MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Rui, J. R., & Xie, J. (2026). Rationalization or reactance: How psychological distance and efficacy beliefs moderate the effect of perceived inevitability on online privacy protection. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 20*(5), Article 7. https://doi.org/10.5817/CP2026-5-7

Rationalization or Reactance: How Psychological Distance and Efficacy Beliefs Moderate the Effect of Perceived Inevitability on Online Privacy Protection

Jian Raymond Rui[1] *& Jingzhong Xie*[2]

[1]College of Journalism and Communication, South China University of Technology
[2]College of Journalism and Culture Communication, Zhongnan University of Economics and Law

Abstract

By collecting user information, algorithms pose a severe threat to user privacy. However, increased incidents of privacy breaches do not necessarily motivate privacy protection behaviors. Drawing upon System Justification Theory and Construal Level Theory, this research aims to explain how individuals rationalize disengagement from online privacy protection. An online survey of Chinese users of e-commerce platforms (N = 534) reveals that temporal and social distances of online privacy invasion were negatively associated with perceived inevitability of this threat, which was negatively related to the intention to protect online privacy. Furthermore, the relationship between perceived inevitability and the protection intention was only significant at low levels of response efficacy. Self-efficacy did not moderate this relationship. Therefore, individuals disengage from online privacy protection because they perceive privacy threats approaching and as inevitable and do not think there is any effective method mitigating these threats. These findings demonstrate how low psychological distance of online privacy invasion and lack of response efficacy may deprive individuals from their agency in protecting privacy.

Editorial Record

First submission received:
September 14, 2024

Revisions received:
March 23, 2025
November 17, 2025
February 26, 2025
May 30, 2026

Accepted for publication:
August 2, 2026

Editor in charge:
Joris Van Ouytsel

Keywords: perceived inevitability; psychological distance; efficacy appraisal; rationalization; online privacy; e-commerce platforms

Introduction

Privacy concern has received wide scholarly attention since Internet-based technologies became accessible to average individuals (Acquisti & Grossklags, 2005). In recent years, many online services such as e-commerce platforms have adopted algorithms. By collecting user information such as their purchase history, user comments, and background information, these algorithms can develop better understanding of user preferences and needs, which can help platforms provide users with tailored recommendations (Wang et al., 2021). However, these recommendations are made at the cost of user privacy.

Earlier research has applied privacy calculus model and conceptualized privacy protection as the result of cost-benefit analyses (Dienlin & Metzger, 2016; Krasnova et al., 2010). Other research argued that privacy protection was essentially a behavior aimed at mitigating threats and thereby was motivated by risk perception (Zhang et al., 2018) and efficacy appraisals including response efficacy (Boerman et al., 2018; Yu et al., 2024) and self-efficacy (Chen & Chen, 2015; Kee & Shin, 2022; van Ooijen et al., 2024). By linking socio-cognitive variables and privacy protection, these studies suggest that privacy protection is the result of personal choices.

However, recent research provides an alternative explanation by positing that frequent privacy breaches may deprive individuals' agency in privacy protection (Lutz et al., 2020). As a result, individuals either experience privacy fatigue (Choi et al., 2018; Chung & Kwon, 2025; Zhang et al., 2022) or privacy cynicism (Hoffmann et al., 2016; Lutz et al., 2020; van Ooijen et al., 2024), which eventually causes the inaction on privacy protection. Additionally, both concepts suggest that individuals rationalize their withdrawal from online privacy protection as a coping strategy in response to the stress of privacy breaches (Choi et al., 2018; Hoffmann et al., 2016; Lutz et al., 2020).

Despite these insights, research on privacy fatigue and privacy cynicism has yet to provide clear explanations about the mechanism by which rationalization of privacy protection disengagement happens. As a response, the present study employs System Justification Theory (Jost, 2019; Jost et al., 2004; Kay et al., 2009; Kay & Zanna, 2009) and Construal Level Theory (Liberman & Trope, 2008). Specifically, we propose that frequent privacy breaches may lower individuals' psychological distance of privacy invasion and make them perceive this threat as inevitable, which likely drives individuals to engage in rationalization through lowering their intention to protect privacy on e-commerce platforms (Laurin, 2018; Laurin et al., 2012). Thus, we examined whether perceived inevitability mediated the relationship between psychological distance of online privacy invasion and the intention to protect privacy. Additionally, as perceived inevitability does not always predict rationalization (Laurin et al., 2012), we investigated whether efficacy appraisals of online privacy protection, composed of response efficacy and self-efficacy, moderated the relationship between perceived inevitability and the intention to protect online privacy.

We conducted our research among a sample of Chinese users of e-commerce platforms, a typical example of algorithmic technologies. In China, as of December 2023, the number of people who engaged in online shopping had reached 915 million, accounting for 83.8% of the overall number of Internet users in this country (China Internet Network Information Center, 2024). In addition, Chinese netizens expressed lowered levels of concerns about algorithms collecting user data, compared to Americans (Xing et al., 2023). Therefore, the Chinese sample provides an appropriate context for the current investigation.

Privacy Protection Disengagement

By collecting, analyzing, and commercializing users' information and behavioral data, Internet platforms have established a new form of capitalism: data capitalism (West, 2019). As user data constitute the core asset of data capitalism, privacy breaches have occurred repeatedly, which eventually deprives individuals of their agency in privacy protection (Lutz et al., 2020). Consequently, individuals decide to disengage from online privacy protection as a coping strategy.

Previous research has proposed two similar concepts that explain how disengagement from online privacy protection happens. First, privacy fatigue refers to "a sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet" (Choi et al., 2018; p.42). Specifically, according to Choi et al. (2018), privacy fatigue functions similarly to burnout and is derived from over-engagement in privacy protection attempts.

In addition, privacy cynicism is conceptualized as "an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile" (Hoffmann et al., 2016; p.5). Thus, privacy cynicism is conceptualized as a mix of cognitive, affective, and behavioral responses to external threats (Hoffmann et al., 2016; Lutz et al., 2020).

While both concepts provide insights on how individuals rationalize their disengagement from online privacy protection, the mechanism by which rationalization happens remains unclear. For instance, as Choi et al. (2018) argued, individuals reporting privacy fatigue should experience a transition from over-engagement to disengagement. However, this process of change has yet to receive empirical support. In fact, empirical studies on privacy fatigue have generated a wide range of variables related to privacy fatigue, including privacy experiences, users' knowledge, skills, and sense of control, personality, and privacy policies (see a scoping review by van Der Schyff et al., 2023).

As for privacy cynicism, its four dimensions (uncertainty, powerlessness, mistrust, resignation) may operate in a sequential manner and influence each other. For instance, uncertainty about how Internet platforms may handle user data likely contributes to powerlessness in privacy protection (Acquisti et al., 2015), which cultivates mistrust in these platforms and eventually causes resignation (Hargittai & Marwick, 2016). Alternatively, mistrust

in Internet platforms may cultivate uncertainty and powerlessness (Cho, 2024). For instance, a recent study shows that when individuals perceived the Internet platforms provided unfair privacy policies, this reduced their sense of privacy control (Pu & Chen, 2026). However, research has yet to explicate the relationship between these dimensions, leaving the mechanism by which privacy cynicism is related to rationalization of privacy protection disengagement unclear.

