

Article

The Role of Privacy Fatigue in Privacy Paradox: A PSM and Heterogeneity Analysis

Xinluan Tian ^{1,†}, Lina Chen ^{2,†} and Xiaojuan Zhang ^{3,4,*}¹ School of Philosophy and Public Management, Henan University, Kaifeng 475001, China² School of Economics, Peking University, Beijing 100871, China³ School of Information Management, Wuhan University, Wuhan 430072, China⁴ Department of Computer Science, University of Western Ontario, London, ON N6A 3K7, Canada

* Correspondence: xjz@whu.edu.cn or jxzhang0012@gmail.com

† These authors contributed equally to this work.

Abstract: Powerful rising trends of mobile media platforms have also resulted in the escalation of users' privacy concerns. However, there is a paradox between users' attitudes towards privacy and their actual privacy disclosure behaviors. This study attempts to explain the phenomenon of privacy paradox in the mobile social media context from the privacy fatigue perspective. Based on the Elaboration Likelihood Model (ELM) and employing the method of Propensity Score Matching (PSM), this paper confirmed that privacy fatigue could directly explain the privacy paradox. Among the findings, cynicism turned the relationship between privacy concern and privacy protection behaviors from positive influence to negative influence, while emotional exhaustion would weaken the positive influence relationship between privacy concern and the intention to undertake privacy protection behaviors. In addition, the study also revealed the heterogeneous effects of individual characteristics and usage characteristics variables on how the privacy fatigue influences privacy paradox.



Citation: Tian, X.; Chen, L.; Zhang, X. The Role of Privacy Fatigue in Privacy Paradox: A PSM and Heterogeneity Analysis. *Appl. Sci.* **2022**, *12*, 9702. <https://doi.org/10.3390/app12199702>

Academic Editors: Konstantinos Rantos, Konstantinos Demertzis and George Drosatos

Received: 1 September 2022

Accepted: 23 September 2022

Published: 27 September 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: mobile social media; privacy fatigue; privacy paradox; privacy concern; propensity score matching

1. Introduction

As mobile internet technologies develop, social media apps break the barriers of time and space, satisfying user demands for interaction and expression anytime and anywhere. The value of personal data in their circulation and appropriation accumulates ceaselessly. Users are inevitably shadowed by issues of privacy security. An IBM Security research report indicates that 44% of leaking across the world in 2021 involved user privacy data. The average cost of an individual leaking event is as high as USD4.24 million for the companies interviewed. In previous research, privacy concerns reflected the subjective attitude of users towards privacy risks, with most academics considering this concern as encouraging privacy protection behaviors and being the crucial antecedent variable for privacy behavior decisions [1]. However, recent studies discover that users' privacy concerns cannot measure and predict the degree of their intention to adopt privacy protection behaviors [2–5]. This inconsistency between user worries of privacy risks and their decisions concerning privacy protection behaviors is termed the phenomenon of privacy paradox [6,7]. It has become synonymous with this concern–behavior discrepancy [8]. The privacy paradox phenomenon signifies subjective fatigue, and laxness appeared in crucial nodes of the user protecting his/her own privacy security, clearly constituting a negative influence on the secure protection of user privacy information under the social media context. The privacy paradox attracts the research interest of many academics, and explanations on this paradoxical phenomenon have been offered from various research perspectives. However, there is still no consensus [8].

The most recent research on privacy attempted to illustrate the complexity of privacy decisions through privacy fatigue, which is the fatigue caused by the complexity in data disclosure and privacy control [9]. As an example, although repeatedly disclosing data would increase people's worries about privacy, with them suspecting that efficacious decisions and measures cannot be adopted to protect one's privacy, eventually, people fall into abandoning privacy protection behaviors [10]. The privacy fatigue phenomenon of internet users is perceived to be already widely present. An illustration is an American survey on internet users, finding that 32.4% of them did not understand how to protect their privacy online and 13% of users expressed they had already lost interest in the issue of enhancing privacy protection [11]. There are now studies pointing out that, being something new in the developmental stage of mobile media, privacy fatigue may be an important cause affecting the privacy paradox [9]. Thus, the issue of privacy fatigue is not only a new topic in privacy security earnestly awaiting research, but also a strong perspective to explain the user privacy paradox in the new stage of social media.

Though the significance of privacy fatigue has already been noticed, at present, its roles in the privacy paradox and how much it can explain the paradox have still not been clearly delineated in research. To better understand how privacy fatigue acts in user privacy behavior decisions on mobile social media, more studies are needed. Furthermore, since personal privacy is a constituent of "individual personality rights" [12,13], personal characteristics can explain and predict sensitivity towards privacy concerns and privacy fatigue in users [14]. However, previous studies on privacy found it very hard to discern confounding factors' effects on privacy decisions. Their findings are often very vague [15]. At this juncture, prior studies on privacy fatigue are very limited, with even fewer researching personal characteristics as influencing variables. Considering this status quo, an exploration of the effects from user heterogeneity is added in this paper, which would be helpful in supplying a theoretical reference to the adoption of differentiated protection practices for users. Summing up the above, the research questions raised by this research are:

- (1) Is privacy fatigue among users of mobile social media the reason leading to the phenomenon of the privacy paradox?
- (2) Would individual differences among users of mobile social media affect the explanatory strength of privacy fatigue in the privacy paradox phenomenon?

In order to answer the research questions above, this study introduced the Elaboration Likelihood Model (ELM) to construct the research model suitable to the research context. The influence from privacy fatigue on the privacy paradox is considered the central route, with heterogeneous influences of users' individual differences being the peripheral route. In addition, in order to control and eliminate selection bias caused by confounding variables, the paper employed Propensity Score Matching (PSM) as the data analysis method to simulate a scenario of individuals with the same level in their characteristics undergoing experimental intervention, so as to lower confounding bias. This study intends to commence from the angle of privacy fatigue to explore its action mechanism in the process of the privacy paradox, aiming to provide important theoretical references for comprehending privacy behaviors of social media users and be of help in resolving the user privacy issue in the new stage of social media digitization.

The rest of this paper is organized as follows. Section 2 is the literature review, which briefly discusses prior studies concerning the privacy paradox and privacy fatigue. In Section 3, we introduce the paper's theoretical backgrounds and propose the study's research framework and hypotheses based on the theoretical buttresses. The research design as well as the process of data analysis and results are shown in Sections 4 and 5. Finally, Section 6 is the summary of the paper.

2. Literature Review

2.1. Privacy Paradox

In 2006, Barnes first realized the "privacy paradox" phenomenon in behaviors of social media users [16], namely, the discrepancy between users wary of risks of privacy

leaks and disclosing personal information lightly when using social media. Afterwards, a number of academics investigated the causes of this phenomenon from multiple angles. Generally, angles of explanation can be divided into these two: the opinion perspective and behavioral perspective. Researchers from the opinion perspective consider privacy paradox to be caused by a rationality limitation in the users, namely, the users are constrained by influences from internal and external environmental factors, engendering cognitive biases on estimating the risks of privacy disclosure. Several user cognitive biases are exhibited, for example: (1) optimism bias, which is when people's perception of the risk of privacy leakage is based on descriptions of non-personal experiences. Therefore, when making decisions about privacy violation of disclosure risk assessment, people often have an optimistic illusion that they are luckier than others. This bias is present all over the world. As examples, a study in South Korea found that the experience of privacy infringement affects people's level of optimism. Users who have no experience of privacy infringement are more optimistic and more inclined to adopt privacy protection behaviors. Research in Singapore concluded that an individual's prior experience and cognition control significantly affect the degree of his/her optimism bias [17,18]; (2) self-confidence bias, which refers to the degree to which an individual's prior experience and cognition control will significantly impact their optimism bias; this bias is reflected in the user's high confidence in their ability to cope with privacy disclosure or risk of being violated, that is inconsistent with reality. Research data revealed that among those users who have a high assessment of their own privacy protection techniques, less than a quarter of those really know how to prevent privacy risks through technical means [19]; (3) hyperbolic discounting, which refers to the user's perception of long-term and short-term benefits and the influence of time factors in the measurement; that is, the user's perception of benefits will weaken with the lapse of time. Therefore, long-term benefits will be underestimated since they are in the future [20].

