MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Wang, L. H., Dienlin, T., & Metzger, M. J. (2026). Disentangling the paradox of the privacy paradox on social media: The role of privacy dimensions, perceived benefits, privacy self-efficacy, and privacy cynicism. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 20*(4), Article 5.
https://doi.org/10.5817/CP2026-4-5

Disentangling the Paradox of the Privacy Paradox on Social Media: The Role of Privacy Dimensions, Perceived Benefits, Privacy Self-Efficacy, and Privacy Cynicism

Laurent H. Wang[1], *Tobias Dienlin*[2], *& Miriam J. Metzger*[3]

[1] Stan Richards School of Advertising and Public Relations, Moody College of Communication, University of Texas at Austin, Austin, USA
[2] Department of Communication and Media Research, University of Zurich, Zurich, Switzerland
[3] Department of Communication, University of California, Santa Barbara, USA

Abstract

This study extends research on the 'privacy paradox' to the horizontal (privacy vis-à-vis peers) and vertical (privacy vis-à-vis institutions) dimensions of privacy on social media, and tests perceived benefits, privacy self-efficacy, and privacy cynicism as moderating factors for the privacy paradox on both dimensions. A cross-sectional online survey with a sample of U.S. adult social media users (N = 1,398) revealed no evidence for the privacy paradox on either the horizontal or the vertical privacy dimension (i.e., privacy concerns were positively associated with privacy management behaviors). Interestingly, perceived benefits and privacy cynicism moderated the relationships between privacy concerns and privacy management behaviors, though in the opposite direction to our prediction. In particular, the positive relationship between privacy concerns and privacy management behaviors was stronger among those with higher perceived benefits on the vertical dimension, and among those with higher privacy cynicism on both the horizontal and vertical dimensions. On the other hand, privacy self-efficacy was not a significant moderator on either dimension. Results demonstrate the multidimensional nature of online privacy and highlight the impact of conceptual and operational decisions on "finding" the privacy paradox.

Keywords: privacy paradox; horizontal/vertical privacy; privacy self-efficacy; privacy cynicism; social media

Editorial Record

First submission received:
July 9, 2025

Revisions received:
December 20, 2025
June 20, 2026

Accepted for publication:
June 23, 2026

Editor in charge:
Lenka Dedkova

Introduction

Despite concerns about privacy as a result of using communication technology, many people do not enact strategies to protect their privacy online. This concern-behavior discrepancy in online privacy—called the privacy paradox—suggests that privacy concerns do not necessarily translate into privacy management behaviors (Acquisti & Gross, 2006; Tufekci, 2008). The privacy paradox has garnered massive scholarly attention (see Dienlin et al., 2023; Kokolakis, 2017; Masur, 2023 for a review). While some studies support the existence of a paradox (e.g., Reynolds et al., 2011; Xu & Li, 2022; Vimalkumar et al., 2021), others instead find a positive relationship between privacy concerns and privacy management behaviors (Baruh et al., 2017; Dienlin & Trepte, 2015). We

argue that understanding these inconsistencies requires adopting more refined conceptualizations and operationalizations of key privacy concepts and uncovering patterns of when the privacy paradox may be more or less likely to be observed.

This study contributes to privacy paradox research in some important ways. We draw from the integrated model of online privacy (Bazarova & Masur, 2020) to conceptualize privacy concerns and privacy management behaviors on both the horizontal (i.e., privacy vis-à-vis peers) and vertical (i.e., privacy vis-à-vis institutions) dimensions of privacy. Testing evidence for the privacy paradox on these dimensions allows for a more nuanced understanding of this phenomenon. In addition, we test perceived benefits, privacy self-efficacy, and privacy cynicism as moderating factors for the privacy paradox on both dimensions. Finally, we situate privacy in the context of social media to recognize the contextual dependency of privacy (i.e., privacy attitudes and behaviors change as context shifts; Nissenbaum, 2010).

Empirical Evidence on the Privacy Paradox

Early privacy paradox research claims that people are willing to compromise their personal information for relatively small rewards (Acquisti & Gross, 2006; Tufekci, 2008). For example, Brown (2001) found that people were willing to have their personal information tracked by online retailers for financial gain. Tufekci (2008) also found little relationship between privacy concerns and information disclosure on Facebook and Myspace among college students. More recently, in line with the privacy paradox, Barth et al. (2019) experimentally demonstrated that participants were not motivated to take privacy-protective actions, despite high privacy concerns. Similarly, in the context of AI voice assistants, Xu and Li (2021) showed that increased privacy concerns were not associated with decreased self-disclosure behavior, and Vimalkumar et al. (2021) found that privacy concerns about voice-based digital assistants were not significantly related to users' adoption intentions. These findings suggest that, to date, the privacy paradox is still of scholarly interest and has received some supporting evidence.

Refuting the notion of the privacy paradox are findings of a positive relationship between privacy concerns and privacy management behaviors by research that uses cross-sectional and longitudinal surveys (e.g., Dienlin et al., 2023; Dienlin & Metzger, 2016; Krasnova et al., 2010), meta-analysis (Baruh et al., 2017; Kim et al., 2023), specification curve analysis (Masur, 2023), and systematic literature review (Memarian et al., 2025; Kokolakis, 2017). For example, using three-wave longitudinal survey data, Dienlin et al. (2023) found that people who were more concerned about privacy than others shared less personal information, and people who were more concerned than before shared less information than before, providing evidence against the privacy paradox at both the between-person and within-person levels. Kim et al.'s (2023) meta-analysis also showed that privacy concerns were positively associated with both privacy protection intentions and actual privacy protection behaviors. Some scholars thus concluded that "the evidence for a pronounced paradox appears to be weakening over time" (Hoffmann et al., 2016, p. 3) and that the privacy paradox "can be considered a relic of the past" (Dienlin & Trepte, 2015, p. 295).