Thus, it is necessary to explicate the mechanism by which individuals rationalize their inaction on privacy management. Theories provide a tool for our investigation, specifically System Justification Theory.

System Justification Theory and Rationalization

Rationalization is conceptualized as a process in which individuals try to persuade themselves so the target situation appears more palatable to them (Laurin et al., 2012). This concept can be traced back to cognitive dissonance theory (Cooper, 2007), which assumes that individuals are driven to keep their perceptions of the reality consistent with the existential reality of the world (Festinger, 1957). When individuals' perceptions do not align with reality, they tend to experience cognitive dissonance, which motivates them to restore the balance between their perception and the reality (Festinger, 1957). Specifically, they tend to rationalize their choices and provide an explanation of the reality so they can be convinced that their current situation is less disappointing and more appealing (Festinger, 1957).

Subsequent research extended this work by explicating what triggers rationalization (Jost, 2019; Jost et al., 2004; Kay & Zanna, 2009; Kay et al., 2009). Specifically, System Justification Theory noted that individuals could be motivated to enhance the legitimacy of the system in which they live (Jost et al., 2004; Kay et al., 2009). Particularly, perceived inevitability of certain events can facilitate rationalization (Jost, 2019; Kay & Zanna, 2009). When individuals believe something will certainly happen but they cannot escape from the situation or change what has happened or will happen, they tend to engage in rationalization (Jost, 2019; Kay & Zanna, 2009).

A series of research by Laurin (2018) and her colleagues (2010, 2012, 2013) provided empirical evidence supporting these arguments. For example, they found that while non-absolute restrictions might trigger psychological reactance, individuals tended to respond to absolute restrictions with rationalization (Laurin et al., 2012). Likewise, when individuals realized that it was impossible to change the reality, they tended to engage in rationalization by changing their attitude towards or appraisal of the reality (Laurin, 2018; Laurin et al., 2010, 2013).

Therefore, rationalization is likely to happen when certain events are perceived inevitable. Based on System Justification Theory, when individuals perceive online privacy invasion as inevitable, they tend to engage in rationalization to maintain cognitive balance (Laurin, 2018; Laurin et al., 2010, 2012, 2013). Prior research assessed rationalization by measuring one's attitude towards or reactions to the target event (Laurin, 2018; Laurin et al., 2012). In the present study, we used the lowered intention to protect online privacy as a proxy for rationalization. Based on the research reviewed above, we propose that:

H1: Perceived inevitability of online privacy threat is negatively related to the intention to protect their online privacy.

Notably, perceived inevitability differs from the powerlessness dimension of privacy cynicism. Powerlessness refers to the loss of control over personal privacy (Hoffman et al., 2016; Lutz et al., 2020). Essentially, it reflects an individual's capacity to manage privacy and is related to the efficacy of privacy management. In contrast, perceived inevitability is defined as one's estimates of "the probability or necessity of" the target event (Nestler & Egloff, 2009, p. 1540), which describes one's perception of the external threat. Thus, they represent two different categories of variables which are predicted to influence one's engagement in risk-mitigating behaviors (Rogers, 1975; Witte, 1992). The role of privacy-related efficacy, as it moderates this process, will be examined subsequently.

Psychological Distance and Perceived Inevitability

The next question is what contributes to perceived inevitability. Construal Level Theory provides a theoretical framework for addressing this question (Liberman & Trope, 2008). Construal level is conceptualized as how individuals mentally present a given object and is closely related to psychological distance (Liberman & Trope,

2008). Construal level theory distinguishes four types of psychological distance: spatial, social, temporal, and hypothetical (Liberman & Trope, 2008). Spatial distance refers to the geographical distance between individuals and the target object (Liberman & Trope, 2008). Social distance is conceptualized as the relational closeness between individuals and the target object, often indicated by similarity, familiarity, and group membership (Liberman & Trope, 2008). Temporal distance is defined as how far the target event will happen or happened from the present time (Liberman & Trope, 2008). Hypothetical distance refers to the certainty of the event (Liberman & Trope, 2008).

Liberman and Trope (2008) argued that the construal level was correlated with psychological distance. At a high level of psychological distance, individuals tend to develop abstract mental representations of the target object, prompting them to only perceive central and superordinate characteristics of the target (Liberman & Trope, 2008). By contrast, as psychological distance reduces, individuals tend to develop detailed understanding of the target object (Liberman & Trope, 2008).

Individuals can vary in their psychological distance of online privacy invasion. Some may have heard that these incidents happened to their family or friends or even have experienced similar incidents. This can lower their *social* distance of online privacy invasion. Additionally, if they notice that online privacy invasion has happened recently, this can reduce their *temporal* distance of online privacy invasion.

Previous research has demonstrated that a negative relationship may exist between psychological distance and perceived inevitability (Laurin, 2018; Laurin et al., 2012). For example, Laurin (2018) found that Americans' attitude towards Trump improved after his inauguration, a sign of rationalization, compared to that before the inauguration. They argued that as the inauguration of the U.S. President Trump approached, individuals knew it was real and inevitable, which drove them to rationalize this unpleasant fact (Laurin, 2018). Thus,

H2: (a) Temporal and (b) social distances of online privacy threats are negatively related to perceived inevitability of these threats.

We only considered temporal and social distances of privacy threats because the other two types of psychological distance may not apply to the current study. First, online privacy threats have happened across the world, so spatial distance may not matter. Second, given the frequency of privacy breaches reported in the news, there is strong evidence of privacy invasion. Thus, we do not consider hypothetical distance either.

Taken together, individuals perceiving low temporal and social distances of online privacy threats are likely to think these threats are inevitable. They may then engage in rationalization by lowering their intentions to protect their privacy online. This suggests a mediation path from temporal and social distances to the intention for online privacy protection through perceived inevitability.

H3: Perceived inevitability of online privacy threats mediates the relationship between (a) temporal and (b) social distances of these threats and the intention to protect online privacy.

The Moderation Effect of Privacy-Related Efficacy Appraisals

Laurin et al. (2012) suggests that individuals may not necessarily engage in rationalization when facing threats. Instead, they can take actions to defend themselves from the threats, and this reaction was termed as reactance (Laurin et al., 2012). Thus, there may be variables moderating the relationship described in H1.

The moderators we proposed are efficacy appraisals, often composed of response efficacy and self-efficacy (Witte, 1992). While response efficacy refers to the extent to which individuals think the target action can inhibit the threat, self-efficacy is defined as the degree to which individuals think they can perform the target action (Witte, 1992).

Although efficacy appraisal was originally proposed in the health context (Witte, 1992), subsequent research extended their effects to the context of online privacy protection. Research found that response efficacy (Boerman et al., 2018; Yu et al., 2024) and self-efficacy (Chen & Chen, 2015; Kee & Shin, 2022; van Ooijen et al., 2024) were positively related to privacy protection behaviors. We extended these studies by arguing that privacy-related efficacy appraisals may moderate the relationship between perceived inevitability and the intention to protect online privacy. As reviewed above, Laurin et al. (2012) found that absolute restrictions triggered rationalization, whereas non-absolute restrictions triggered reactance. Thus, the likelihood that individuals think the current situation can be reverted should affect their subsequent reactions. If they think the threat can be

mitigated, they may take actions to defend themselves from the threat (Laurin et al., 2012). On the contrary, they may rationalize the threat (Laurin et al., 2012).

