.550	0.255	**0.928**	0.421	−0.445	−0.450	0.511	0.564	−0.568	0.078	0.275	0.144	0.182	0.215
Tra1	0.501	0.695	0.442	**0.802**	−0.356	−0.320	0.376	0.533	−0.340	0.065	0.121	0.039	0.162	0.104
Tra2	0.651	0.515	0.594	**0.896**	−0.450	−0.424	0.478	0.550	−0.454	0.062	0.170	0.139	0.163	0.189
Tra3	0.590	0.488	0.462	**0.851**	−0.502	−0.512	0.529	0.500	−0.529	0.022	0.105	0.172	0.098	0.165
PV1	−0.525	−0.425	−0.515	−0.459	**0.890**	0.643	−0.607	−0.620	0.686	0.129	−0.114	−0.013	−0.201	−0.099
PV2	−0.528	−0.401	−0.432	−0.434	**0.892**	0.655	−0.567	−0.553	0.613	0.129	−0.074	0.005	−0.152	−0.052
PV3	−0.504	−0.442	−0.403	−0.465	**0.866**	0.639	−0.627	−0.554	0.593	0.048	−0.094	−0.103	−0.168	−0.107
PS1	−0.455	−0.384	−0.461	−0.455	0.655	**0.911**	−0.645	−0.543	0.666	0.012	−0.248	−0.168	−0.206	−0.145
PS2	−0.461	−0.350	−0.458	−0.416	0.671	**0.909**	−0.623	−0.583	0.675	0.022	−0.207	−0.063	−0.155	−0.120
PS3	−0.482	−0.414	−0.442	−0.465	0.660	**0.894**	−0.659	−0.542	0.625	0.004	−0.162	−0.109	−0.166	−0.134
RE1	0.476	0.455	0.525	0.504	−0.587	−0.636	**0.903**	0.604	−0.601	0.069	0.248	0.168	0.182	0.230
RE2	0.446	0.432	0.509	0.499	−0.619	−0.663	**0.918**	0.604	−0.636	0.036	0.223	0.161	0.223	0.196

Variables	Fai	Exp	Acc	Tra	PV	PS	RE	SE	PB	PS	PA	SN	PBC	Int
RE3	0.411	0.380	0.539	0.473	−0.642	−0.631	**0.897**	0.689	−0.715	0.033	0.215	0.135	0.230	0.202
SE1	0.626	0.617	0.593	0.620	−0.641	−0.589	0.634	**0.871**	−0.594	0.051	0.199	0.138	0.206	0.161
SE2	0.615	0.635	0.635	0.577	−0.592	−0.536	0.587	**0.971**	−0.605	0.068	0.233	0.121	0.217	0.210
SE3	0.492	0.497	0.618	0.503	−0.560	−0.557	0.692	**0.895**	−0.701	0.070	0.270	0.145	0.292	0.266
PB1	−0.523	−0.361	−0.568	−0.427	0.599	0.611	−0.616	−0.625	**0.881**	−0.168	−0.401	−0.185	−0.209	−0.326
PB2	−0.516	−0.390	−0.547	−0.505	0.658	0.660	−0.655	−0.624	**0.912**	−0.028	−0.279	−0.198	−0.221	−0.310
PB3	−0.432	−0.355	−0.452	−0.429	0.626	0.633	−0.620	−0.574	**0.831**	−0.054	−0.326	−0.191	−0.256	−0.223
PS1	0.023	0.121	0.067	0.029	0.115	0.007	0.046	0.044	−0.060	**0.890**	0.470	0.407	0.035	0.404
PS2	0.068	0.107	0.102	0.071	0.081	−0.007	0.056	0.069	−0.113	**0.867**	0.490	0.417	0.105	0.412
PS3	0.088	0.071	0.103	0.053	0.111	0.035	0.030	0.067	−0.079	**0.869**	0.491	0.387	0.055	0.452
PA1	0.131	0.159	0.254	0.116	−0.078	−0.157	0.189	0.205	−0.273	0.443	**0.842**	0.436	0.216	0.481
PA2	0.186	0.192	0.275	0.144	−0.103	−0.201	0.225	0.229	−0.346	0.487	**0.874**	0.453	0.234	0.560
PA3	0.193	0.178	0.272	0.141	−0.092	−0.222	0.229	0.223	−0.358	0.484	**0.843**	0.434	0.228	0.486
SN1	0.104	0.147	0.143	0.158	−0.042	−0.127	0.157	0.149	−0.199	0.420	0.454	**0.933**	0.288	0.458
SN2	0.081	0.143	0.149	0.121	−0.045	−0.117	0.143	0.132	−0.207	0.423	0.500	**0.940**	0.252	0.495
SN3	0.087	0.147	0.128	0.109	−0.026	−0.106	0.178	0.133	−0.206	0.448	0.493	**0.924**	0.285	0.452
PBC1	0.107	0.140	0.170	0.141	−0.192	−0.185	0.219	0.219	−0.229	0.024	0.222	0.284	**0.821**	0.219
PBC2	0.145	0.172	0.194	0.142	−0.164	−0.168	0.206	0.241	−0.243	0.107	0.269	0.291	**0.916**	0.286
PBC3	0.117	0.137	0.140	0.134	−0.137	−0.127	0.153	0.186	−0.165	0.042	0.148	0.126	**0.742**	0.140
Int1	0.185	0.164	0.259	0.193	−0.098	−0.120	0.189	0.230	−0.318	0.433	0.574	0.450	0.249	**0.888**
Int2	0.137	0.144	0.209	0.161	−0.080	−0.140	0.211	0.204	−0.278	0.435	0.497	0.444	0.193	**0.891**
Int3	0.129	0.166	0.206	0.125	−0.079	−0.131	0.211	0.183	−0.273	0.413	0.512	0.437	0.270	**0.870**