Researchers attribute contradictory findings for the privacy paradox to various conceptual and operational decisions made regarding key privacy variables. These decisions include, for example, the operationalizations of privacy behaviors (e.g., self-disclosure vs. privacy management strategies) and personal information (e.g., name, age, social security number), research methodology (e.g., surveys vs. experiments), the digital context being studied (e.g., social media vs. e-government services), data types (e.g., self-report vs. log data), sample characteristics (e.g., gender, culture, age), and the inclusion of control variables (Baruh et al., 2017; Masur, 2023; Memarian et al., 2025; Kim et al., 2023; Kokolakis, 2017).

One other factor that has received increasing scholarly attention is the alignment between measures of privacy concerns and management behaviors. Dienlin and Trepte (2015) point out that early privacy paradox studies tended to predict specific privacy behaviors (e.g., using a real name online) using general privacy concern items (e.g., "How concerned are you about your online privacy?"). This fails the principle of compatibility, which argues that the conceptualizations and measurement items should align in terms of action, target, context, and time (Fishbein & Ajzen, 2010), and thus could explain the nonsignificant relationships found. Indeed, Baruh et al. (2017) in their meta-analysis found that privacy concerns were not associated with general social media use, but were associated with specific privacy-related behavioral outcomes (e.g., information sharing, use of protective measures). Similarly, Masur's (2023) specification curve analysis showed that specific concerns about personalization based on disclosed information were stronger predictors of users' information sharing than general concerns about online behavior being recorded. These findings demonstrate how measurement

compatibility between privacy concerns and behaviors shapes the extent to which evidence may be "found" for the privacy paradox.

A Dimensionalized Approach to Conceptualizing the Privacy Paradox

One possible approach to reconciling the empirical inconsistencies that aligns with the principle of compatibility is to differentiate dimensions (i.e., aspects or types) of privacy (Dienlin, 2023; Quinn & Epstein, 2023; Masur, 2023). This is because privacy perceptions and behaviors vary depending on the audience and/or the violator, the specific platform and channel, and other factors (Nissenbaum, 2010). For instance, the level of privacy concern and the likelihood of using privacy protection strategies required to avoid identity theft on commercial websites likely differ from those of managing social media posts to avoid parental surveillance (Epstein & Quinn, 2025; Young & Quan-Haase, 2013).

The integrated model of online privacy (Bazarova & Masur, 2020) suggests a horizontal/vertical distinction corresponding to privacy threats posed by other users versus by institutions (see also Raynes-Goldie, 2010 for a similar notion of social/institutional privacy). On the horizontal dimension, people manage privacy vis-à-vis other people in online social networks. Horizontal privacy encompasses individualistic approaches that emphasize control of personal information by individuals and/or their personal network connections, for example by sharing some posts only with specific (sub-) audiences. On the vertical dimension, people manage privacy vis-à-vis institutions. Vertical privacy thus refers to personal information that may be accessed, processed, and analyzed by advertisers, marketing companies, law enforcement, government officials, and social media companies, often without user awareness.

Based on these distinctions, privacy concerns can be defined as the degree to which an individual feels risk about the collection and use of personal information online either by unintended users (e.g., family members, coworkers; i.e., horizontal concerns) or by institutions (e.g., advertisers, government agencies) (i.e., vertical concerns; Masur & Trepte, 2021). Privacy management behaviors can be defined as the use of privacy protection strategies against peer privacy invasions (e.g., creating separate disclosure lists, blocking users; horizontal strategies) and against institutional surveillance (e.g., opting out from personalized advertising, using pseudonyms when signing up for website accounts; vertical strategies; Epstein & Quinn, 2020).

We adopt this horizontal/vertical distinction to analyze the privacy paradox, as the concern-behavior relationship may vary vis-à-vis different audiences for personal information. Research indeed suggests that users distinguish horizontal and vertical privacy threats when evaluating online privacy risks. For example, using topic modeling of social media users' definitions of privacy, Quinn et al. (2019) found that users' understanding of privacy tends to emphasize horizontal over vertical phenomena. Hargittai and Marwick (2016) similarly found that their interviewees' risk awareness was stronger on the horizontal than the vertical dimension (see also Young & Quan-Haase, 2013). In contrast, as consumers accumulate knowledge about institutional privacy risks, other research found that users reported higher institutional privacy concerns than social concerns (Auxier et al., 2019; Gruzd et al., 2018; Lutz & Newlands, 2021; Lutz & Ranzini, 2017; Petro & Gonzales, 2025). Nonetheless, these findings demonstrate the utility of distinguishing horizontal/vertical privacy to gain more nuanced insights into the privacy paradox phenomenon.

Social Media as the Context

The privacy paradox has been researched across different digital contexts, such as social media, mobile apps, e-commerce, personalized advertising, and the Internet (Kim et al., 2023; Kokolakis, 2017; Masur, 2023; Memarian et al., 2025). The importance of context in privacy research is well-established, as it shapes the types of personal information shared (e.g., health records, location data), the audiences who access it (e.g., peers, institutional actors), the regulatory mechanisms available for information protection, technological affordances (e.g., anonymity, editability), and community norms that facilitate or constrain privacy protection (King et al., 2026; Lin & Wang, 2026; Nissenbaum, 2010). The extent to which privacy concerns translate into protection behaviors may thus differ based on the contextual parameters being taken into consideration (Kokolakis, 2017). Specifying the context also allows us to abide by the principle of compatibility and ensure the alignment of privacy concern and behavior measurements. Indeed, Kim et al. (2023) in their meta-analysis found that the technological context moderated the positive relationship between privacy concerns and risk perceptions; this relationship was strongest for social media, followed by mobile apps, e-commerce, and the Internet.