The lines of research from the behavior perspective mostly make use of the privacy calculation theory as theoretical support. Based on the "rational person" hypothesis, after balancing risks and benefits as a whole, participants in socio-economic activities would attempt to achieve the greatest gains with the least cost. During the process of privacy calculation, there are diverse benefits that can be sensed, such as obtaining economic benefits or social benefits, displaying individuality or attaining convenience. Benefits are also built up based on demands for social capital, entertainment, social relations and identity construction [3,20–22]. Studies have shown that in making decisions on disclosing privacy information, users would evaluate the respective weights of privacy risks and sensed benefits. When benefits are sensed to be greater than risks, users would choose to disclose privacy information [23]. Nonetheless, the works above mainly focus on opinion and behavior inclinations, ignoring the influence from users' emotional cognition on the privacy paradox. According to the cognitive dissonance theory, psychological pressures will be produced when an individual experiences cognitive dissonance. To lessen the pressures of this uncomfortable psychological state, the individual will look for outlets to reduce the dissonance to arrive at the balanced state of cognitive harmony. Getting down to the issue of user privacy in social media, factors such as escalation of the complexity of privacy measures, frequent incidents of privacy fatigue, as well as overload in sensing information all can produce mismatches between needs for privacy protection in users and their ability to handle privacy. Integrating previous studies for the topic of user privacy in social media, in the face of internet privacy issues becoming more severe daily, users would instinctively adopt this response mechanism centered on emotions. Out of privacy fatigue, they proactively increase the self-adaptation cognitive distance with the privacy issue to lower the feeling of discomfort. This mode of response would elicit quite crucial influences on users' original attitude to privacy and patterns of privacy behaviors. Therefore, this paper strives to attend to how users' privacy fatigue emotions explain the privacy paradox.

2.2. Privacy Fatigue

Fatigue is originally a concept from medicine, denoting a passive emotion [24]. When the matter people have to decide on and deal with exceeds the range of their ability, the passive response of “fatigue” is often engendered. In mobile application environments, obscure and complex system privacy practices and the system’s privacy functionalities frequently have such an effect [25]. To tackle the issue of American users being deficient in privacy protection behaviors, Hargittai and Marwick introduced the privacy fatigue concept in their research [26]. Within the connotations of privacy fatigue, cynicism and emotional exhaustion are considered the most prominent features [9]. Emotional exhaustion reflects the user instinctively adopting this emotion-centered response mechanism to raise the adaptive cognitive distance with the privacy issue; then, the sense of discomfort is reduced through privacy fatigue. Cynicism is defined as attitudes of uncertainty, helplessness and distrust towards online services handling personal information [9]. In earlier studies, academics believed users’ privacy concern to be a multi-dimensional cognition of risks. Being the key measure of decisions towards privacy protection behaviors, the higher the degree of privacy concern, the stronger the user’s sense of risks would be, and thus users become more inclined to adopt privacy protection behaviors [27,28]. However, as the phenomenon of privacy fatigue appeared, academics discovered changes in user behavioral responses. As an example, Furnell and Thomson found that when internet users became tired of the issue of network safety, they would loosen defense behaviors towards security risks [29]. Under other situations, fatigue was also shown in users directly skipping the reading of privacy policies and choosing to accept [9]. Hence, there are also academics proposing that, compared to privacy concern, privacy fatigue is a higher influencing factor in privacy decisions and may even be one of the reasons to explain the discrepancy between user privacy concern and privacy behavior decisions, i.e., the privacy paradox [9].

It is notable that the existing research emphasizes the complexity in terms of the reasons for the privacy paradox and are mainly opinion and behavior oriented, while ignoring the effects of user’s emotional cognition and response to the privacy paradox, although some scholars have proposed some possible explanations of privacy fatigue. As far as we can understand, there has not been research deeply discussing how privacy fatigue specifically acts on the privacy paradox and how the two factors of privacy fatigue, namely cynicism and emotional exhaustion, respectively influence behavioral decisions in the privacy paradox. Given the limitations of existing studies, this paper intends to conduct research from the perspective of privacy fatigue to investigate its impacts on the process of the privacy paradox in the mobile social media context. This study also distinguishes the different effects of cynicism and emotional exhaustion, which would be of help to resolve the user privacy issue in the new stage of social media digitization.

3. Theoretical Background and Hypothesis Development

3.1. Elaboration Likelihood Model Theory

The elaboration likelihood model (ELM) was proposed by Petty and Cacioppo [30], which supplied a dual process theory to understand the effectiveness of persuasion and attitude changes [31]. ELM is based on the two-process model of human cognition in cognitive psychology, namely, human attitudinal changes may be caused by two influencing “routes”—the central route and peripheral route [30]. The central route requires individuals to critically think over opinions on the information related to the issue. On the other hand, the peripheral route usually relies on environmental clues connected to the information, not catering to any grand thinking or cognitive efforts [32,33]. Concretely speaking, the central route refers to the process requiring a high level of cognitive efforts, while the peripheral route indicates the process needing less cognitive efforts and may also be influenced by other factors [34].

ELM has already been employed by many researchers to study factors from central and peripheral routes influencing user attitudes and decisions in information systems. For example, Lee applied ELM to study the influence from the quality and number of

consumer comments on attitudes towards consumer goods [32]. Park (2007) explained how the degree of participation in products (sensing personal relevance of the product) modified influences from central and peripheral clues on consumer purchasing intention [35]. Zhou (2016) demonstrated that self-efficacy significantly softened the influence on initial trust from quality of opinions [36].

Zhu et al. believed that, although privacy decisions in the online environment were dissimilar to those under advertising or sales, the method for handling external information was similar. They expanded the range of the ELM and validated the dual route of the ELM in the mHealth privacy context by combining privacy fatigue and privacy calculus.

We suggest that the process of users' privacy decisions in the social media context follows both a central route and a peripheral route. Specifically, the central route handles evidence related to the information, requiring time and effort to understand and investigate, before arriving at the ultimate judgment and attitudinal response. On the other hand, the peripheral route makes use of sample clues such as source factors and individual heterogeneity characteristics to affect the efficacy of privacy decisions.

3.2. Hypothesis Development

3.2.1. Central Route: Privacy Fatigue and Privacy Paradox

Privacy concern denotes the attitudinal measure of the user towards a series of privacy decision behaviors, such as privacy disclosure and privacy protection. It is the core of privacy research. The positive influence relationship between privacy concern and privacy protection behaviors has been fully documented by academics. For example, Xu et al. discovered that when users of mobile social media believed personal information had been accessed by unknown means or used inappropriately, they would tend to choose to give up using social media [23]. Academics such as Bansal et al. also similarly confirmed that privacy concern would lower users' privacy disclosure intention [27]. Mamonov et al. noted that privacy concerns would influence users' goods purchasing behaviors in the social business environment [37]. Research by Feng et al. found that the privacy concerns of young and teenage users of social media led to a significant positive influence on their practice of privacy protection behaviors [38]. These studies demonstrated that privacy concern could clearly affect users' information security behavior intention. Stronger privacy concern usually implies fewer privacy disclosures and a greater willingness towards privacy protection behaviors. The positive influence between privacy concern and privacy protection behaviors is one of the prerequisite assumptions of the privacy paradox being valid. Our hypothesis is thus:

H1. *There is a positive influence relationship between privacy concern and the intention towards privacy protection behaviors.*