The likelihood that individuals think the target threat can be mitigated should be related to their efficacy appraisals. Repeated events of privacy breaches can make individuals feel no effective techniques can protect their privacy online (Choi et al., 2018), causing low privacy-related *response* efficacy. Additionally, these incidents of privacy invasion can reduce individuals' confidence in controlling their privacy online (Hargittai & Marwick, 2016), causing low privacy-related *self*-efficacy. Individuals exhibiting low levels of privacy-related response efficacy and self-efficacy should feel helpless to protect their privacy (Witte, 1992). This perception may cause rationalization (Laurin et al., 2012). Thus, the relationship between perceived inevitability and the intention to protect online privacy can be strengthened for individuals reporting low levels of privacy-related response efficacy and self-efficacy. Conversely, individuals exhibiting high levels of privacy-related response efficacy and self-efficacy may feel it is possible to control the damage of online privacy invasion (Witte, 1992). Therefore, among these individuals, no matter whether they report high or low levels of perceived inevitability of online privacy invasion, their intention to protect online privacy should be similar.

H4: Privacy-related (a) response efficacy and (b) self-efficacy moderate the relationship between perceived inevitability and the intention to protect online privacy. This relationship should be negative among those reporting low levels of privacy-related (a) response efficacy and (b) self-efficacy, whereas this relationship should be nonsignificant among those reporting high levels[1].

Methods

Overview

We conducted an online survey to test our hypotheses. The survey was hosted via credamo.com, a large company in China that offers sampling services and functions similarly to MTurk. Participants were limited to users of e-commerce platforms. Thus, we first asked whether participants had used any online platforms for shopping. Examples of e-commerce platforms were provided for participants. Those who answered no were directed to the end of the survey.

Next, participants read the information about the survey and gave their consent to participate. They answered questions about their intention to protect their privacy on e-commerce platforms, followed by other variables mentioned above. This procedure received approval from the research ethics committee at the first author's institute.

The data collection was completed in February 2024. We received 550 responses. Two attention check questions were positioned in the survey. One asked the participants to choose *moderately disagree* and the other asked the participants to choose *strongly agree*. Those failing either question were removed, leading to a final sample of 534.

Sample

There were more female participants (343, or 64.2%) than male (191, or 35.8%). They were around 32 years old (M = 32.06, SD = 14.15, Min = 18, Max = 58). Most participants finished college education (394, or 73.8%), followed by graduate degree (78, or 14.6%), associated degree (50, or 9.4%), high school (8, or 1.5%), middle school (2, or .4%) and elementary school or lower (2, or .4%). Fewer than half of the participants reported monthly income between 5001 RMB and 10,000 RMB (214, or 40.1%), followed by 5000 RMB or less (136, or 25.5%), between 10,001 RMB and 15,000 RMB (98, or 18.4%), between 15,001 RMB and 20,000 RMB (43, or 8.1%), and 20,001 RMB or above (43, or 8.1%).

Measures

The Dependent Variable

All the variables were measured on 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*). *The intention to protect online privacy* was adapted from a three-item scale assessing the intention to engage in privacy

protection behaviors on social network sites (Ho et al., 2017). Participants indicated their agreement with these three statements on a 7-point Likert scale ("I intend to/will try to/plan to engage in privacy protection behaviors on e-commerce platforms in the next month"; Cronbach's α = .93, *M* = 5.48, *SD* = 1.30).

The Mediator

We adapted the scale of *perceived inevitability* by Nestler and Egloff (2009) ("on the contemporary e-commerce platforms, privacy violation is inevitable" and "it is inevitable to sacrifice personal privacy on the e-commerce platforms"; Spearman's r = .73, p < .001, *M* = 4.03, *SD* = 1.67).

The Independent Variables

We adjusted the scale by Spence et al. (2011) to measure *social distance of online privacy threat* ("privacy invasion on e-commerce platforms is most likely to affect people like me/have a big impact on average people just like me"). However, their measure of temporal distance was only one item (Spence et al., 2011), so we used the two-item scale of *temporal distance* by Sanna et al. (2006) instead ("it seems very distant that your privacy is violated when you use e-commerce platforms" and "privacy violation on e-commerce platforms happens every day"). We reverse coded the items so that a larger value indicated farther temporal (Spearman's r = .71, p < .001, *M* = 3.27, *SD* = 1.73) and social distances (Spearman's r = .76, p < .001, *M* = 3.18, *SD* = 1.67). The confirmatory factor analysis via the Lavaan package through R provides empirical evidence on the validity of our measures of these two types of psychological distance, $\chi^2(3) = 11.27$, p = .010, CFI = .995, TLI = .99, RMSEA = .072.

The Moderators

Witte et al. (1996) created scales that measure response efficacy and self-efficacy in the health context. We adjusted their questions to the current research to measure *privacy-related response efficacy* ("privacy protection techniques work in preventing my privacy on e-commerce platforms from being threatened", "learning privacy protection techniques is effective in preventing my privacy on e-commerce platforms from being threatened", "if I engage in privacy protection techniques, my privacy on e-commerce platforms is less likely violated"; Cronbach's α = .87, *M* = 5.54, *SD* = 1.16) and *self-efficacy* ("I'm able to protect my privacy on e-commerce platforms", "I think I can adopt effective techniques to protect my privacy on e-commerce platforms", "I think I'm capable to protect my privacy on e-commerce platforms"; Cronbach's α = .91, *M* = 5.35, *SD* = 1.33). Table 1 presents descriptive statistics of and bivariate correlations between the variables mentioned above.

Table 1. *Descriptive Statistics and Bivariate Correlations Between Major Variables.*

	1	2	3	4	5	6
Intention	5.48 (1.30)	−.00	−.13**	−.13**	.11***	.16***
Inevitability		4.03 (1.67)	−.63***	−.67***	−.40***	−.48***
Temporal distance			3.18 (1.67)	.82***	.39***	.43***
Social distance				3.27 (1.73)	.38***	.44***
Response efficacy					5.54 (1.16)	.75***
Self-efficacy						5.35 (1.33)

Note. ***p < .001, **p < .01.

Control Variables

Control variables include sex (0 = *male*, 1 = *female*), age (*M* = 32.06, *SD* = 14.15), education (1 = *primary school or below*, 2 = *middle school*, 3 = *high school*, 4 = *associate degree*, 5 = *college degree*, 6 = *master or PhD*; *M* = 5.00, *SD* = .63), income (1 = 5,000 RMB or below, 2 = 5,001–10,000 RMB, 3 = 10,001–15,000 RMB, 4 = 15,001–20,000 RMB, 5 = 20,001 RMB or above; *M* = 2.33, *SD* = 1.17), frequency of using e-commerce platforms, and user intensity of e-commerce platforms. *Frequency* was assessed through one question, which asked participants to indicate how frequently they used e-commerce platforms the month before (1 = *once or never*, 2 = *once per week*, 3 = *2–3 times per week*, 4 = *once every day*, 5 = *2–3 times every day*, 6 = *used it every one or two hours*, 7 = *almost every minute on*

these platforms; *M* = 3.89, *SD* = 1.16). Examples of e-commerce platforms were offered to participants to assist their answer. In addition, we adapted the *user intensity* scale of social network sites by Ellison et al. (2007) to the current research context (Cronbach's α = .74, *M* = 5.40, *SD* = 1.24).