We focus on the social media context for several reasons. Unlike other contexts where privacy risks dominate on one dimension (e.g., vertical risks for targeted advertising), on social media users need to simultaneously manage both horizontal and vertical privacy threats. For example, when posting sensitive information on X (formerly Twitter), users may need to make sure that their content is only visible to a certain group of people (horizontal privacy) and/or will not cause trouble due to government surveillance (vertical privacy) (Marwick et al., 2017). In addition, users constantly negotiate competing tensions between privacy protection and self-disclosure given various benefits and costs on social media (Dienlin & Metzger, 2016), whereas in other contexts such as e-government services, the need for information sharing may be more salient, thus making privacy behavior less "paradoxical" (Memarian et al., 2025). Finally, empirical studies that adopt a dimensionalized approach to study the privacy paradox on social media are still limited (discussed below), thus warranting more research.

Testing the Privacy Paradox on the Horizontal and Vertical Dimensions

In response to increasing scholarly interest in a dimensionalized approach, research has started to test the privacy concern-behavior relationship on the horizontal and vertical dimensions. For example, Epstein and Quinn (2025) demonstrated that privacy concerns are positively correlated with privacy protection behaviors on both the horizontal and vertical dimensions, thus refuting the privacy paradox. However, many of their measurement items are operationalized in the general internet context (e.g., use encryption software for email) and thus are not applicable to social media. Gruzd and Hernández-García (2018) distinguished concerns about social (i.e., horizontal) and organizational (i.e., vertical) privacy threats on social media and found that both negatively predicted the amount and depth of self-disclosure. Similarly, Schwartz-Chassidim et al. (2020) found that both social and institutional privacy concerns predicted more frequent change of privacy settings on social media, and that social concerns were a stronger predictor than institutional concerns. While informative, these studies do not distinguish privacy protection strategies on the horizontal and vertical dimensions. Their focus on self-disclosure or privacy settings adjustments also does not capture the wider range of privacy protection mechanisms available. Finally, though not in social media, Lutz and Newlands (2021) demonstrated that both social and institutional privacy concerns about smart speakers positively predicted the use of technical strategies (e.g., turning off the speaker when having private conversations) and data strategies (e.g., deleting device recordings), and social privacy concerns additionally predicted the use of social strategies (e.g., moderating language around the speaker). In sum, empirical evidence seems to suggest a positive concern-behavior relationship on both the horizontal and vertical privacy dimensions, although a comprehensive investigation in the specific context of social media is still limited. Based on our review above and guided by the principle of compatibility (Fishbein & Ajzen, 2010), we pose:

H1: Horizontal privacy concerns will be positively correlated with horizontal privacy management behaviors on social media.

H2: Vertical privacy concerns will be positively correlated with vertical privacy management behaviors on social media.

Testing Moderating Factors for the Privacy Paradox

The second goal of this research is to investigate moderating factors for the privacy paradox on social media. Masur (2023) argued that researchers should shift their focus away from (dis)proving the privacy paradox, and instead toward potential explanations or moderators for this attitude-behavior discrepancy (see also Kim et al., 2023; Kokolakis, 2017). Indeed, Hoffmann et al. (2016) claimed that the privacy paradox might be more salient *when* people a) see greater benefits over privacy risks, b) lack literacy, skills, and efficacy, and c) develop a sense of subjective futility over privacy protection (see also Epstein & Quinn, 2025). Thus, in response to Masur's (2023) call and following Hoffmann et al.'s (2016) suggestion, we empirically test perceived benefits, privacy self-efficacy, and privacy cynicism as moderators of the privacy paradox on both horizontal and vertical privacy dimensions. Studying these moderators also has practical implications, as it allows us to identify potential cues that can be incorporated in technology and intervention designs to strengthen the concern-behavior relationship. For example, privacy nudge designs could be incorporated to highlight potential privacy risks in addition to benefits, if perceived benefits are found to weaken the concern-behavior relationship, and hope appeals could be used to enhance efficacy, combat privacy cynicism, and motivate privacy protection if self-efficacy and privacy cynicism significantly moderate this relationship (see Wang et al., 2026).

Perceived Benefits

Perceived benefits of self-disclosure refer to positive attributes people make about revealing personal information on social media (Krasnova et al., 2010). Although not yet explicitly studied in the literature, perceived benefits can be mapped onto the horizontal (e.g., social support, capital building) (Dienlin & Metzger, 2016) and vertical dimensions of privacy (e.g., tailored content, monetary rewards; Bol et al., 2018) on social media.

The privacy calculus model holds that people are likely to self-disclose when perceived benefits outweigh perceived risks (Dienlin & Metzger, 2016). Empirical research on the privacy calculus tends to examine perceived benefits and risks as independent predictors of behavioral outcomes (see Meier et al., 2023). For example, Krasnova et al. (2010) found that the benefits of relationship-building and enjoyment positively predicted the amount of information shared on social media. Dienlin and Metzger (2016) demonstrated that perceived (horizontal) benefits on Facebook were a stronger predictor of self-disclosure than privacy concerns (see also Kezer et al., 2022). In the context of personalized search engines, Bol et al. (2018) found that perceived (vertical) benefits led to self-disclosure intention.