Note: The bolded data represent the primary loadings of each variable; the remaining data represent the cross-loadings.

Appendix D. Test Results for Heterotrait–Monotrait Ratio

Variables	Fai	Exp	Acc	Tra	PV	PS	RE	SE	PB	PS	PA	SN	PBC
Exp	0.765												
Acc	0.787	0.524											
Tra	0.844	0.796	0.703										
PV	0.706	0.561	0.597	0.616									
PS	0.609	0.486	0.581	0.581	0.838								
RE	0.578	0.533	0.668	0.640	0.777	0.797							
SE	0.743	0.725	0.776	0.730	0.743	0.687	0.779						
PB	0.680	0.494	0.709	0.627	0.839	0.836	0.827	0.796					
PS	0.085	0.131	0.123	0.070	0.136	0.026	0.059	0.079	0.112				
PA	0.245	0.247	0.379	0.191	0.127	0.266	0.296	0.299	0.460	0.665			
SN	0.112	0.175	0.170	0.159	0.058	0.138	0.189	0.162	0.248	0.521	0.596		
PBC	0.187	0.221	0.248	0.212	0.242	0.232	0.279	0.311	0.318	0.086	0.324	0.334	
Int	0.205	0.206	0.299	0.215	0.113	0.169	0.264	0.264	0.384	0.566	0.713	0.563	0.317

References

1. Dwivedi, Y.K.; Hughes, L.; Ismagilova, E.; Aarts, G.; Coombs, C.; Crick, T.; Williams, M.D. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.* **2021**, *57*, 101994. [CrossRef]
2. Ashok, M.; Madan, R.; Joha, A.; Sivarajah, U. Ethical framework for artificial intelligence and digital technologies. *Int. J. Inf. Manag.* **2022**, *62*, 102433. [CrossRef]
3. Son, J.Y.; Kim, S.S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Q.* **2008**, *32*, 503–529. [CrossRef]
4. Shin, D. The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *Int. J. Hum.-Comput. Stud.* **2021**, *146*, 102551. [CrossRef]
5. Shin, D.; Kee, K.F.; Shin, E.Y. Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms. *Int. J. Inf. Manag.* **2022**, *65*, 102494. [CrossRef]
6. Shin, D.; Park, Y.J. Role of fairness, accountability, and transparency in algorithmic affordance. *Comput. Hum. Behav.* **2019**, *98*, 277–284. [CrossRef]
7. Gran, A.; Booth, P.; Bucher, T. To be or not to be algorithm aware. *Inf. Commun. Soc.* **2021**, *24*, 1779–1796. [CrossRef]
8. Eslami, M.; Rickman, A.; Vaccaro, K.; Aleyasen, A.; Vuong, A.; Karahalios, K.; Hamilton, K.; Sandvig, C. I always assumed that I wasn't really that close to her. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, 18–23 April 2015; pp. 153–162.
9. Zarouali, B.; Boerman, S.C.; de Vreese, C.H. Is this recommended by an algorithm? The development and validation of the algorithmic media content awareness scale (AMCA-scale). *Telemat. Inform.* **2021**, *62*, 101607. [CrossRef]