Data Analysis

Hypotheses were tested through Macro Process 5.0 via SPSS 29. We built four moderated mediation models. Temporal distance and social distance were tested as the independent variable respectively, whereas response efficacy and self-efficacy were tested as the moderator for the relationship between perceived inevitability and the intention to protect online privacy respectively. We requested perceived inevitability, response efficacy and self-efficacy standardized for the moderation analyses. If a significant relationship emerged, we proceeded to the simple slope analysis. Specifically, the relationship between perceived inevitability and the intention to protect privacy was compared at the low (1 standard deviation below the mean) and high levels (1 standard deviation above the mean) of the moderator (i.e., response efficacy and self-efficacy).

All the values of variance inflation factor ranged between 1.05 and 2.33. Therefore, no evidence of multicollinearity was found. A 95% confidence interval (CI) was reported to indicate the significance of the proposed mediation effects and moderated mediation effects. The Johnson-Neyman technique was applied to define the significance region of the moderation analysis and plot it. We plotted the figures of the moderation analysis by using the gglot2 package via R.

Results

Temporal Distance

Response Efficacy as the Moderator

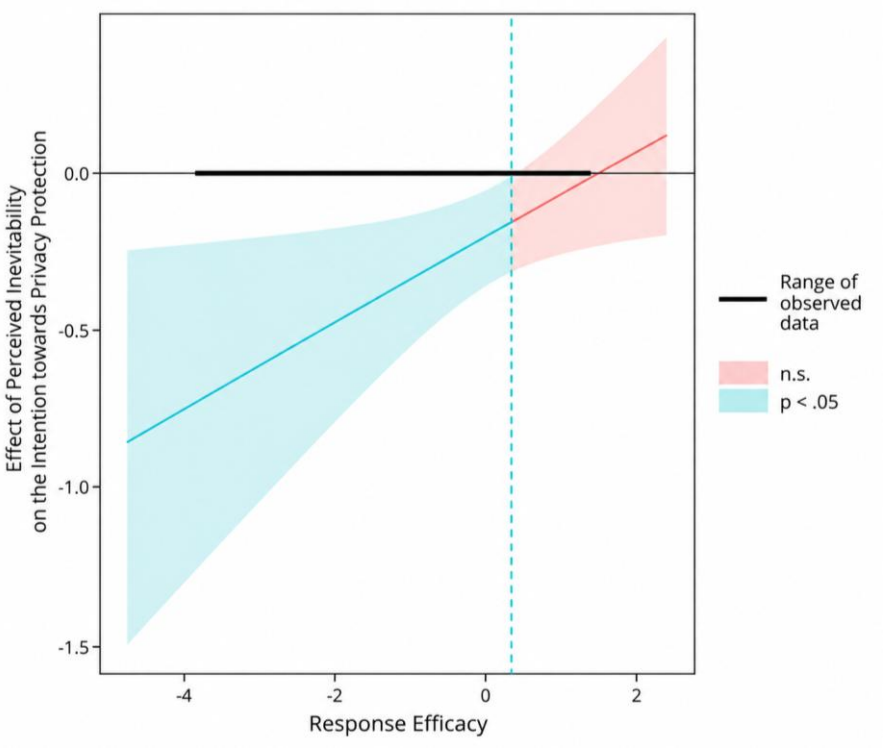
Temporal distance was negatively related to perceived inevitability of online privacy invasion (β = −.60, $p < .001$, Table 2). In addition, perceived inevitability was negatively associated with the intention to protect online privacy (β = −.16, $p = .004$). Their relationship was moderated by response efficacy (β = .11, $p = .035$). Specifically, perceived inevitability was negatively related to the intention when response efficacy was low (β = −.26, $p < .001$), whereas this relationship was nonsignificant when response efficacy was high ($p = .406$ Figure 1). Therefore, H1, H2a, and H4a were supported.

Table 2. *Results of Moderated Mediation Analysis (Temporal Distance as the Independent Variable and Response Efficacy as the Moderator).*

	Perceived inevitability	The intention to protect online privacy
Temporal distance	−.60***	−.27***
Perceived inevitability	NA	−.16**
Response efficacy	NA	.02
Interaction, perceived inevitability and response efficacy	NA	.11*
Sex	.02	−.07+
Age	.00	.02
Education	−.01	−.08+
Income	−.12**	−.12**
Frequency of using e-commerce platforms	−.02	−.05
User intensity	.00	.28***
Adjusted R^2, *p, F*	.40***, $F(7, 525) = 51.22$	.13***, $F(10, 522) = 8.60$

Note. ***$p < .001$, **$p < .01$, *$p < .05$, +$p < .1$; Sex: 0 = *male*, 1 = *female*.

Figure 1. *Response Efficacy Moderated the Relationship Between Perceived Inevitability of Online Privacy Invasion and the Intention to Protect Online Privacy (When the Independent Variable was Temporal Distance).*



The moderated mediation was not significant (−.04, 95% CI [−.08, .004]). Specifically, the mediation effect of perceived inevitability between temporal distance and the intention to protect online privacy was only significant at a low level of response efficacy (.12, 95% CI [.05, .19]). Therefore, H3a received partial support

Self-Efficacy as the Moderator

When the moderation effect of self-efficacy was analyzed, perceived inevitability was still negatively related to the intention for online privacy protection (β = −.09, p = .034, Table 3). However, self-efficacy did not moderate this relationship (p = .174). Therefore, H1 and H2a were supported, but H4b was rejected.

Again, the moderated mediation relationship was not significant (−.02, 95% CI [−.06, .01]), as it was only supported at a low level of response efficacy (.09, 95% CI [.016, .16]). H3a was partially supported.

Table 3. *Results of Moderated Mediation Analysis (Temporal Distance as the Independent Variable and Self-Efficacy as the Moderator).*

	Perceived inevitability	The intention to protect online privacy
Temporal distance	−.60***	−.30***
Perceived inevitability	NA	−.12*
Self-efficacy	NA	.14*
Interaction, perceived inevitability and self-efficacy	NA	.07
Sex	.02	−.07+
Age	.00	.02
Education	−.01	−.08+
Income	−.12**	−.13**
Frequency of using e-commerce platforms	−.02	−.05
User intensity	.00	.26***
Adjusted R^2, p, F	.40***, F(7, 525) = 51.22	.14***, F(10, 522) = 9.78

Note. ***p < .001, **p < .01, *p < .05, +p < .1. Sex: 0 = *male*, 1 = *female*.

Social Distance

Response Efficacy as the Moderator

Social distance was negatively related to perceived inevitability (β = −.65, p < .001, Table 4). Perceived inevitability was negatively associated with the intention to protect online privacy (β = −.15, p = .008). Response efficacy moderated the relationship between perceived inevitability and the intention (β = .12, p = .022). Specifically, this relationship was only significant at a low level of response efficacy (β = −.26, p < .001), whereas it was not significant at a high level (p = .542, Figure 2). H1, H2b, and H4a were supported.