More recently, however, scholars argue that perceived benefits and privacy concerns should be studied in tandem with each other, and that the interaction of both factors should paint a more accurate picture of how the "risk-benefit calculus" guides online privacy decisions (Meier et al., 2023; see also Wang, Arch, et al., 2025). In particular, Meier et al. (2023) found that at the within-person level, perceived benefits of using a COVID-19 contact tracing app and privacy concerns interacted to impact German people's likelihood of using the app, such that high privacy concerns decreased the positive relationship between benefits and app use, and that high perceived benefits decreased the negative relationship between privacy concerns and app use. Applying this logic to the privacy paradox, perceived benefits should play a moderating role in the concern-behavior relationship, as perceived benefits may undermine the impact of privacy concerns on privacy management behaviors. To further advance our theoretical understanding, we test these relationships on both the horizontal and vertical dimensions of social media privacy:

H3: Perceived benefits will moderate the relationship between privacy concerns and privacy management behaviors on the (a) horizontal and (b) vertical dimensions of privacy on social media, such that the concern-behavior relationship will be weaker among people who perceive more benefits on both dimensions.

Privacy Self-Efficacy

Online privacy self-efficacy describes users' confidence in their own ability to protect their privacy online (van Ooijen et al., 2024). It dictates the amount of control individuals perceive to have over their personal information vis-à-vis other social media users (i.e., horizontal efficacy) and/or institutions (i.e., vertical efficacy), and can motivate privacy management behaviors.

Protection motivation theory (PMT, Rogers, 1983) suggests that in online privacy, appraisals of a privacy threat (e.g., perceived severity and vulnerability) and coping potentials (e.g., self-efficacy) interact to impact individuals' likelihood to engage in privacy management behaviors. Specifically, Rogers (1983) posited that the effect of threat appraisal on protection motivation is dependent on levels of coping appraisal. That is, at high levels of coping appraisal, threat appraisal will have a main effect on behavioral intention; at low levels of coping appraisal, threat appraisal will either have no effect or reduce behavioral intention (Rogers, 1983, p. 170). Extending this logic to online privacy, the effect of privacy concerns on privacy management behavior will likely be dependent on levels of privacy self-efficacy, and it is possible to observe a privacy paradox only at low levels of privacy self-efficacy. Thus privacy self-efficacy should moderate the relationship between privacy concerns and privacy management behaviors.

Extant research has demonstrated a direct relationship between privacy self-efficacy and privacy management behaviors (Chen, 2018; Dienlin & Metzger, 2016; van Ooijen et al., 2024). However, less attention has been paid to the moderating role of privacy self-efficacy in understanding the privacy paradox, and the very few existing studies have produced mixed evidence. For example, Chen and Chen (2015) found that on the horizontal dimension, privacy self-efficacy heightened the effect of privacy concerns on privacy protection (operationalized as less friending behaviors) on social media. Conversely, in the context of smart speaker use, Kang and Oh (2023) demonstrated that the main effects of privacy risk perceptions on a range of privacy boundary management behaviors *weakened* at higher levels of privacy self-efficacy. This finding suggests that high confidence in privacy

protection facilitated an optimistically biased risk perception and could potentially contribute to a privacy paradox. Such conflicting evidence thus calls for more investigations of privacy self-efficacy as a moderator for the privacy paradox. Therefore, we pose the following:

RQ1: Does privacy self-efficacy moderate the relationship between privacy concerns and privacy management behaviors on both a) the horizontal and b) the vertical privacy dimensions on social media, and if so, how?

Privacy Cynicism

Privacy cynicism is a cognitive coping mechanism for users to deal with the imbalance between high privacy concerns and (lack of) privacy protection behaviors, and privacy-cynical individuals tend to render privacy management behaviors as cumbersome and futile in the face of (vertical) privacy threats posed by online service providers, companies, and other institutions (Hoffmann et al., 2016). It is conceptualized to encompass users' mistrust, uncertainty, powerlessness, and resignation with regard to vertical privacy (Lutz et al., 2020).

Hoffmann et al. (2016) proposed that the effect of privacy concerns on privacy management behaviors might be weaker among highly privacy-cynical individuals, who attempt to avoid cognitive dissonance due to a lack of protective behaviors. Privacy cynicism might thus serve as a moderator of the privacy paradox on the vertical dimension. Drawing from the PMT, van Ooijen et al. (2024) found that the positive relationship between perceived vulnerability of data breaches and privacy protection behaviors among less privacy-cynical individuals turned negative for more cynical individuals, thereby confirming the moderating role of privacy cynicism in understanding the privacy paradox.

Further, although privacy cynicism is conceptually rooted in the vertical privacy dimension (e.g., data/surveillance capitalism), Lutz et al. (2020) argued that horizontal and vertical privacy pressures tend to interact with and impact each other in the digital environment (see also Epstein & Quinn, 2025). For example, fear of institutional data collection may impede social interactions. It is possible that privacy cynicism applies to the horizontal dimension of privacy and moderates the concern-behavior relationship on that dimension too. Moreover, as research on privacy cynicism is still developing, most studies focus on the general internet context rather than social media (e.g., van Ooijen, 2024). To fill these gaps, we pose the following:

H4: Privacy cynicism will moderate the relationship between vertical privacy concerns and vertical privacy management behaviors on social media, such that the concern-behavior relationship will be weaker among people who report higher levels of privacy cynicism.

RQ2: Does privacy cynicism moderate the relationship between horizontal privacy concerns and horizontal privacy management behaviors on social media, and if so, how?

Methods

Upon IRB approval, we administered an online survey between February and April 2023 through Qualtrics XM's Research Panel.[1] Participants were compensated based on their panel membership agreement. To qualify for participation, a panel member must be a U.S. social media user and indicate their commitment to providing high-quality responses. Participants who straight-lined the questions, sped through the survey in less than five minutes, and failed the attention check were excluded from the final dataset during our data cleaning. Missing data analyses showed that only 45 data points were missing (0.051%). Hence, no data were imputed, and missing data were treated with casewise deletion. We additionally checked for response patterns using the autocorrelation screening method (Gottfried et al., 2022). Confirmed by visual inspection, three cases showed clear response patterns and were removed, resulting in a final sample of 1,398 participants (average completion time: 17.50 minutes). See Table 1 for descriptives of the final sample used for the analysis. For more detailed information on data cleaning and analysis, see the Open Science Foundation (OSF) site: https://osf.io/ufpcw.