10. Monzer, C.; Moeller, J.; Helberger, N.; Eskens, S. User perspectives on the news personalization process. *Digit. J.* **2020**, *8*, 1142–1162.
11. Ahmad, F.; Widén, G.; Huvila, I. The impact of workplace information literacy on organizational innovation. *Int. J. Inf. Manag.* **2020**, *51*, 102041. [CrossRef]
12. Siles, I.; Segura-Castillo, A.; Solís, R.; Sancho, M. Folk theories of algorithmic recommendations on Spotify. *Big Data Soc.* **2020**, *7*, 2053951720923377. [CrossRef]
13. Spanaki, K.; Karafili, E.; Despoudi, S. AI applications of data sharing inagriculture 4.0: A framework for role-based data access control. *Int. J. Inf. Manag.* **2021**, *59*, 102350. [CrossRef]
14. Gutierrez, A.; O'Leary, S.; Rana, N.P.; Dwivedi, Y.K.; Calle, T. Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Comput. Hum. Behav.* **2019**, *95*, 295–306. [CrossRef]
15. Hargittai, E.; Gruber, J.; Djukaric, T.; Fuchs, J.; Brombach, L. Black box measures? *Inf. Commun. Soc.* **2020**, *23*, 764–775.
16. Zhang, L.; Yencha, C. Examining perceptions towards hiring algorithms. *Technol. Soc.* **2022**, *68*, 101848. [CrossRef]
17. Swart, J. Experiencing algorithms: How young people understand, feel about, and engage with algorithmic news selection on social media. *Soc. Media+ Soc.* **2021**, *7*, 20563051211008828. [CrossRef]
18. Xu, H.; Luo, X.R.; Carroll, J.M.; Rosson, M.B. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decis. Support Syst.* **2011**, *51*, 42–52. [CrossRef]
19. Liu, B.; Sun, W. Research on Mobile Users' Information Disclosure Decision Process from the Perspective of the Whole CPM Theory. *J. Manag. Sci.* **2021**, *34*, 76–87. (In Chinese)
20. Kim, M.S.; Kim, S. Factors influencing willingness to provide personal information for personalized recommendations. *Comput. Hum. Behav.* **2018**, *88*, 143–152. [CrossRef]
21. Zhang, J.; Liu, J.; Zhong, W. Advertising Accuracy and Effectiveness: A Field Experiment on Privacy Concern. *J. Manag. Sci.* **2019**, *32*, 123–132. (In Chinese)
22. Liu, J.; Sun, G.; Wu, D. Research on the Digital Native Algorithms Perception and Action Mechanism. *Inf. Doc. Serv.* **2023**, *44*, 80–87. (In Chinese)
23. Li, Y. Theories in online information privacy research: A critical review and an integrated framework. *Decis. Support Syst.* **2012**, *54*, 471–481. [CrossRef]
24. Dinev, T.; Hart, P.; Mullen, M.R. Internet privacy concerns and beliefs about government surveillance—An empirical investigation. *J. Strateg. Inf. Syst.* **2008**, *17*, 214–233. [CrossRef]
25. Zhu, H.; Ou, C.X.; van den Heuvel, W.J.A.; Liu, H. Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Inf. Manag.* **2017**, *54*, 427–437. [CrossRef]
26. Jiang, Z.; Heng, C.; Ben, C.F.C. Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Inf. Syst. Res.* **2013**, *24*, 579–595. [CrossRef]
27. Cheng, X.; Hou, T.; Mou, J. Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. *Inf. Manag.* **2021**, *58*, 103450. [CrossRef]
28. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
29. Liu, X.; Chao, L. Analysis of Fairness in Al Governance and Its Evaluation Methods. *Inf. Doc. Serv.* **2022**, *43*, 24–33. (In Chinese)
30. Li, G.; Liang, Y.; Su, J. Breaking the Algorithmic Black-box Governance Dilemma of Digital Platform Companies: Research on the Diffusion of Algorithm Transparency Strategy in China. *J. Inf. Resour. Manag.* **2023**, *13*, 81–94. (In Chinese)
31. Zhou, X. Algorithmic Interpretability: The Normative Research Value of a Technical Concept. *J. Comp. Law* **2023**, *3*, 188–200. (In Chinese)
32. Lepri, B.; Oliver, N.; Letouzé, E.; Pentland, A.; Vinck, P. Fair, transparent, and accountable algorithmic decision-making processes. *Philos. Technol.* **2018**, *31*, 611–627. [CrossRef]
33. An, J. Hierarchy of Algorithmic Transparency. *Chin. J. Law* **2023**, *45*, 52–66. (In Chinese)
34. Wang, Q. The Multiple Dimensions of Algorithmic Transparency and Algorithmic Accountability. *J. Comp. Law* **2020**, *6*, 163–173. (In Chinese)
35. Maddux, J.E.; Rogers, R.W. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol.* **1983**, *19*, 469–479. [CrossRef]
36. Zhang, X.; Liu, S.; Chen, X.; Wang, L.; Gao, B.; Zhu, Q. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Inf. Manag.* **2018**, *55*, 482–493. [CrossRef]
37. Dinev, T.; Hart, P. An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [CrossRef]
38. Smith, H.J.; Dinev, T.; Xu, H. Information privacy research: An interdisciplinary review. *MIS Q.* **2011**, *35*, 989–1015. [CrossRef]
39. Chellappa, R.K.; Sin, R.G. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Inf. Technol. Manag.* **2005**, *6*, 181–202. [CrossRef]
40. Deng, X. Consumers' Ethical Purchasing Intention in Chinese Context: Based on TPB Perspective. *Nankai Bus. Rev.* **2012**, *15*, 22–32. (In Chinese)
41. Zhang, K.; Wang, W.; Li, J.; Xie, Y. Research on Influencing Factors of User Information Disclosure Behavior in Electronic Health Websites. *Libr. Inf. Serv.* **2018**, *62*, 82–91. (In Chinese)
42. Johnston, A.C.; Warkentin, M.; Siponen, M. An enhanced fear appeal rhetorical framework. *MIS Q.* **2015**, *39*, 113–134. [CrossRef]