Figure 2. *Response Efficacy Moderated the Relationship Between Perceived Inevitability of Online Privacy Invasion and the Intention to Protect Online Privacy (When the Independent Variable was Social Distance)*

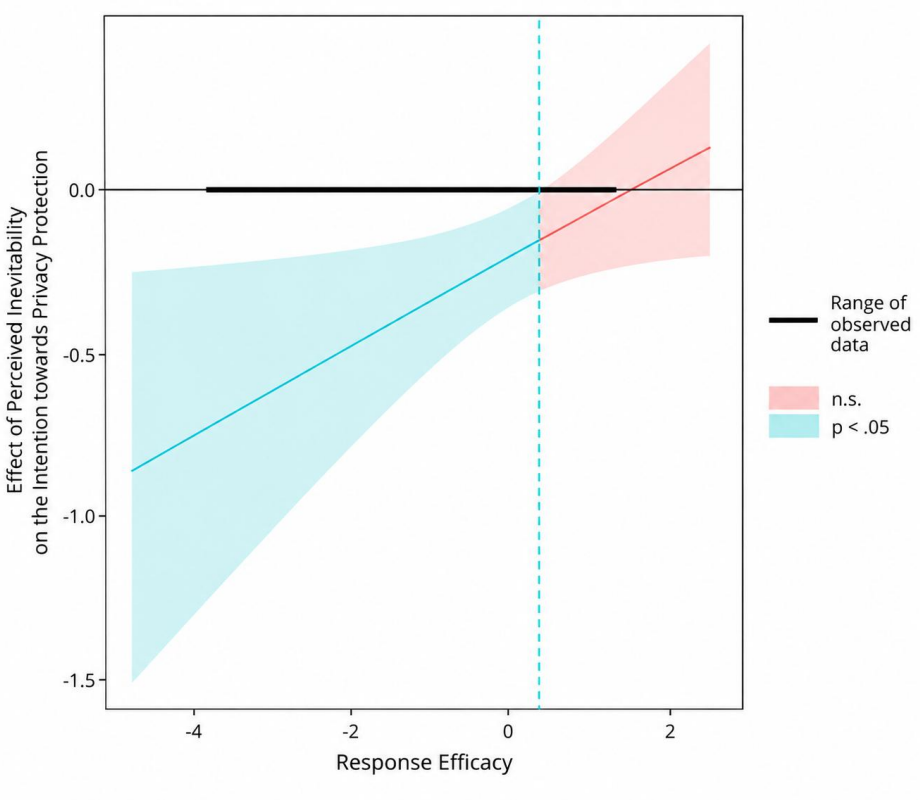


Table 4. *Results of Moderated Mediation Analysis (Social Distance as the Independent Variable and Response Efficacy as the Moderator).*

	Perceived inevitability	The intention to protect online privacy
Social distance	−.65***	−.24***
Perceived inevitability	NA	−.15**
Response efficacy	NA	.01
Interaction, perceived inevitability and response efficacy	NA	.12*
Sex	.02	−.07+
Age	−.00	.01
Education	.01	−.08+
Income	−.07+	−.11*
Frequency of using e-commerce platforms	.01	−.04
User intensity	−.04	.26***
Adjusted R^2, p, F	.45***, F(7, 525) = 62.05	.11***, F(10, 522) = 7.80

Note. ***p < .001, **p < .01, *p < .05, +p < .1. Sex: 0 = *male*, 1 = *female*.

The moderated mediation was supported (−.05, 95% CI [−.09, .003]). Specifically, the mediation effect of perceived inevitability between social distance and the intention to protect online privacy was only significant at a low level of response efficacy (.13, 95% CI [.05, .20]). H3b was partially supported.

Self-Efficacy as the Moderator

When the interaction between perceived inevitability and self-efficacy was probed controlling for social distance, self-efficacy did not moderate this relationship (p = .140, Table 5). H1 and H2b were supported, but H4b was rejected.

Table 5. *Results of Moderated Mediation Analysis (Social Distance as the Independent Variable and Self-Efficacy as the Moderator).*

	Perceived inevitability	The intention to protect online privacy
Social distance	−.65***	−.27***
Perceived inevitability	NA	−.11*
Self-efficacy	NA	.14*
Interaction, perceived inevitability and self-efficacy	NA	.08
Sex	.02	−.07
Age	−.00	.01
Education	.01	−.07+
Income	−.07+	−.12**
Frequency of using e-commerce platforms	.01	−.03
User intensity	−.04	.23***
Adjusted R^2, *p, F*	.45***, $F(7, 525) = 62.05$	.13***, $F(10, 522) = 8.88$

Note. ***p < .001, **p < .01, *p < .05, +p < .1. Sex: 0 = *male*, 1 = *female*.

The moderated mediation effect was not significant (−.03, 95% CI [−.07, .01]). The mediation effect of perceived inevitability between social distance and the intention to protect online privacy was only confirmed for the low level of self-efficacy (.09, 95% CI [.02, .17]). H3b was partially supported.

Discussion

Recent research has noted that individuals demonstrate disengagement from online privacy protection (Choi et al., 2018; Hargittai & Marwick, 2016). Although prior research on privacy fatigue and privacy cynicism has offered theoretical explanations about how individuals rationalize their inaction on privacy protection (Choi et al., 2018; Chung & Kwon, 2025; Hoffmann et al., 2016; Lutz et al., 2020; van Ooijen et al., 2024; Zhang et al., 2022), the mechanism of this rationalization remains unclear. Built on System Justification Theory and Construal Level Theory, this study revealed that low temporal and social distances of online privacy invasion were related to high levels of perceived inevitability of this threat, which was then negatively associated with the intention to protect online privacy. Furthermore, the negative relationship between perceived inevitability and the intention to protect online privacy was only significant among individuals reporting low levels of response efficacy of privacy management. Privacy-related self-efficacy did not moderate this relationship. Therefore, individuals indicated they did not intend to protect their online privacy because they perceived privacy threats were approaching and inevitable and they did not believe there was effective measures mitigating these threats.

Major Findings

Our result first reveals that individuals can be unmotivated to protect their privacy online when they think privacy invasion is inevitable. This finding offers additional evidence supporting System Justification Theory which posits that perceived inevitability of the threat can trigger rationalization (Jost, 2019; Jost et al., 2004; Kay et al., 2009; Kay & Zanna, 2009). Moreover, this result supports a series of research by Laurin (2018) and her colleagues (2010, 2012, 2013), which demonstrates that individuals tend to engage in rationalization when they think certain events will certainly happen. As rationalization functions to mitigate cognitive dissonance

(Festinger, 1957), when individuals perceive privacy invasion inevitable, they likely change their appraisal of privacy invasion (Laurin, 2018; Laurin et al., 2012), which in the present study was lowering intentions to protect online privacy.

Second, our findings highlight the potential role that low temporal and social distances of online privacy invasion might play in predicting high levels of perceived inevitability of this threat. Low temporal and social distances might prompt individuals to think that online privacy invasion is happening right now and to them (Liberman & Trope, 2008). This perception could elevate their level of perceived inevitability. This finding aligns with System Justification Theory, which posits that rationalization can be triggered when individuals think they cannot escape from the current situation (Jost, 2019; Kay & Zanna, 2009).