Table 1. *Sample Descriptives.*

Characteristic	Sample descriptives
Age	Mean: 41.31 years old Standard deviation: 16.40 years old Range: 18 to 101 years old
Gender/sex identity	60.6% Female (*n* = 847) 39.0% Male (*n* = 545) .4% Non-binary (*n* = 6)
Income	Mean: Between $55,000 and $64,999 Range: Under $5,000 to $200,000 and over
Education	Median: Associate degree in college (2-year) Range: Less than a high school degree to professional degree
Race and ethnicity	25.3% Black, African, or African American (*n* = 354) 20.0% Hispanic, Latina/Latino, Latine, or Latinx (*n* = 280) 25.6% White (*n* = 358) 15.4% East Asian (*n* = 215) 4.1% South East Asian (*n* = 58) 3.4% South Asian (*n* = 47) 1.1% Native Hawaiian or Other Pacific Islander (*n* = 16) .1% Native American, American Indian, or Alaskan Native (*n* = 2) .3% Middle Eastern or North African (*n* = 4) .2% Other (*n* = 3) 4.5% Mixed race/ethnicity (*n* = 61)
Time spent on social media per day	Mean: 5.43 hours Standard deviation: 4.91 hours Range: 0 to 24 hours
Frequency of updating social media	Median: About once or twice a month Range: Never to several times a day

Data Analysis

The reliability and factorial validity of all variables were tested and confirmed using confirmatory factor analyses (CFA) (see Table 2). In case of misfit, for each variable we carefully inspected modification indices and residual covariances, and after adding correlated residuals among items, all variables demonstrated adequate model fit indices (see OSF). Discriminant validity was assessed using the Fornell-Larcker criterion, according to which the square root of the Average Variance Extracted (AVE) for each latent variable must exceed the highest correlation with any other variable. This was the case for all variables except vertical privacy management behavior, which as expected correlated substantially with horizontal privacy management behavior (r = .68), thereby supporting convergent validity. For the subsequent analyses, we used the variables' factor scores derived from the CFA to increase precision. Several constructs were expected to correlate substantially (e.g., horizontal and vertical concerns). Analyzing them in the same multiple regression or structural equation model would result in multicollinearity (Vanhove, 2021). For example, when including both horizontal and vertical concerns in the same model, we would estimate the influence of horizontal concerns on privacy protection *independent* from vertical concerns (or vice versa), which diverges from our research question and may yield misinterpreted coefficients (Vanhove, 2021). As a result, the relationships (e.g., horizontal and vertical privacy paradox) were analyzed in separate regression models. Inspection of bivariate relations (see Table 3) suggested certain constructs are correlated (e.g., horizontal concerns and vertical concerns, r = .63, p < .001), as expected. Effects were considered significant if the p-value was smaller than .05. For all models, the assumption of normally distributed residuals was tested using ggplots, and no violations were shown based on the plots (see OSF).

Finally, theoretical perspectives and empirical evidence suggest that the way people form privacy-related attitudes (e.g., privacy concerns, privacy self-efficacy) and enact protective strategies (e.g., privacy protection, self-disclosure) is shaped by their socioeconomic and demographic backgrounds (Epstein & Quinn, 2020; Wang, 2026; Wang & Metzger, 2024). For example, Dodel and Mesch (2018) found that younger people, men, and more educated people reported higher proficiency in their digital privacy skills than their counterparts. Park (2021) showed that better-educated, more affluent, and younger people displayed higher confidence in handling their online personal data. As a result, in all analyses we controlled for the potentially confounding effects of age, gender identity, education, and income on our outcome variables of interest (Rohrer, 2018).

Table 2. *Psychometrics of the Variables' Factor Scores and Factorial Validity of Measures.*

Measure	*M*	*SD*	Min	Max	Chisq	*df*	*p*	CFI	TLI	RMSEA [90%CI]	SRMR	Rel Ω	AVE
Privacy concerns horiz.	4.54	1.11	1.37	6.54	345.62	27	< .001	0.95	0.93	0.09 [.08, .10]	0.04	0.89	0.48
Privacy concerns vert.	4.71	1.19	1.67	6.69	63.69	7	< .001	0.99	0.97	0.08 [.06, .09]	0.02	0.87	0.57
Privacy behavior horiz.	2.42	0.85	1.22	4.69	214.99	18	< .001	0.96	0.94	0.09 [.08, .10]	0.03	0.88	0.48
Privacy behavior vert.	2.46	0.82	1.21	4.52	126.56	13	< .001	0.97	0.95	0.08 [.07, .09]	0.03	0.83	0.44
Benefits horiz.	4.82	1.11	1.47	6.73	10.27	5	.068	1.00	1.00	0.03 [.00, .05]	0.01	0.88	0.59
Benefits vert.	3.94	1.07	1.47	6.40	10.46	4	.033	1.00	0.99	0.03 [.01, .06]	0.01	0.82	0.52
Privacy efficacy horiz.	4.60	1.17	1.56	6.65	10.20	2	.006	1.00	0.99	0.05 [.01, .10]	0.02	0.85	0.63
Privacy efficacy vert.	4.01	1.31	1.41	6.71	55.16	5.00	< .001	0.99	0.98	0.08 [.07, .11]	0.02	0.90	0.66
Privacy cynicism	3.24	1.23	1.43	6.30	3.27	2.00	.195	1.00	1.00	0.02 [.00, .06]	0.02	0.81	0.59