"Privacy fatigue" is exhibited in people cutting their efforts or even directly abandoning the goal when the pressure they are facing is too big [39]. In response to privacy threats, the user reduced corresponding behaviors, resulting in slackening of daily security actions [9]. Individuals experiencing privacy fatigue often hope to reduce their efforts regarding privacy decisions as much as possible, rather than look for solutions to the issue. They may withdraw from actively tackling privacy threats [25]. Through interviews, the research by Hargittai and Marwick concluded that the mental distancing of users from the privacy issue or an attitude of cynicism was the important reason leading to decoupling of privacy concern and privacy protection behaviors [26]. Previous research suggested that in such scenarios as social media and e-commerce, users' great investment of time, money and cognitive efforts and deep involvement with social links with other users leads to a high sunk cost. In these scenarios, privacy fatigue, functioning as a coping mechanism, encourages disclosure behaviors [34]. Hence, our hypotheses are as below:

H2a. *Cynicism would weaken the positive influence relationship between privacy concern and privacy protection behaviors.*

H2b. *Emotional exhaustion would weaken the positive influence relationship between privacy concern and privacy protection behaviors.*

3.2.2. Peripheral Route: Heterogeneous Influences on Privacy Paradox

Individual traits are the internal specifics towards personality stability, having a durable and fundamental influence on individuals' psychology and behaviors. Although prior literature has not yet deeply probed the influencing factors of privacy fatigue, at present, there are already multiple authors describing the influence of user personality characteristics on social media tiredness. For example, Lee's study showed young women users experiencing higher tiredness [40]. Adhikari et al. believed group differences such as gender and age would play important roles in social network fatigue [41]. Thus, this paper posits that individuality traits would engender heterogeneous effects on privacy fatigue's explanatory strength on the privacy paradox. In addition, usage characteristics are also important heterogeneous factors affecting users' privacy behaviors. Study examples include Ravindran et al. holding that users' personal immersion tendency is one of the main factors leading to social media fatigue [42] and Kim et al. finding experience factors such as interaction among good friends as also having significant effects on tiredness [43]. In lieu of these, this paper presumes that usage characteristics such as the number of friends on WeChat and usage duration would produce heterogeneous effects on how privacy fatigue explains the privacy paradox.

H3a. *Individual characteristics (gender, age, level of education) have heterogeneous effects on privacy fatigue's explanatory strength on privacy paradox.*

H3b. *Usage characteristics (number of friends on WeChat, usage duration) have heterogeneous effects on privacy fatigue's explanatory strength on privacy paradox.*

As a whole, the research model of this paper is presented in Figure 1.

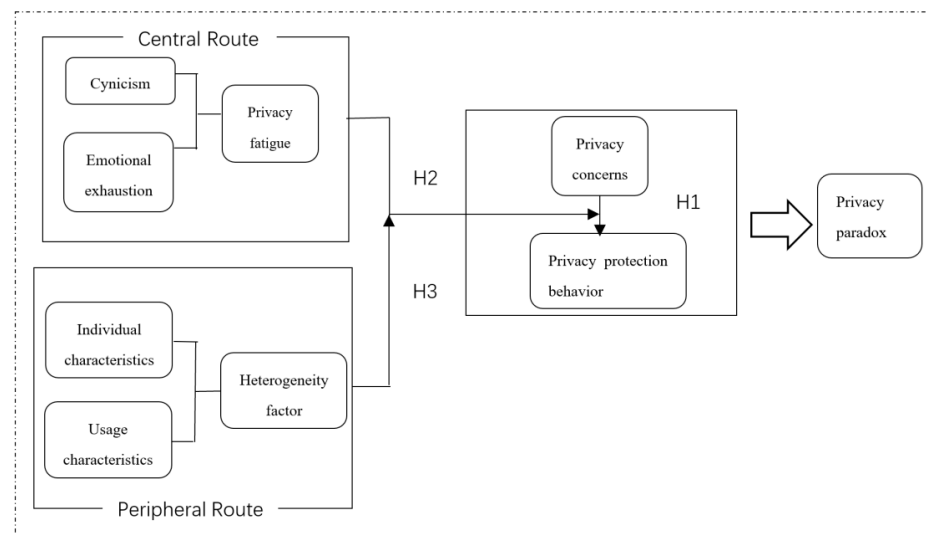


Figure 1. The research model.

4. Methodology and Data Collection

4.1. Designing the Research Method

To study the effects of privacy fatigue on the privacy paradox, the following issue has to be considered. That is, if conventional empirical research methods were employed, owing to the presence of confounding variables, it would be quite difficult to observe the net effects between the independent variable and the dependent variable. Specifically, since initial conditions are not identical within the samples, selection bias is present, and the influence from privacy fatigue on the privacy paradox may be “over-estimated” or “under-estimated”.

In order to control and eliminate selection errors caused by confounding variables, this study employs propensity score matching (PSM) to study the influencing relationships by privacy fatigue on the privacy paradox, namely matching individuals with variation in core variables and similar levels in other characteristics so as to simulate the scenario of individuals with the same characteristic levels randomly receiving experimental intervention, thus effectively lowering confounding bias.

Specifically, the basic thinking is to make the non-random data close to random through constructing a counterfactual framework. By dividing users into a control group and experience group by the degree of privacy fatigue, then calculating the propensity score according to demographic variables as well as using characteristic variables, followed by matching individuals in both groups with close propensity scores, endogenous issues due to individual characteristic variables can be effectively resolved. The paper considers the sample with a high level of privacy fatigue as the experience group, otherwise, the control group. Processing variable $D_i = \{0, 1\}$ indicates whether the individual is in a state of privacy fatigue. With privacy fatigue, a value of 1 will be given, without the fatigue a value of 0. $protect_{1i}$ and $protect_{0i}$ respectively denote the intention for privacy protection behaviors in individuals under privacy fatigue or not. The average treatment effect on the treated (ATT) on privacy fatigue is defined as:

$$ATT = E(protect_{1i} - protect_{0i} | D_i = 1) = E(protect_{1i} | D_i = 1) - E(protect_{0i} | D_i = 1) \quad (1)$$

In Equation (1), $E(protect_{0i} | D_i = 1)$ is the non-observable outcome, since, in reality, we can only observe the intention for privacy protection behavior of an individual under one specific state. By employing PSM, for the privacy fatigue group, a close sample from the non-privacy fatigue group can be matched. The substitute value for $E(protect_{0i} | D_i = 1)$ can thus be constructed. Equation (1) can be changed to:

$$ATT = E\{E(protect_{1i} - protect_{0i} | D_i = 1, p(X_i))\} \\ = E\{E(protect_{1i} | D_i = 1, p(X_i)) - E(protect_{0i} | D_i = 0, p(X_i)) | D_i = 1\} \quad (2)$$

In Equation (2), $p(X_i)$ represents the propensity score, indicating the conditional probability of privacy fatigue of individuals with characteristic variables fixed. It is calculated as:

$$p(X_i) = \frac{\exp(\beta X_i)}{1 + \exp(\beta X_i)} \quad (3)$$

Upon the basis of propensity score calculation, selecting an appropriate matching method would enable conditional probabilities of the control group and the experience group to be as close to each other as possible. Selection bias can be eliminated via controlling observable characteristics. After matching, the main focus of this paper is the direction of action of privacy concern on intention for privacy protection behaviors, whether the individual is under a state of privacy fatigue or not. Regression analysis is conducted on this basis. The regression formula is:

$$protect_i = \beta_1 + \beta_2 pc_i + \beta_3 pc_i \times D_i + \beta X_i + \varepsilon_i \quad (4)$$

In Equation (4), i represents the interviewee, pc_i stands for user privacy concern, $pc_i \times D_i$ represents the interactive item of user privacy concern and privacy fatigue, X_i is the control variables and ε_i is the random error. Coefficient β_3 in interaction term $pc_i \times D_i$ indicates the influence relationship from privacy concern to intention of privacy protection behavior under a state of privacy fatigue. $\beta_2 + \beta_3$ represents that the influence relationship between privacy fatigue and privacy paradox can be directly observed, not merely the correlation between the two.