These results develop the scholarship on rationalization. Specifically, prior research has found a series of factors that contribute to rationalization, including perceived absoluteness of the target event, peripheral processing of the policy that limits personal freedom, and the perception that the target event is embedded in the current social system (Proudfoot & Kay, 2014). Our research adds to this scholarship by providing an additional factor that can facilitate rationalization indirectly: low psychological distance of the target threat. Thus, Construal Level Theory may present another perspective of understanding how rationalization may happen. However, it is important to note that psychological distances may trigger rationalization only *indirectly*. As shown in Tables 2–5, our results provide an indication that temporal and social distances exhibited *direct negative* relationships with the intention to protect online privacy, which differs from the positive indirect relationship between temporal/social distances and the intention. These inconsistent mediation effects can be explained through Construal Level Theory. Psychological distance indicates one's evaluation of the distance of certain events compared to them (Liberman & Trope, 2008). Thus, as the distance is reducing, the threat is approaching, which can naturally motivate individuals to defend themselves from the threat. This explains why a direct negative relationship between psychological distance and the intention to protect online privacy might exist. However, low psychological distance can also create a feeling of inescapability, which can prompt individuals to give up fighting and rationalize their situation. Therefore, Construal Level Theory provides two opposite explanations for the effect of low psychological distances.

These inconsistent mediation relationships suggest that individuals do not necessarily engage in rationalization when they think the threat is approaching. Instead, their relationship can be moderated by other variables such as privacy-related response efficacy. Our results reveal that perceived inevitability was only negatively related to the intention when individuals reported low and medium levels of privacy-related response efficacy. As explained earlier, whether individuals choose rationalization (give up) or reactance (fight) may depend on whether they think the threat can be reverted (Laurin et al., 2012). High levels of response efficacy likely prompt people to think that there are effective ways to mitigate the threat of online privacy invasion. Thus, no matter whether they think online privacy invasion is inevitable, this perception should have minimal influences on their intention for privacy protection. On the contrary, low levels of response efficacy demonstrate that individuals do not think there is any effective method to protect their privacy. This can strengthen the relationship between perceived inevitability and lowered intentions towards privacy protection (Jost, 2019; Kay & Zanna, 2009).

In contrast, self-efficacy did not moderate the relationship between perceived inevitability and the intention. This finding aligns with Boerman et al. (2018), which showed response efficacy rather than self-efficacy predicted the intention to protect online privacy. At the individual level, what average laypersons can do to protect their privacy is limited such as deleting cookies, cleaning browser history, or adjusting privacy mode. However, most of these actions cannot prevent their information from being collected; perhaps only at the corporate or government level there can be effective actions that truly protect user privacy. Therefore, our participants might believe effective techniques of privacy protection were beyond their ability (Boerman et al., 2018). Thus, self-efficacy did not mitigate the relationship between perceived inevitability and the intention to protect online privacy.

Theoretical Implications

This study extends prior research on online privacy protection in the following aspects. First, our study suggests that low psychological distance of privacy invasion could be indirectly related to and high perceived inevitability of privacy invasion could be directly related to the lowered intention to protect privacy. These results can be understood through the lens of learned helplessness, which posited that repeated negative experiences could cultivate a sense of helplessness (Maier & Seligman, 1976). Similarly, direct or indirect experiences with privacy

breaches may prompt individuals to think that Internet platforms have deprived their right of privacy (West, 2019). Thus, disengagement from online privacy protection is not a free choice. This conclusion provides additional evidence for the research on privacy fatigue and privacy cynicism (Choi et al., 2018; Hoffman et al., 2016; Lutz et al., 2020), which underscores that users have minimum agency for their privacy.

Second, our study explicates the mechanism by which individuals rationalize their disengagement from online privacy protection. According to our findings, the inaction on privacy protection can be the combined outcomes of privacy threats and lack of effective techniques of privacy protection. These variables—psychological distance and perceived inevitability of privacy invasion as well as privacy-related response efficacy—all refer to external influences beyond personal control. The only variable in our model that represents personal control is self-efficacy, which did not moderate the relationship between perceived inevitability and the intention. Thus, perhaps personal efforts to protect privacy make very little difference. Frequent threats and lack of effective preventive methods deprive average individuals' agency, which again confirms prior research on privacy fatigue and privacy cynicism (Choi et al., 2018; Hoffman et al., 2016; Lutz et al., 2020).

Finally, it is necessary to discuss how our findings are distinct from privacy fatigue and privacy cynicism. In addition to providing a theory-based explanation about how rationalization of privacy protection disengagement happens, this study is distinct from privacy fatigue and privacy cynicism in terms of how a passive attitude towards privacy protection forms. Empirical research suggests that lack of self-efficacy in mitigating online privacy threats may be an important predictor of privacy fatigue and privacy cynicism (Lutz et al., 2020; van Der Schyff et al., 2023). For example, Lutz et al. (2020) found that Internet skill was negatively related to privacy cynicism. Although Internet skill is not equivalent to self-efficacy, it still represents one's ability to control the privacy issue. Similarly, limited knowledge, skills, or user control over their data was consistently identified as a predictor of privacy fatigue (van Der Schyff et al., 2023). However, our results show that privacy threats alone were positively related to perceived inevitability. Given our models did not examine the relationship between response/self-efficacy and perceived inevitability, we conducted post-hoc analyses[2], which revealed that both types of psychological distance were more strongly related to perceived inevitability compared to response efficacy and self-efficacy. In other words, even when self-efficacy was considered, psychological distance of privacy threats still exhibited a significant and strong relationship with perceived inevitability. Of course, stronger evidence is needed to systematically compare how threat-related variables and self-efficacy are associated with privacy fatigue and privacy cynicism. Nevertheless, our result suggests that frequent privacy threats are likely the key factor that shape passive attitude towards privacy protection and increasing self-efficacy may not be sufficient to encourage individuals to protect their privacy.

Practical Implications

Our results highlight the important role that high response efficacy plays in mitigating the relationship between perceived inevitability and the intention to protect online privacy. Thus, education and campaigns should aim at improving individuals' response efficacy in online privacy protection. For example, education and campaigns should teach individuals how to protect their online privacy and explain why these methods are effective.

Limitations

This study has several limitations worth noting. First, the cross-sectional nature of this study makes it impossible to establish causal claims. Self-report measures also limit the validity of our measures. Future research should consider experiments, particularly manipulating psychological distance, to establish causality and measure actual behaviors.

Second, our sample is convenience in nature, which can limit the validity of our findings. Third, our study was conducted within a sample of Chinese users of e-commerce platforms. As mentioned earlier, Chinese netizens were more positive about algorithms than Americans (Xing et al., 2023). Thus, this can threaten the generalizability of our results.

Next, we limited our investigation to e-commerce platforms only. However, we focus on how individuals respond to privacy invasion caused by algorithms, which are widely used by other Internet-based platforms to collect user information. Therefore, low psychological distances and high perceived inevitability of online privacy invasion should apply to most Internet-based platforms. Although this may ensure the external validity of our

findings, future research is needed to replicate our findings in other Internet-based platforms that leverage algorithms.

In addition, following prior research (Laurin, 2018; Laurin et al., 2012), this study used the intention as the proxy for rationalization. However, future work should develop direct and more robust measure of rationalization.