Table 3. *Zero-Order Correlation Table.*

	Privacy concerns horiz.	Privacy concerns vert.	Privacy behavior horiz.	Privacy behavior vert.	Benefits horiz.	Benefits vert.	Privacy efficacy horiz.	Privacy efficacy vert.
Privacy concerns vert.	0.63***							
Privacy behavior horiz.	0.21***	0.21***						
Privacy behavior vert.	0.22***	0.25***	0.68***					
Benefits horiz.	0.06*	0.07*	0.20***	0.14***				
Benefits vert.	0.09***	0.03	0.23***	0.16***	0.55***			
Privacy efficacy horiz.	−0.10***	−0.05	0.22***	0.20***	0.45***	0.44***		
Privacy efficacy vert.	−0.06*	−0.07*	0.24***	0.21***	0.37***	0.53***	0.65***	
Privacy cynicism	−0.13***	−0.09***	0.08*	−0.02	0.12***	0.31***	0.19***	0.33***

Note. * $p < .05$, ** $p < .01$, *** $p < .001$

Measures

Key variables were measured based on the horizontal and vertical dimensions of privacy. Question stems prompted participants to reflect on their privacy experiences regarding different types of audiences on social media. For example, the horizontal privacy question stems asked participants to think about friends, family members, coworkers, employers, strangers, and other individual social media users that may have access to their personal information on social media. The vertical privacy question stems asked about government agencies, social media companies, advertisers, corporations, and other organizations as potential audiences. At the time of data collection, no validated measures that explicitly incorporate the horizontal/vertical privacy distinction within the social media context were available that adequately reflected the nuances our study sought to examine. Therefore, we adapted items from various existing scales used to measure social and institutional privacy threat and coping responses. Variables were measured on a 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*) unless otherwise noted. All scales demonstrated strong reliability based on Cronbach's Alpha and McDonald's Omega. A complete list of survey items can be found on the OSF site. See Table 2 for item descriptives.

Privacy Concerns

Horizontal privacy concerns included nine items adapted from Krasnova et al. (2009) to assess how concerned people were about privacy violations by peer social media users, such as: *I am concerned that someone I don't expect (e.g., a stranger, my "ex," my parents, teacher, boss) could view my social media profile.* Vertical privacy concerns included six adapted items (e.g., Auxier et al., 2019; Dinev et al., 2008; Krasnova et al., 2009) to measure concerns about institutional and organizational surveillance, such as: *It bothers me that the information in my social media profile may be used to display personalized advertising to me.*

Privacy Management Behaviors

Privacy management behaviors were measured on a 5-point Likert scale (1 = *never*, 5 = *always*) to gauge the frequency of using privacy management strategies on social media. Horizontal strategies included eight items adapted from Wang and Metzger (2023), such as: *Use an exclusive disclosure list to limit my posts to certain contacts.* Vertical strategies included seven items inspired by previous research (Marwick et al., 2017; Walker & Hargittai, 2021), such as: *Avoid posting information that may be seen as problematic by government agencies or law enforcement if they monitor my social media accounts.*

Perceived Benefits

Perceived benefits of information sharing assessed how much participants found it beneficial to share personal information on social media vis-à-vis different audiences. Horizontal benefits included five items adapted from Dienlin and Metzger (2016), such as: *It has allowed me to make new social or business contacts*. Vertical benefits included five items adapted from Bol et al. (2018) and Auxier et al. (2019), such as: *Sharing personal information with companies and advertisers on social media has made information seeking easier.*

Privacy Self-Efficacy

Privacy self-efficacy captured participants' sense of control over personal information on social media. Horizontal privacy self-efficacy included four items adapted from Dienlin and Metzger (2016), such as: *I feel confident in my ability to protect my privacy from other users by using social media's privacy settings.* Vertical privacy self-efficacy included five items adapted from Madden (2017) and Auxier et al. (2019), such as: *I feel confident in my ability to use social media without having my online behaviors tracked by advertisers or government surveillance.*

Privacy Cynicism

Research on privacy cynicism and related constructs (e.g., privacy fatigue, helplessness, apathy) is still developing. While many conceptualizations and measures exist, there is currently no consensus in terms of which measure captures these constructs most closely (see Draper et al., 2024). To avoid participant fatigue, we opted to measure privacy cynicism by adapting Choi et al.'s (2018) three-item scale, which assessed participants' lack of motivation and interest in protecting online privacy, such as: *I am not particularly motivated to protect my private information online*. This scale has been used by research that similarly tests privacy cynicism as a moderator for privacy perception-behavior relationships (van Ooijen et al., 2024). The items also closely resemble Lutz et al.'s (2018) measures of privacy resignation, which was found to be the only subdimension of privacy cynicism that negatively predicted privacy protection behavior.

Results

H1 held that horizontal privacy concerns would positively predict horizontal privacy management behaviors. Results supported this hypothesis (b = 0.17, 95% CI [0.13, 0.20], $t(1390) = 8.62$, $p < .001$; β = .22, 95% CI [.17, .27]). H2 hypothesized that vertical privacy concerns would positively predict vertical privacy management behaviors. Findings showed such a relationship indeed exists (b = 0.16, 95% CI [0.13, 0.20], $t(1390) = 9.27$, $p < .001$; β = .24, 95% CI [.19, .29]), thus supporting H2.