4.2. Defining Variables

4.2.1. Core Variables

This chapter designs the questionnaire according to the privacy fatigue concept proposed by Choi, dividing privacy fatigue into the two measurement indicators of cynicism and emotional exhaustion [9]. From the definition of privacy paradox, the variables involved are privacy concern and intention for privacy protection behavior. The former refers to user worries on the possible consequences or losses when disclosed personal information is transmitted or appropriated [1], while the intention for privacy protection behavior denotes the behavioral intention of the user to adopt secure protection measures for privacy [38]. On the basis of studies by Xu [23], Chen [28], etc. and combining them with the status quo of Chinese mobile social media, this chapter constructed the measurement indicator system between privacy concern and intention of privacy protection behavior. Specifics of items asked for the indicators can be seen in Table 1.

Table 1. Measurement indicator system of core variables.

Variables		Items asked
Privacy fatigue	Cynicism	1. I am starting to hold a skeptical attitude towards the importance of the privacy issue on social networks.
		2. I believe measures I have adopted to protect privacy (such as masking identity information, setting visible zone for friends' circle) have no big effect on preventing my privacy from being threatened.
		3. If someone wants to invade my privacy on social media, relying on my own to defend it is far from enough.
	Emotional exhaustion	1. I loathe taking privacy protection measures (such as signing privacy agreements, setting visible zone for friends' circle) in the social network environment.
		2. Privacy leaks occur frequently, so I would not take further measures.
		3. Information on privacy in social media is too complicated, exceeding what I can handle.
Privacy paradox	Privacy concern	1. When WeChat asks for my personal information, I would think it over carefully.
		2. I worry that WeChat would sell my personal information to other companies for other uses.
		3. I worry that other people can discover my personal information on WeChat (friends' circle).
	Intention for privacy protection behavior	1. When WeChat requires me to register, I supply false personal information.
		2. I don't provide my information (such as day of birth, photo, location, etc.) which can identify me on WeChat, as much as possible.
		3. When WeChat suggests saving my log-in and password for later use, I would reject.

4.2.2. Control Variables

According to hypotheses in this paper, individual characteristics (gender, age, level of education) and usage characteristics (number of friends on WeChat, usage duration) engender heterogeneous effects on privacy fatigue's explanatory contribution to the privacy paradox. In order to avoid endogenous influences from these factors, the paper sets interviewees' gender, age and level of education as well as usage characteristics which include length of time using WeChat every day and number of friends on WeChat as control variables. Specific values given can be seen in Table 2.

Table 2. Measurement indicator system for variables of individuals and usage characteristics.

Variables' Dimensions		Choices and Values
Individual characteristics	Gender	"Male" = 1 "Female" = 2
	Age	"Under 20" = 1 "20–30" = 2 "30–40" = 3 "40–50" = 4 "Over 50" = 5
	Level of education	"High school and under" = 1 "Undergraduate and tertiary" = 2 "Master's student" = 3 "Doctor's student" = 4
Usage characteristics	No. of friends on WeChat	"Under 100" = 1 "100–300" = 2 "300–600" = 3 "600–1000" = 4 "Over 1000" = 5
	Usage duration	"Under one hour per day" = 1 "1–3 h daily" = 2 "3–5 h daily" = 3 "5–8 h daily" = 4 "Over 8 h per day" = 5

4.3. Source of Data and Sample Selection

This research selects users of the Chinese social media platform with the biggest number of daily active users, namely WeChat, as samples for data collection. WeChat currently has 1.299 billion monthly active users, which makes it the mobile social media platform with the highest monthly active users and the most widely used mobile social media platform in China. As a matter of fact, WeChat has penetrated into people's daily life and has broad implications for the development of civil society [44,45]. Data collection is conducted through the largest Chinese online questionnaire platform at present (<https://www.wjx.cn>, accessed on 19 September 2021). Items in the questionnaire consist of two sections. Items about users' demographic characteristics and social media usage characteristics make up the first section, with those on variables related to privacy fatigue the second. A total of 1734 valid samples are obtained for this study. Descriptive statistics of the survey sample are shown in Table 3.

Table 3. Descriptive statistics of the sample.

Characteristic Variables	Variables	Choices	Number	Percentage (%)
Demographic characteristics	Gender	Male	439	25.3
		Female	1295	74.7
	Age	Under 20	214	12.3
		20–30	406	23.4
		30–40	802	46.3
		40–50	265	15.3
		Over 50	47	2.7
	Level of education	High school and under	961	55.4
		Undergraduate and tertiary	631	36.4
		Master's student	99	5.7
		Doctor's student	43	2.5

Table 3. Cont.

Characteristic Variables	Variables	Choices	Number	Percentage (%)
Mobile social media usage characteristics	Intensity of WeChat usage	Under one hour per day	193	11.1
		1–3 h daily	556	32.1
		3–5 h daily	549	31.6
		5–8 h daily	218	12.6
		Over 8 h per day	218	12.6
	Number of friends on WeChat	Under 100	651	37.5
		100–300	675	38.9
		300–600	258	14.9
		600–1000	81	4.7
		Over 1000	69	4.0

5. Empirical Analysis

5.1. Estimation of Propensity Score

The key to propensity score matching (PSM) lies in finding individuals with the same propensity score and matching them. This chapter employs the logit regression model, the most widely used, to conduct dimensionality reduction on demographic variables and usage characteristics variables. Results of the logit regression are shown in Table 4. From Table 4, we can learn that location, gender, age, level of education and number of friends on WeChat all can have significant influence on the possibility of privacy fatigue. Although the intensity of WeChat usage is statistically not significant, prior studies have indicated personal immersion tendency of social media users to be one of the important factors causing social media fatigue [42]. Hence, there is reliability in this paper selecting these six characteristic variables to estimate propensity scores.

Table 4. Results of the logit regression model.

Variable	Coef.	Std. Err.	Z
pro	0.049 **	0.023	2.13
sex	−0.246 *	0.138	−1.78
age	−0.271 ***	0.064	−4.24
edu	0.179 *	0.093	1.93
freq	−0.014	0.056	−0.26
friends	−0.172 **	0.073	−2.35
_cons	−1.038 **	0.520	−1.99

Notes: *, ** and *** respectively denote significance on the 10%, 5% and 1% levels.

5.2. Assessing the Matching Quality

Ideal matching results can simultaneously satisfy the common support assumption and balancing assumption. The former requires distribution of propensity scores of individuals in the experience group and the control group to be as close as possible after matching. The latter demands no significant difference in observable variables in both groups after the matching. According to the nearest-neighbor matching within caliper (caliper $\varepsilon = 0.01, k = 5$), Figure 2a,b, respectively, represent the kernel density function figures of “privacy fatigue (experience group)” and “non-privacy fatigue (control group)” before and after matching. From Figure 2, it can be seen that there are clear differences in the probability distribution of propensity scores in both the experience and the control groups before matching, and, indeed, the zone of overlap is quite small. After matching, the distributions of propensity scores of samples in both groups are very close, better satisfying the common support conditions. Learning from the method in Rubin (2001) [46] the balance test is conducted. The results are shown in Table 5. The standardized bias (%bias) of most variables is in reasonable ranges after matching. Furthermore, t test results of all variables do not reject the original hypothesis of no systematic differences between the

experience group and control group. Figure 3 intuitively shows the common value range of propensity scores. The observed values of the control group are all within the common value range, while only four observations of the experience group do not fall in the range. Therefore, just a small number of samples will be lost during propensity score matching. Summing up the points above, matching significantly lowered differences in observations between the two groups, which can be seen as this paper having appropriately selected observable variables and that the matching method is suitable.