Finally, we adapted the measure of psychological distance in the environmental (Spence et al., 2011) and educational contexts (Sanna et al., 2006) to the current research context. However, several issues related to our measures need to be noted. Specifically, we did not include a concrete example of privacy violation, which could make the statement abstract. Moreover, the items included expressions related to other types of psychological distance. For example, in the items measuring temporal distance, there are expressions suggesting hypotheticality (i.e., it seems) and social distance (i.e., your privacy). As a result, the measures can be compounded with other types of psychological distance. Thus, while our findings provide preliminary evidence demonstrating how perceived inevitability, psychological distance, and efficacy beliefs were related to online privacy management, future research needs to retest our findings through validated measures.

Future Directions

In addition to addressing these limitations, future research can extend this study in the following aspects. First, as mentioned above, it is necessary to compare how threat-related variables versus efficacy-related variables are associated with one's attitude towards and intention for privacy protection. This research can provide better understanding about how this disengagement from online privacy protection forms, no matter whether it is privacy fatigue, privacy cynicism, or perceived inevitability of privacy invasion.

Second, this study, along with privacy fatigue and privacy cynicism, all focus on explaining how individuals rationalize disengagement from online privacy protection. However, individuals may also rationalize privacy invasion. Specifically, as rationalization is essentially a process of self-persuasion with the goal of improving one's appraisal of the current situation (Laurin et al., 2012), individuals may view privacy invasion from another perspective which reminds them of the potential benefits that sacrificing privacy can bring such as tailored recommendations (Fast & Jago, 2020). Hence, future research should consider examining how perceived benefits of privacy loss are related to privacy protection disengagement and exploring whether it moderates the effect of other variables such as perceived inevitability.

Additionally, Laurin et al. (2012) proposed that rationalization versus reactance were two opposite responses to external threats. Our results also suggest that low psychological distance of privacy threats can exhibit a negative direct relationship with the intention to protect privacy but can also be indirectly related to the intention positively. Therefore, future research should examine the boundary between rationalization versus reactance of privacy invasion. Theories like protection motivation theory (Rogers, 1975) and extended parallel process model (Witte, 1992) distinguish the adaptive versus maladaptive responses to health threats. Future research can employ these theories to delineate the boundary condition of rationalization versus reactance in the context of online privacy protection[3].

Finally, while this study focuses on individual-level variables related to disengagement from online privacy protection, future research can extend the investigation to other levels and examine the role that interpersonal, cultural, technological, economic, and political factors play in this process (Draper et al., 2024; Hoffman et al., 2024). Indeed, recent research has investigated how companies deal with the rising demand for privacy (McGuigan et al., 2024). Furthermore, how the interplay between individuals, platforms, and the government affects privacy management is another important direction worthy investigations (Martin et al., 2023; Zhu, 2024).

Conclusion

The current research represents a response to the increased events of privacy breaches. Our results demonstrate that individuals may disengage from online privacy protection because they perceive that privacy invasion is close to them and thereby inevitable and they do not believe there is any effective measure mitigating this threat. Thus, disengagement from online privacy protection is a passive reaction to the increasing external privacy threats which deprive individuals' agency in their personal data.

Footnotes

[1]The hypotheses were updated after data collection in line with the reviewers' suggestion. Originally, we proposed that temporal/social distances moderated the relationship between perceived inevitability and the intention to protect online privacy. In the first round of revision, the reviewer suggested changing it to the current hypothesis given the correlation between psychological distance and perceived inevitability.

[2]We regressed perceived inevitability on psychological distance, response efficacy and self-efficacy, controlling for sex, age, education, income, frequency of using e-commerce platforms and user intensity. Given the high correlation between temporal distance and social distance (r = .82, p < .001), we put them in separate regression models to prevent multicollinearity. Temporal distance (β = −.51, p < .001) and self-efficacy (β = −.24, p < .001) were significantly associated with perceived inevitability. Similarly, social distance (β = −.56, p < .001) and self-efficacy (β = −.21, p < .001) were significantly associated with perceived inevitability. Response efficacy was not related to perceived inevitability in either model (temporal distance: p = .616, social distance: p = .522). Furthermore, results of z-tests comparing the standardized coefficients between temporal/social distance and self-efficacy show that the relationship between temporal (z = 3.75, p < .001)/social distance (z = 4.99, p < .001) and perceived inevitability was significantly stronger than the contribution of self-efficacy to perceived inevitability.

[3]A post-hoc analysis was conducted through Process Macro 5.0 to investigate whether there was a three-way interaction between perceived inevitability, response efficacy, and self-efficacy on the intention to protect online privacy. Results confirmed that this three-way interaction was significant (β = .32, p = .003) such that only at a high level of self-efficacy, response efficacy moderated the relationship between perceived inevitability and the intention (β = .20, p = .005). Specifically, among individuals exhibiting low response efficacy and low self-efficacy, perceived inevitability was negatively associated with the intention (β = −.20, p = .009), suggesting that rationalization tends to occur when individuals do not think there are effective measures against privacy threats and they have the ability to manage their privacy. Conversely, for high response efficacy and high self-efficacy, perceived inevitability was positively related to the intention to protect privacy (β = .25, p < .001), which suggests a sign of reactance due to heightened levels of efficacy appraisal.

Conflict of Interest

The authors have no conflicts of interest to declare.

Use of AI Services

The authors declare they have not used any AI services to generate any part of the manuscript or data.

Data Availability Statement

The data of this study are available through https://figshare.com/s/572dc9b59082f1a88d97.

Authors' Contribution

Jian Raymond Rui: conceptualization, methodology, project administration, writing—original draft. **Jingzhong Xie:** formal analysis, investigation,, writing—review & editing.

Acknowledgement

This work was supported by China Postdoctoral Science Foundation [Certificate Number: 2023M743936].

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Boerman, S.C., Kruikemeier, S., & Zuiderveen Borgesius, F.J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Cho, H. (2024). The interplay of rational evaluation and motivated reasoning in privacy helplessness: An integrative approach. *Big Data & Society, 11*(1). https://doi.org/10.1177/20539517241237485

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Chung, J., & Kwon, H. Y. (2025). Privacy fatigue and its effects on ChatGPT acceptance among undergraduate students: Is privacy dead? *Education and Information Technologies, 30*(9), 12321–12343. https://doi.org/10.1007/s10639-024-13198-6

China Internet Network Information Center. (2024). *The 53rd Statistical Report on China's Internet Development.* https://www.cnnic.net.cn/NMediaFile/2024/0325/MAIN1711355296414FIQ9XKZV63.pdf

Cooper, J. (2007). *Cognitive dissonance: Fifty years of a classic theory.* Sage. https://doi.org/10.4135/9781446214282

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Draper, N. A., Hoffman, C. P., Lutz, C., Ranzini, G., & Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. *Big Data & Society, 11*(3). https://doi.org/10.1177/20539517241270663

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Fast, N. J., & Jago, A. S. (2020). Privacy matters… or does it? Algorithms, rationalization, and the erosion of concern for privacy. *Current Opinion in Psychology, 31,* 44–48. https://doi.org/10.1016/j.copsyc.2019.07.011

Festinger, L. (1957). *A theory of cognitive dissonance.* Stanford University Press.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737–3757. https://ijoc.org/index.php/ijoc/article/view/4655/1738