H3 predicted that perceived benefit would moderate the relationship between privacy concerns and privacy management behaviors on the (a) horizontal and (b) vertical dimensions of privacy, such that the effect of privacy concerns on privacy management behaviors would be weaker among people who perceive more benefits on both dimensions. On the horizontal dimension, results showed that perceived benefits did not moderate the effect of privacy concerns on privacy management (b = 0.01, 95% CI [-0.02, 0.04], $t(1388) = 0.70$, $p = .487$; β = .01, 95% CI [−.03, .06]), thus rejecting H3a. On the vertical dimension, perceived benefits *did* moderate the effect of privacy concerns on privacy management (b = 0.03, 95% CI [0.01, 0.06], $t(1388) = 2.49$, $p = .013$; β = .05, 95% CI [.01, .09]). However, contrary to the prediction, a stronger effect of concerns on privacy behaviors was observed among participants who reported *higher* vertical benefits, thus rejecting H3b.

RQ1 asked whether privacy self-efficacy moderates the relationship between privacy concerns and privacy management behaviors on both privacy dimensions. Although patterns emerged suggesting a stronger concern-behavior relationship among those with higher privacy self-efficacy, evidence for the interaction effect was limited. The interaction effect on the horizontal dimension reached conventional significance based on the p value, but the confidence interval approached zero, suggesting limited evidence for a robust moderation effect (b = 0.03, 95% CI [0.00, 0.06], t(1388) = 2.20, p = .028; β = .05, 95% CI [.01, .09]). On the vertical dimension the interaction was not significant (b = 0.02, 95% CI [-0.00, 0.04], t(1388) = 1.81, p = .070; β = .04, 95% CI [−.00, .08]).

H4 predicted that privacy cynicism would moderate the relationship between vertical privacy concerns and vertical privacy management behaviors, such that the privacy paradox would be weaker among people who report higher levels of privacy cynicism. The results revealed a significant interaction effect, b = 0.04, 95% CI [0.02, 0.07], t(1388) = 3.11, p = .002; β = .07, 95% CI [.03, .12], though in the opposite direction to the hypothesis: A stronger effect of vertical privacy concerns on vertical privacy management was observed among participants with *higher* privacy cynicism.

Finally, RQ2 asked if privacy cynicism moderated the relationship between horizontal privacy concerns and horizontal privacy management behaviors. The results showed a significant interaction effect b = 0.05, 95% CI [0.03, 0.08], t(1388) = 3.73, p < .001; β = .08, 95% CI [.04, .13]. Again, participants with higher privacy cynicism showed a stronger effect of horizontal privacy concerns on horizontal privacy management. For an illustration of the interaction effects, see Figure 1.

In sum, some interesting results emerged from the data on both the direct and moderating effects. However, we note that all effect sizes were small.