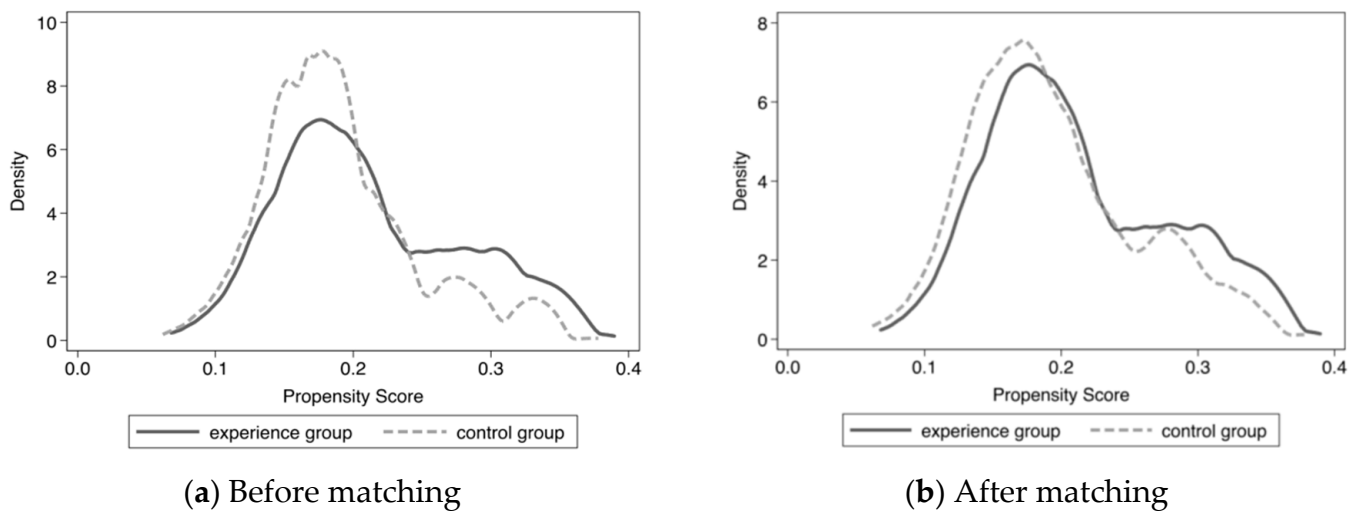


Figure 2. Comparison of kernel density function before and after matching.

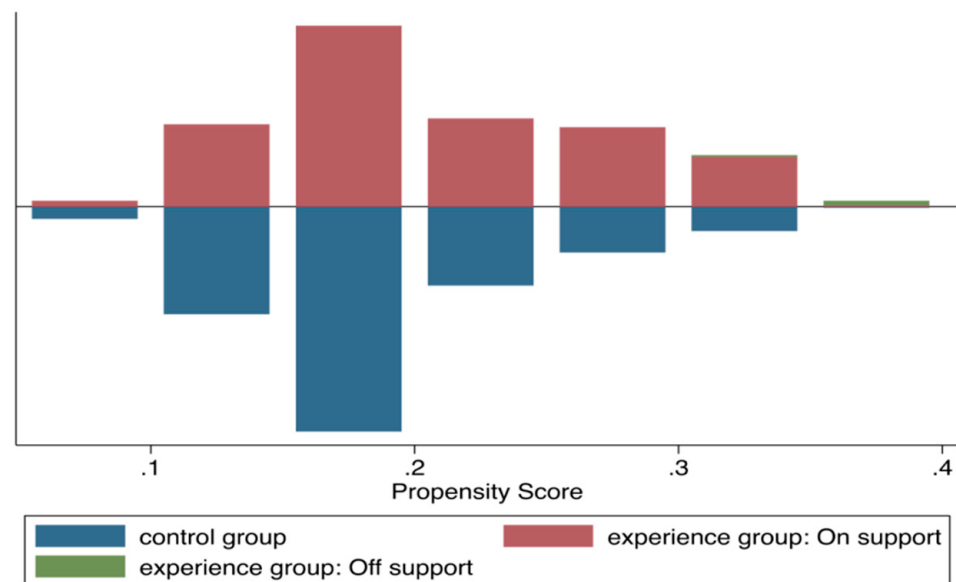


Figure 3. Check common support.

5.3. Analysis of Empirical Results

Conducting regression analysis from Equation (4), the influence relationship from privacy fatigue on the privacy paradox is investigated. The results are shown in Table 6. Regression results in list (1) indicate that every unit increase in individual privacy concern would raise 0.066 units of intention for privacy protection behavior. In contrast, when the individual is under a state of privacy fatigue (cynicism), the relationship between privacy concern and intention for privacy protection behavior is altered. Every unit increase in privacy concern instead lowers the intention for privacy protection behavior by 0.110 units.

As a whole, for individuals under privacy fatigue, each unit increase in privacy concern lessens the intention for privacy protection behavior by 0.044 units. Our hypothesis 1 is valid, namely, cynicism would dissolve the positive influence relationship between privacy concern and intention for privacy protection behavior. Lists (2) and (3) reflect that, after changing the proxy variables of privacy concern, the above conclusion still holds.

Table 5. Results of the balance test.

Variable	Sample	Mean		%Bias	%Reduct Bias	t
		Experience Group	Control Group			
pro	Unmatched	17.438	17.083	11.9	98.7	1.89 *
	Matched	17.380	17.375	0.2		0.02
sex	Unmatched	1.694	1.760	−14.9	50.9	−2.51 **
	Matched	1.696	1.728	−7.3		−0.92
age	Unmatched	2.515	2.777	−26.5	97.4	−4.53 ***
	Matched	2.521	2.514	0.7		0.08
edu	Unmatched	1.566	1.549	2.1	−368.4	0.37
	Matched	1.539	1.464	10		1.32
freq	Unmatched	2.753	2.853	−8.4	27.2	−1.41
	Matched	2.753	2.680	6.1		0.76
friends	Unmatched	1.857	2.017	−15.3	31.5	−2.55 **
	Matched	1.855	1.746	10.5		1.39

Notes: *, ** and *** respectively denote significance on the 10%, 5% and 1% levels.

Table 6. The results of regression.

Variable	(1)	(2)	(3)
pc1	0.066 *** (−0.021)		
pc1 × D	−0.110 *** (−0.017)		
pro	−0.001 (−0.009)	−0.001 (−0.009)	−0.001 (−0.009)
sex	−0.094 (−0.064)	−0.097 (−0.064)	−0.103 (−0.064)
age	0.015 (−0.028)	0.012 (−0.028)	0.014 (−0.027)
edu	0.057 (−0.041)	0.037 (−0.041)	0.049 (−0.041)
freq	−0.041 * (−0.024)	−0.040 * (−0.024)	−0.041 * (−0.024)
friends	−0.018 (−0.029)	−0.020 (−0.029)	−0.020 (−0.029)
pc2		0.099 *** (−0.021)	
pc2 × D		−0.108 *** (−0.018)	
pc3			0.102 *** (−0.023)
pc3 × D			−0.117 *** (−0.017)
Constant	2.364 *** (−0.231)	2.294 *** (−0.230)	2.273 *** (−0.232)
Observations	905	905	905
R-squared	0.058	0.065	0.070

Notes: *, *** respectively denote significance on the 10%, 1% levels, and standard error is in parentheses.

The empirical results of hypothesis 2 are shown in Table 7. The regression results in list (1) indicate that every unit increase in individual privacy concern would raise the intention for privacy protection behavior by 0.091 units. However, for individuals under a state of privacy fatigue (emotional exhaustion), the relationship between privacy concern and intention for privacy protection behavior also shifted. Each additional unit of privacy concern lowers individual intention for privacy protection behavior by 0.079 units. Hypothesis 2 is valid, namely, emotional exhaustion would weaken the positive influence relationship between privacy concern and intention for privacy protection behavior. However, unlike cynicism, emotional exhaustion can only weaken the positive influence relationship between privacy concern and intention for privacy protection behavior, but is not able to reverse the relationship between the two. Similarly, with proxy variables in lists (2) and (3) changed, the above conclusion still holds.