43. Xu, H.; Teo, H.H.; Tan, B.C.; Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *J. Manag. Inf. Syst.* **2009**, *26*, 135–174. [CrossRef]
44. Kaushik, K.; Jain, N.K.; Singh, A.K. Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electron. Commer. Res. Appl.* **2018**, *32*, 57–68. [CrossRef]
45. Xu, H.; Dinev, T.; Smith, J.; Hart, P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *J. Assoc. Inf. Syst.* **2011**, *12*, 798–824. [CrossRef]
46. Sarstedt, M.; Ringle, C.M.; Hair, J.F. Partial least squares structural equation modeling. *Eur. Bus. Rev.* **2014**, *26*, 106–121.
47. Harman, H.H. *Modern Factor Analysis*; University of Chicago Press: Princeton, NJ, USA, 1976.
48. Kim, H.Y. Statistical notes for clinical researchers: Assessing normal distribution (2) using skewness and kurtosis. *Restor. Dent. Endod.* **2013**, *38*, 52–54. [CrossRef] [PubMed]
49. Kock, N. Common method bias in PLS-SEM: A full collinearity assessment approach. *Int. J. E-Collab.* **2015**, *11*, 1–10. [CrossRef]
50. Hair, J.F.; Ringle, C.M.; Sarstedt, M. PLS-SEM: Indeed a silver bullet. *J. Mark. Theory Pract.* **2011**, *19*, 139–152. [CrossRef]
51. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
52. Kline, R.B. *Principles and Practice of Structural Equation Modeling*; Guilford Publications: New York, NY, USA, 2015; pp. 262–299.
53. Petter, S.; Straub, D.; Rai, A. Specifying formative constructs in information systems research. *MIS Q.* **2007**, *31*, 623–656. [CrossRef]
54. Chin, W.W. The partial least squares approach to structural equation modeling. *Mod. Methods Bus. Res.* **1998**, *295*, 295–336.
55. Geisser, S. The predictive sample reuse method with applications. *J. Am. Stat. Assoc.* **1975**, *70*, 320–328. [CrossRef]
56. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *J. Consum. Psychol.* **2020**, *30*, 736–758. [CrossRef]
57. Min, S. From algorithmic disengagement to algorithmic activism. *Telemat. Inform.* **2019**, *43*, 101251. [CrossRef]