Ho, S., Lwin, M. O., Yee, A. Z. H., & Lee, E. W. J. (2017). Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 572–579. https://doi.org/10.1089/cyber.2017.0061

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), Article 7. https://doi.org/10.5817/cp2016-4-7

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2024). Inequalities in privacy cynicism: An intersectional analysis of agency constraints. *Big Data & Society, 11*(1). https://doi.org/10.1177/20539517241232629

Jost, J. T. (2019). A quarter century of system justification theory: Questions, answers, criticisms, and societal applications. *British Journal of Social Psychology*, *58*(2), 263–314. https://doi.org/10.1111/bjso.12297

Jost, J. T., Banaji, M. R., & Nosek, B. A. (2004). A decade of system justification theory: Accumulated evidence of conscious and unconscious bolstering of the status quo. *Political Psychology, 25*(6), 881–919. https://doi.org/10.1111/j.1467-9221.2004.00402.x

Kay, A. C., Gaucher, D., Peach, J. M., Laurin, K., Friesen, J., Zanna, M. P., & Spencer, S. J. (2009). Inequality, discrimination, and the power of the status quo: Direct evidence for a motivation to see the way things are as the way they should be. *Journal of Personality and Social Psychology, 97*(3), 421–434. https://doi.org/10.1037/a0015997

Kay, A. C., & Zanna, M. P. (2009). A contextual analysis of the system justification motive and its societal consequences. In J.T. Jost, A.C. Kay, & H. Thorisdottir (Eds.), *Social and psychological bases of ideology and system justification* (pp. 158–181). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195320916.003.007

Kee, K., & Shin, E. (2022). Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms? *International Journal of Information Management, 65*, Article 102494. https://doi.org/10.1016/j.ijinfomgt.2022.102494

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Laurin, K. (2018). Inaugurating rationalization: Three field studies find increased rationalization when anticipated realities become current. *Psychological Science, 29*(4), 483–495. https://doi.org/10.1177/0956797617738814

Laurin, K., Gaucher, D., & Kay, A. C. (2013). Stability and the justification of social inequality. *European Journal of Social Psychology, 43*(4), 246–254. https://doi.org/10.1002/ejsp.1949

Laurin, K., Kay, A. C., & Fitzsimons, G. J. (2012). Reactance versus rationalization: Divergent responses to policies that constrain freedom. *Psychological Science, 23*(2), 205–209. https://doi.org/10.1177/0956797611429468

Laurin, K., Shepherd, S., & Kay, A. C. (2010). Restricted emigration, system inescapability, and defense of the status quo: System-justifying consequences of restricted exit opportunities. *Psychological Science, 21*(8), 1075–1082. https://doi.org/10.1177/0956797610375448

Liberman, N., & Trope, Y. (2008). The psychology of transcending the here and now. *Science, 322*(5905), 1201–1205. https://doi.org/10.1126/science.1161958

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Maier, S. F., & Seligman, M. E. (1976). Learned helplessness: Theory and evidence. *Journal of Experimental Psychology: General*, *105*(1), 3–46. https://doi.org/10.1037//0096-3445.105.1.3

Martin, Z. C., Ridel, M. J., & Woolley, S. C. (2023). How pro- and anti-abortion activities use encrypted messaging apps in post-Roe America. *Big Data & Society, 10*(2). https://doi.org/10.1177/20539517231221736

McGuigan, L., West, S. M., Sivan-Sevilla, I., & Parham, P. (2023). The after party: Cynical resignation in Adtech's pivot to privacy. *Big Data & Society, 10*(2). https://doi.org/10.1177/20539517231203665

Nestler, S., & Egloff, B. (2009). Increased or reversed? The effect of surprise on hindsight bias depends on the hindsight component. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 35*(6), 1539–1544. https://doi.org/10.1037/a0017006

Proudfoot, D., & Kay, A. C. (2014). Reactance or rationalization? Predicting public responses to government policy. *Policy Insights from the Behavioral and Brain Sciences, 1*(1), 256–262. https://doi.org/10.1177/2372732214550489

Pu, Y., & Chen, H. (2026). Power imbalance between platforms and users: An exploration of privacy apathy towards platform surveillance. *Behavior & Information Technology*, *45*(13), 3164–3180. https://doi.org/10.1080/0144929x.2026.2614049

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sanna, L. J., Chang, E. C., Carter, S. E., & Small, E. M. (2006). The future is now: Prospective temporal self-appraisals among defensive pessimists and optimists. *Personality and Social Psychology Bulletin, 32*(6), 727–739. https://doi.org/10.1177/0146167205285896

Spence, A., Poortinga, W., & Pidgeon, N. (2011). The psychological distance of climate change. *Risk Analysis, 32*(6), 957–972. https://doi.org/10.1111/j.1539-6924.2011.01695.x

van Der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: A scoping review and research agenda. *Future Internet*, *15*(5), Article 164. https://doi.org/10.3390/fi15050164

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2024). Privacy cynicism and its role in privacy decision-making. *Communication Research*, *51*(2), 146–177. https://doi.org/10.1177/00936502211060984

Wang, Z., Maalla, A., & Liang, M. (2021, December). Research on e-commerce personalized recommendation system based on big data technology. In *2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)* (Vol. 2, pp. 909–913). IEEE. https://doi.org/10.1109/ICIBA52610.2021.9688086

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317–342. https://doi.org/10.1080/108107396127988

Xing, Y., He, W., Zhang, J. Z., & Cao, G. (2023). AI privacy opinions between US and Chinese people. *Journal of Computer Information Systems*, *63*(3), 492–506. https://doi.org/10.1080/08874417.2022.2079107

Yu, L., He, L., Du, J., & Wu, X. (2024). Protection or cynicism? Dual strategies for coping with privacy threats. *Information Systems Frontiers*, *27*(4), 1507–1527. https://doi.org/10.1007/s10796-024-10531-9

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management, 55*(4), 482–493. https://doi.org/10.1016/j.im.2017.11.003

Zhang, X., Tian, X., & Han, Y. (2022). Influence of privacy fatigue of social media users on their privacy protection disengagement behavior: A PSM-based analysis. *Journal of Integrated Design and Process Science*, *25*(1), 78–92. https://doi.org/10.3233/jid200015

Zhu, Y. (2024). Privacy cynicism and diminishing utility of state surveillance: A natural experiment of mandatory location disclosure on China's Weibo. *Big Data & Society, 11*(2). https://doi.org/10.1177/20539517241242450

About Authors

Jian Raymond Rui is a professor at the School of Journalism and Communication at South China University of Technology. His research interests focus on the intersection between technology and health persuasion.

https://orcid.org/0000-0001-5521-5680

Jingzhong Xie is an assistant professor in the School of Journalism and Cultural Communication at Zhongnan University of Economics and Law. His research interests lie in new media and society, and health communication.

https://orcid.org/0000-0002-9204-4160

Correspondence to
Jingzhong Xie, 182 Nanhu Rd, Wuhan, Hubei Province, China, 430073, xjzhong1989@163.com

© Author(s). The articles in Cyberpsychology: Journal of Psychosocial Research on Cyberspace are open access articles licensed under the terms of the Creative Commons BY-SA 4.0 International License which permits unrestricted use, distribution and reproduction in any medium, provided the work is properly cited and that any derivatives are shared under the same license.