Table 7. The results of regression.

Variable	(1)	(2)	(3)
pc1	0.091 *** (−0.019)		
pc1 × D	−0.079 *** (−0.013)		
pro	−0.104 * (−0.055)	−0.098 * (−0.055)	−0.107 * (−0.055)
sex	0.014 (−0.025)	0.008 (−0.025)	0.011 (−0.025)
age	0.012 (−0.036)	−0.003 (−0.037)	0.009 (−0.036)
edu	−0.020 (−0.021)	−0.023 (−0.021)	−0.022 (−0.021)
freq	−0.021 (−0.025)	−0.023 (−0.025)	−0.022 (−0.025)
friends	0.002 (−0.007)	0.003 (−0.007)	0.002 (−0.007)
pc2		0.113 *** (−0.019)	
pc2 × D		−0.077 *** (−0.014)	
pc3			0.112 *** (−0.021)
pc3 × D			−0.074 *** (−0.014)
Constant	2.327 *** (−0.197)	2.267 *** (−0.196)	2.263 *** (−0.199)
Observations	1181	1181	1181
R-squared	0.042	0.048	0.043

Notes: *, *** respectively denote significance on the 10%, 1% levels, and standard error is in parentheses.

5.4. Robustness Test

In order to ensure robustness of the results, this paper tested, respectively, with nearest neighbor matching with return (1:1), kernel matching, replacing core variables, as well as changing matching methods on the basis of replacing core variables. The regressions indicate that results from these four methods all support the above conclusions, demonstrating robustness in the empirical results. Table 8 displays results of the robustness test.

Table 8. The result of robustness test.

Variable	(1)	(2)	(3)	(4)
pc1	0.064 *** (−0.018)	0.058 *** (−0.016)	0.081 *** (−0.020)	0.067 *** (−0.021)
pc1 × D	−0.141 *** (−0.017)	−0.128 *** (−0.015)	−0.092 *** (−0.014)	−0.081 *** (−0.029)
pro	−0.004 (−0.013)	0.005 (−0.007)	0.008 (−0.008)	0.004 (−0.023)
sex	−0.041 (−0.062)	−0.092 * (−0.049)	−0.122 ** (−0.057)	−0.072 (−0.068)
age	0.010 (−0.027)	0.017 (−0.022)	−0.004 (−0.026)	0.026 (−0.031)
edu	0.018 (−0.045)	0.012 (−0.033)	0.017 (−0.038)	−0.057 (−0.061)
freq	−0.026 (−0.024)	−0.026 (−0.019)	−0.017 (−0.022)	−0.021 (−0.027)
friends	0.014 (−0.032)	−0.002 (−0.023)	−0.025 (−0.026)	0.025 (−0.040)
Constant	2.377 *** (−0.272)	2.307 *** (−0.175)	2.335 *** (−0.202)	2.256 *** (−0.447)
Observations	1249	1734	1123	1077
R-squared	0.060	0.047	0.050	0.022

Notes: *, ** and *** respectively denote significance on the 10%, 5% and 1% levels, and standard error is in parentheses.

5.5. Heterogeneity Analysis

From results of Table 9, it can be seen that, for men, the explanatory strength of privacy fatigue on the privacy paradox is even stronger. Compared to the situations of females, the negative relationship between privacy concern and intention for privacy protection behavior is more prominent for men under conditions of privacy fatigue. There is a stronger positive relationship between privacy concern and intention for privacy protection behavior for individuals under 30. However, the weakening of this positive relationship from privacy fatigue is also bigger. Compared to individuals with higher levels of education, the explanatory strength of privacy fatigue on the privacy paradox is greater for those of lower education levels.

From the results in Table 10, it can be seen that, without considering privacy fatigue, respondents who have used WeChat for a short period of time pay more attention to the protection of personal information, and, for them, the positive force between privacy concerns and privacy protection behavior willingness is obviously stronger than the respondents who have used WeChat for a long time, and privacy fatigue has no significant difference in the degree of dissolving the positive relationship between privacy concern and privacy protection behavior. Therefore, we would conclude that for the respondents who have used WeChat for a long time, the explanation of the effect of privacy fatigue on the privacy paradox is stronger, and for the respondents who have few WeChat friends, the explanation of the effect of privacy fatigue on the privacy paradox is stronger compared to respondents with more WeChat friends.

Table 9. The heterogeneity analysis of individual characteristics.

Variable	Sex		Age		Level of Education	
	Male	Female	Under 30	Over 30	Lower Education Levels	Higher Education Levels
pc1	0.074 *	0.063 ***	0.085 **	0.060 ***	0.081 ***	0.034
	(−0.041)	(−0.021)	(−0.037)	(−0.021)	(−0.023)	(−0.032)
pc1 × cy	−0.181 ***	−0.132 ***	−0.179 ***	−0.122 ***	−0.204 ***	−0.066 ***
	(−0.041)	(−0.019)	(−0.030)	(−0.021)	(−0.023)	(−0.025)
age	−0.010	0.019	−0.050	−0.024	−0.049	−0.018
	(−0.051)	(−0.033)	(−0.108)	(−0.076)	(−0.070)	(−0.135)
edu	0.034	0.014	0.143 *	−0.048	0.014	−0.003
	(−0.110)	(−0.049)	(−0.075)	(−0.059)	(−0.033)	(−0.051)
freq	0.026	−0.038	−0.085 *	0.002	−0.037	−0.014
	(−0.061)	(−0.025)	(−0.044)	(−0.028)	(−0.029)	(−0.041)
friends	0.035	0.007	−0.019	0.025	0.046	−0.016
	(−0.086)	(−0.035)	(−0.066)	(−0.036)	(−0.043)	(−0.048)
pro	0.014	−0.010	0.009	−0.027	−0.009	0.000
	(−0.026)	(−0.015)	(−0.016)	(−0.024)	(−0.030)	(−0.015)
Constant	1.891 ***	2.427 ***	2.160 ***	2.785 ***	2.455 ***	2.393 ***
	(−0.544)	(−0.314)	(−0.365)	(−0.467)	(−0.563)	(−0.414)
Observations	284	965	370	879	797	452
R-squared	0.075	0.059	0.112	0.045	0.103	0.018

Notes: *, ** and *** respectively denote significance on the 10%, 5% and 1% levels, and standard error is in parentheses.

Table 10. The heterogeneity analysis of usage characteristics.

Variable	Intensity of WeChat Usage		Number of Friends on WeChat	
	Under 3 h Daily	Over 3 h Daily	Under 100	Over 100
pc1	0.105 ***	0.041	0.066 **	0.061 **
	(−0.027)	(−0.026)	(−0.028)	(−0.025)
pc1 × cy	−0.155 ***	−0.126 ***	−0.158 ***	−0.125 ***
	(−0.024)	(−0.024)	(−0.026)	(−0.023)
age	0.004	−0.137	−0.028	−0.057
	(−0.080)	(−0.095)	(−0.084)	(−0.092)
edu	−0.049	0.094 **	0.021	−0.005
	(−0.034)	(−0.045)	(−0.036)	(−0.045)
freq	−0.037	0.045	−0.027	0.004
	(−0.075)	(−0.057)	(−0.102)	(−0.050)
friends	0.034	−0.019	−0.043	−0.024
	(−0.060)	(−0.038)	(−0.036)	(−0.030)
pro	0.020	−0.010	0.041	−0.005
	(−0.029)	(−0.015)	(−0.049)	(−0.014)
Constant	1.845 ***	2.459 ***	1.598 *	2.529 ***
	(−0.558)	(−0.338)	(−0.895)	(−0.327)
Observations	581	668	555	694
R-squared	0.089	0.052	0.077	0.049

Notes: *, ** and *** respectively denote significance on the 10%, 5% and 1% levels, and standard error is in parentheses.

6. Conclusion and Insights

6.1. Main Findings

The study has yielded various interesting findings. First and foremost, before the effects of privacy fatigue arose, it is valid to claim that a positive influence is engendered by privacy concerns as to the intention for privacy protection behavior. This is consistent with prior studies in academia [27,37]. Privacy concerns are the core factor highlighting user adoption of privacy protection behaviors on social media. At the same time, they further

illustrated the presence of the emerging prerequisite for privacy paradox under the social media context.

Second, for this set of relationship between privacy concerns and intention for privacy protection behavior, owing to the emergence of privacy fatigue, wholesale changes have erupted. Among these, cynicism turns the positive influence between privacy concern and intention for privacy protection behavior into negative influence, while emotional exhaustion would attenuate the positive influence relationship between the two. This discovery echoed the conclusion proffered by academics that the influence from privacy fatigue exceeded privacy concerns [9]. It further confirmed that privacy fatigue could become an explanation for privacy paradox.

Third, personal traits and usage characteristics lead to dissimilar heterogeneous contributions in privacy fatigue's explanation on privacy paradox. For users who are male, lower levels of education and younger age are personal traits with greater explanatory strength of individuals' privacy fatigue concerning the privacy paradox. Regarding usage characteristics, the explanatory power is stronger for interviewees with a longer WeChat using duration and having fewer WeChat friends. Commencing from personality characteristics, previous studies have confirmed them as possessing significant influence on engendering privacy fatigue [25]. This study further added that heterogeneous factors would also play important roles in the influence relationships between privacy fatigue and privacy paradox.

6.2. Theoretical Significance

This study possesses a certain theoretical significance in the following aspects. First, as user privacy data incidents under the mobile social media context frequently erupted and the difficulty for users in adopting protective measures increased, privacy fatigue characterized by negative emotions such as cynicism and emotional exhaustion has gradually become the new feature of user privacy behavior in the digital age. This may furnish new routes of thought for explaining user privacy behaviors on the new stage of the digital scene. Unfortunately, existing studies largely congregate around opinion orientation and behavior orientation, rarely investigating the explanatory effect on the appearance of privacy paradox from users' emotional cognition, namely, privacy fatigue. To fill in this blank in the research, this paper empirically investigated the influence relationship from privacy fatigue in the emergence of the privacy paradox.

Next, prior studies did not significantly consider the issue of selection bias. Individual characteristic variables and usage characteristic variables produce heterogeneous influences on the explanatory role of privacy fatigue. Therefore, by employing the PSM research method and through constructing a counterfactual framework, this paper enabled non-random data to approach randomness, effectively solving endogenous issues brought on by individual characteristic variables, simultaneously further interpreting the influence from a heterogeneity perspective.

Finally, we introduced the theory model, ELM, to construct an explanatory model on the user privacy paradox from central and peripheral routes under a mobile social media context. By applying ELM in the privacy context of mobile social media, we also verified its applicability and persuasiveness. In previous studies, ELM has been applied to online marketing [47], user adoption behaviors [48], as well as other contexts including adoption of online patient follow-up service [49] and the privacy paradox in mHealth applications [34]. However, our research has expanded ELM's reach to the explanation of privacy paradox in the mobile social media context.

6.3. Practical Implications

The present study might also provide some references and guidance for management practices. Progress in digital technology has enabled social media providers to better utilize user data to initiate value adding services. However, if privacy fatigue lingers for a long time, the commercial value of personal data would drop, because privacy fatigue could turn what used to be important into something insignificant [9]. Through reducing the

non-transparency in user privacy protection policies while strengthening technological gatekeeping in user privacy security, service providers can thus reduce the level of privacy fatigue in users.

Next, personal characteristic variables and use ledgers have heterogeneous effects on the influence process from privacy fatigue to privacy paradox. Service providers should be aware of studying and providing differentiated schemes to different users in accordance with the daily usage situation of apps and consider providing broader authorizations in setting service functionalities.

Finally, providers of mobile social media services should be more attentive to users' emotional and cognitive reactions. They need to avoid igniting prevention foci by establishing more secure and reliable personal information protection mechanisms, such as regulating privacy information collection and usage authorization, enhancing anonymity and forbidding collecting and utilizing user information excessively, so as to reduce the anxiety linked to intrusion of privacy.

6.4. Limitations and Further Studies

Limitations of the current study should be noted. First, in the sampling, we have only selected WeChat users. Although WeChat is the social media software with the highest daily activity load in China, as modes of social media software are also continually developing, some open social software, mainly in real time video broadcast, have clear distinctions with private sphere social media represented by WeChat. In this research attempt, we have not conducted distinguishing studies on users' privacy security behaviors under various platforms. Hence, dissimilarities between new modes of mobile social media users and those of traditional mobile social media under the privacy fatigue phenomenon can formulate the coming research directions. Next, to ensure a broad survey zone and quantifiable data, this study made use of a questionnaire. However, owing to possible differences between filling in the questionnaire and emotional reactions in actual situations, checks can be made in future research on this study through in-depth interviews, repeated surveys, etc. In addition, the study sample and linguistic context of this research are largely from China. The survey results could thus be influenced by cultural characteristics to a certain extent.

In future research, on the one hand, checks can be made on this topic through in-depth interviews, repeated surveys, etc. On the other hand, distinguishing studies on user's privacy security behaviors under various platforms can be conducted, and cross-cultural sample data can also be collected for research in the context of different cultures.

Author Contributions: Conceptualization, X.T. and X.Z.; methodology, X.T. and L.C.; software, L.C.; validation, L.C.; formal analysis, L.C. and X.T.; investigation, X.T.; resources, X.Z. and X.T.; data curation, L.C. and X.T.; writing—original draft preparation, X.T. and L.C.; writing—review and editing, X.Z., X.T. and L.C.; visualization, X.T.; supervision, X.Z.; project administration, X.Z.; funding acquisition, X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of China, grant number 71473182.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Awad, N.F.; Krishnan, M.S. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Mis Q.* **2006**, *30*, 13–28. [\[CrossRef\]](#)
2. Tufekci, Z.; Wilson, C. Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square. *J. Commun.* **2012**, *62*, 363–379. [\[CrossRef\]](#)
3. Bernhard, D.; Lovejoy, J.P.; Ann-Kathrin, H.; Brittany, N.H. Facebook and Online Privacy: Attitudes, Behaviors and Unintended Consequences. *J. Comput.-Mediat. Commun.* **2009**, *15*, 83–108.
4. Reynolds, B.; Venkatanathan, J.; Goncalves, J.; Kostakos, V. Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. In *IFIP Conference on Human-Computer Interaction*; Conference Paper; Springer: Berlin/Heidelberg, Germany, 2011; pp. 204–215.
5. Barth, S.; Jong, M.D.; Junger, M.; Hartel, P.H.; Roppelt, J.C. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telemat. Inform.* **2019**, *41*, 55–69. [\[CrossRef\]](#)
6. Spiekermann, S.; Berendt, B.; Grossklags, J. E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior. Social Science Electronic Publishing. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, Tampa, FL, USA, 14–17 October 2001; pp. 38–47.
7. Norberg, P.A.; Horne, D.R.; Horne, D.A. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126. [\[CrossRef\]](#)
8. Masur, P.K. Understanding the effects of conceptual and analytical choices on ‘finding’ the privacy paradox: A specification curve analysis of large-scale survey data. *Inf. Commun. Soc.* **2021**, 1–19. [\[CrossRef\]](#)
9. Choi, H.; Park, J.; Jung, Y. The role of privacy fatigue in online privacy behavior. *Comput. Hum. Behav.* **2018**, *81*, 42–51. [\[CrossRef\]](#)
10. Kwon, J.; Johnson, M.E. The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? Workshop on the Economics of Information Security. *Neth. Delft* **2015**, *6*, 22–23.
11. Kaspersky. The True Value of Digital Privacy: Are Consumers Selling Themselves Short? 2019. Available online: <https://www.kaspersky.com/blog/privacy-report-2019/> (accessed on 20 August 2022).
12. Junglas, I.A.; Spitzmüller, C. Personality Traits and Privacy Perceptions: An Empirical Study in the Context of Location-Based Services. *Eur. J. Inf. Syst.* **2008**, *17*, 387–402. [\[CrossRef\]](#)
13. Warren, S.D.; Brandeis, L.D. The right to privacy. *Harv. Law Rev.* **1890**, *4*, 193–220. [\[CrossRef\]](#)
14. Dhir, A.; Kaur, P.; Chen, S.; Pallesen, S. Antecedents and consequences of social media fatigue. *Int. J. Inf. Manag.* **2019**, *48*, 193–202. [\[CrossRef\]](#)
15. Dienlin, T.; Trepte, S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *Eur. J. Soc. Psychol.* **2015**, *45*, 285–297. [\[CrossRef\]](#)
16. Barness, B. A privacy paradox: Social networking in the United States. *First Monday* **2006**, *11*, 5–7. [\[CrossRef\]](#)
17. Baek, Y.M.; Kim, E.M.; Bae, Y. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Comput. Hum. Behav.* **2014**, *31*, 48–56. [\[CrossRef\]](#)
18. Cho, H.; Lee, J.S.; Chung, S. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Comput. Hum. Behav.* **2010**, *26*, 987–995. [\[CrossRef\]](#)
19. Jensen, C.; Potts, C.; Jensen, C. Privacy practices of Internet users: Self-reports versus observed behavior. *Int. J. Hum.-Comput. Stud.* **2005**, *63*, 203–227. [\[CrossRef\]](#)
20. Wilson, D.W.; Valacich, J.S. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *Proceedings of the 33rd International Conference on Information Systems*. *Florida* **2012**, *41*, 114–125.
21. Karwatzki, S.; Dytynko, O.; Trenz, M.; Veit, D. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *J. Manag. Inf. Syst.* **2017**, *34*, 369–400. [\[CrossRef\]](#)
22. Stutzman, F.; Capra, R.; Thompson, J. Factors mediating disclosure in social network sites. *Comput. Hum. Behav.* **2011**, *27*, 590–598. [\[CrossRef\]](#)
23. Xu, H.; Teo, H.H.; Tan, B.; Agarwal, R. The role of push pull technology in privacy calculus: The case of location based services. *J. Manag. Inf. Syst.* **2010**, *26*, 135–174. [\[CrossRef\]](#)
24. Piper, B.F.; Lindsey, A.M.; Dodd, M.J. Fatigue mechanisms in cancer patients: Developing nursing theory. *Oncol. Nurs. Forum* **1987**, *14*, 17–23. [\[PubMed\]](#)
25. Tang, J.; Akram, U.; Shi, W. Why people need privacy? The role of privacy fatigue in app users’ intention to disclose privacy: Based on personality traits. *J. Enterp. Inf. Manag.* **2020**, *8*, 1–24. [\[CrossRef\]](#)
26. Hargittai, E.; Marwick, A. What Can I Really Do?: Explaining Online Apathy and the Privacy Paradox. *Soc. Sci. Electron. Publ.* **2015**, *10*, 3737–3757.
27. Bansal, G.; Zahedi, F.; Gefen, D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decis. Support Syst.* **2010**, *49*, 138–150. [\[CrossRef\]](#)
28. Chen, H.; Beaudoin, C.E.; Hong, T. Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Comput. Hum. Behav.* **2017**, *70*, 291–302. [\[CrossRef\]](#)
29. Furnell, S.; Thomson, K.L. Recognising and addressing ‘security fatigue’. *Comput. Fraud Secur.* **2009**, *11*, 7–11. [\[CrossRef\]](#)

30. Petty, R.E.; Cacioppo, J.T. *The Elaboration Likelihood Model of Persuasion*; Communication and Persuasion; Springer: New York, NY, USA, 1986; pp. 1–24.
31. Bhattacharjee, A.; Sanford, C. Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Q.* **2006**, *30*, 805–825. [[CrossRef](#)]
32. Lee, J.; Park, D.H.; Han, I. The effect of negative online consumer reviews on product attitude: An information processing view. *Electron. Commer. Res. Appl.* **2008**, *7*, 341–352. [[CrossRef](#)]
33. Bi, S.; Liu, Z.; Usman, K. The influence of online information on investing decisions of reward-based crowdfunding. *J. Bus. Res.* **2017**, *71*, 10–18. [[CrossRef](#)]
34. Zhu, M.; Wu, C.; Huang, S.; Zheng, K.; Young, S.D.; Yan, X.; Yuan, Q. Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telemat. Inform.* **2021**, *61*, 101601. [[CrossRef](#)]
35. Park, D.H.; Lee, J.; Han, I. The effect of on-line consumer reviews on consumer purchasing intention: The moderating role of involvement. *Int. J. Electron. Commer.* **2007**, *11*, 125–148. [[CrossRef](#)]
36. Zhou, T.; Lu, Y.; Wang, B. Examining online consumers' initial trust building from an elaboration likelihood model perspective. *Inf. Syst. Front.* **2016**, *18*, 265–275. [[CrossRef](#)]
37. Mamonov, S.; Benbunan-Fich, R. Exploring factors affecting social e-commerce service adoption: The case of Facebook gifts. *Int. J. Inf. Manag.* **2017**, *37*, 590–600. [[CrossRef](#)]
38. Feng, Y.; Xie, W. Teens concern for privacy when using social net-working sites: An analysis of socializations agents and relationships with privacy-protecting behaviors. *Comput. Hum. Behav.* **2014**, *33*, 153–162. [[CrossRef](#)]
39. Carver, C.S.; Scheier, M.F.; Weintraub, J.K. Assessing coping strategies: A theoretically based approach. *J. Personal. Soc. Psycho* **1989**, *56*, 267–283. [[CrossRef](#)]
40. Lee, E. Why do people leave SNS? The Influences of the Users' Characteristics and SNS Fatigue. *J. HCI Soc. Korea* **2018**, *13*, 11–19. [[CrossRef](#)]
41. Adhikari, K.; Panda, R.K. Evaluation of brand relationship quality using formative index: A novel measurement approach. *J. Prod. Brand Manag.* **2019**, *29*, 505–516. [[CrossRef](#)]
42. Ravindran, T.; Kuan, A.C.Y.; Lian, D.G.H. Antecedents and effects of social network fatigue. *J. Assoc. Inf. Sci. Technol.* **2014**, *65*, 2306–2320. [[CrossRef](#)]
43. Kim, M.S.; Lee, D.J. The role of digital fatigue and flow in SNS usage. *E-Bus. Stud.* **2012**, *13*, 67–87.
44. Tu, F. WeChat and civil society in China. *Commun. Public* **2016**, *3*, 343–350. [[CrossRef](#)]
45. Tencent. Second Quarter and Annual Results Announcement. 2022. Available online: https://view.inews.qq.com/k/20220817A06YCJ00?web_channel=wap&openApp=false (accessed on 20 August 2022).
46. Rubin, D.B. Using propensity scores to help design observational studies: Application to the tobacco litigation. *Health Serv. Outcomes Res. Methodol.* **2001**, *2*, 169–188. [[CrossRef](#)]
47. Cyr, D.; Head, M.; Lim, E.; Stibe, A. Using the elaboration likelihood model to examine online persuasion through website design. *Inf. Manag.* **2018**, *55*, 807–821. [[CrossRef](#)]
48. Shankar, A.; Jebarajakirthy, C.; Ashaduzzaman, M. How do electronic word of mouth practices contribute to mobile banking adoption? *Retail. Consum. Serv.* **2020**, *52*, 101920. [[CrossRef](#)]
49. Crlab, C.; Eza, D.; Jthab, C. Adoption of online follow-up service by patients: An empirical study based on the elaboration likelihood model. *Comput. Hum. Behav.* **2020**, *114*, 106581.