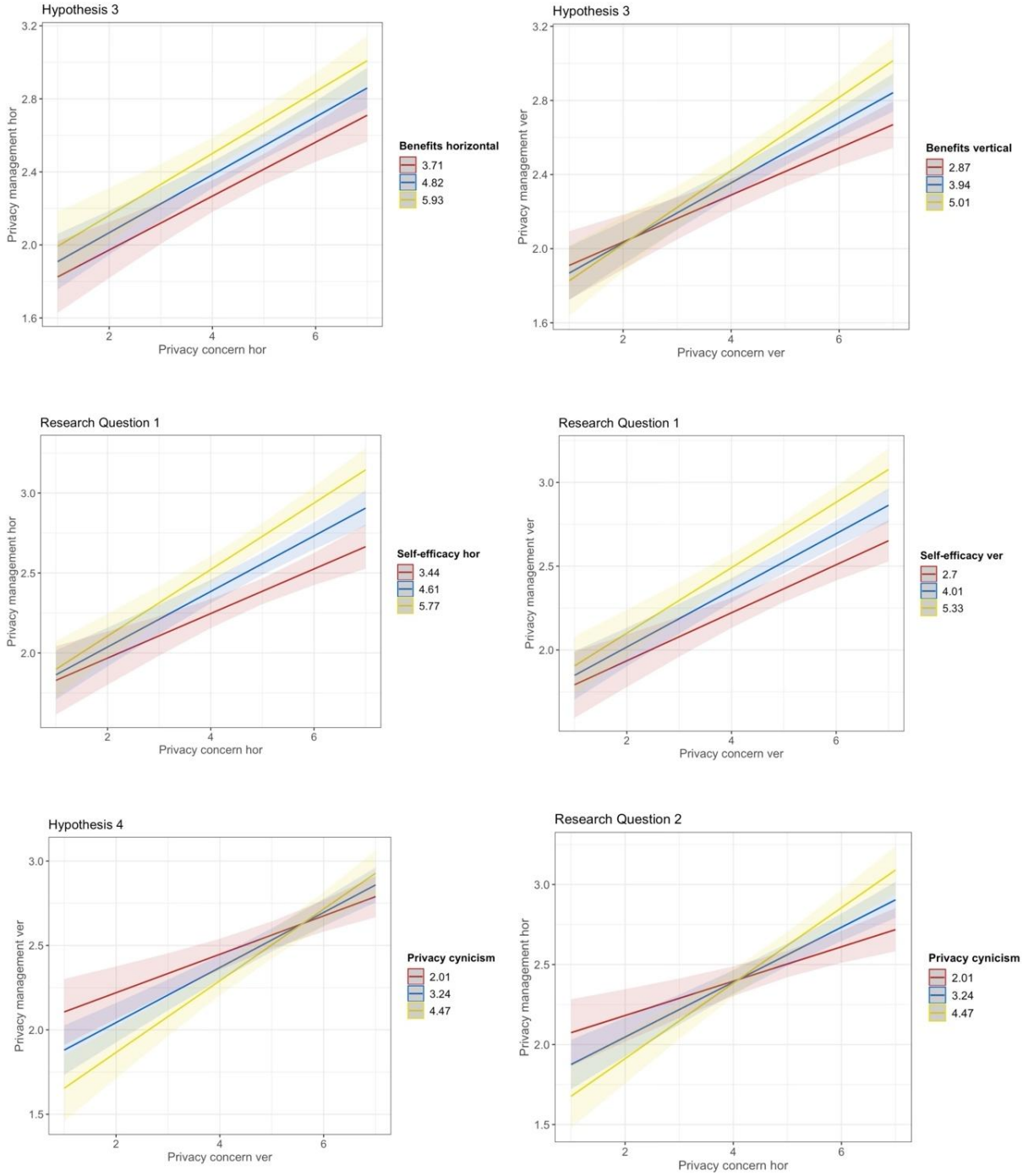
Discussion

This study examined evidence for the privacy paradox on the horizontal and vertical dimensions of privacy on social media, and further tested perceived benefits, privacy self-efficacy, and privacy cynicism as moderating factors for the paradox along both dimensions. Perhaps the most interesting finding is that there is no evidence for the privacy paradox on either the horizontal or the vertical dimension of privacy. That is, privacy concerns predicted the use of privacy management strategies vis-à-vis both other social media users and institutions.

This finding could be explained by several factors. First, unlike some prior research we followed the principle of compatibility to ensure measures of privacy concerns and privacy management behaviors align in terms of the audiences for personal information (i.e., horizontal vs. vertical privacy) and context (i.e., social media; see Dienlin & Trepte, 2015). When key measures comply in levels of specificity, our findings indicate that the privacy concern-behavior gap is bridged. Second, early studies supporting the privacy paradox focused on the type and amount of information disclosure as the outcome variable (e.g., Acquisiti & Gross, 2006; Reynolds et al., 2011). Our outcome measures similarly encompass disclosure but include a wider range of privacy management strategies that users may leverage on social media. Results indicate that when social media users are concerned about privacy being violated by other people and by institutions, they employ various types of protective strategies. This lends support to the privacy calculus approach over the privacy paradox in social media, as privacy concerns do motivate privacy management behaviors.

Our data also revealed some interesting interaction patterns. We found that perceived benefits moderated the impact of vertical privacy concerns on vertical privacy management behaviors. However, the interaction unexpectedly showed that greater benefit perceptions *reduced* the likelihood of observing the privacy paradox, such that the concern-behavior relationship was stronger for people who see greater benefits of sharing information with institutions online. One possible explanation is that those who perceived greater benefits of institutional data collection and processing may have higher privacy literacy. They may have more knowledge about how data could be handled and shared, and perhaps are more likely to critically evaluate the benefits and drawbacks of such practices (see Masur et al., 2023). Thus while appreciating its utility, they may recognize the negative consequences associated with the mistreatment of personal information through targeted advertising and profiling, thus becoming more alert to protect their privacy. Our data indeed showed that perceived benefits are positively correlated with privacy self-efficacy, which could be used as an indicator of subjective literacy. Nonetheless, this explanation is only speculative and future research must measure privacy literacy to test how it shapes privacy perceptions and behavior on both the horizontal and vertical dimensions (Masur et al., 2023).

Figure 1. *Plots of Interaction Effects.*



Note. Moderator values are −1 *SD*, mean, +1 *SD*.

Turning to privacy self-efficacy as a moderator for the privacy paradox, previous research revealed inconsistent findings, showing it could either strengthen (Chen & Chen, 2015) or weaken (Kang & Oh, 2023) the concern-behavior relationship. In our study, although patterns indicate less privacy paradox for more privacy-efficacious individuals, no robust evidence supports the interaction effects on either dimension. One possible explanation is that we did not consider the role of response efficacy (i.e., perceived effectiveness of privacy protection strategies), as suggested by the PMT, in moderating such relationships. Although users may feel confident about their own ability to employ available privacy mechanisms, they may nonetheless consider these strategies to be ineffective and thus refrain from using them. Indeed, constant dataveillance practices may render individual strategies less effective, as changing ad preferences or deleting cookies does not necessarily stop companies from tracking user data. In other words, response efficacy may play a more prominent role in strengthening the concern-behavior relationship than self-efficacy. Supporting our speculation, Boerman et al. (2021) found that response efficacy positively predicted privacy protection behavior, whereas privacy self-efficacy did not. Meier et al. (2020) similarly demonstrated that response efficacy, but not self-efficacy, was associated with Facebook users' self-withdrawal intention.

Finally, privacy cynicism moderated the impact of privacy concerns on privacy management behaviors on both privacy dimensions. Yet unexpectedly, the positive relationships between privacy concerns and privacy management behaviors were stronger among more privacy-cynical individuals. One possibility is that our scale primarily addresses the resignation aspect of cynicism, focusing on the lack of motivation and interest to protect privacy, but does not capture other dimensions of privacy cynicism (see Lutz et al., 2020). Privacy-resigned individuals may not perceive privacy protection to be entirely futile if they find the status quo satisfactory (Lutz et al., 2020), thus explaining why cynical participants in our data were still proactive in privacy management. Indeed, privacy cynicism scale scores were positively related to self-efficacy, implying that people may be resigned or uninterested vis-à-vis privacy protection due to self-confidence. Nonetheless, we acknowledge that our measure of privacy cynicism reflected early conceptual understandings of privacy cynicism in many published studies (e.g., Choi et al., 2018; Kahn et al., 2023; Segijn et al., 2024; van Ooijen et al., 2024), which might be too narrow in capturing the other dimensions of privacy cynicism that future studies should test.

Contributions

Theoretically, this study responds to recent calls for a dimensionalized approach to understanding online privacy phenomena by explicitly testing the privacy paradox on the horizontal and vertical dimensions (e.g., Masur, 2023; Quinn & Epstein, 2023). Our study confirms the positive concern-behavior relationship on both dimensions in social media that has been found in other online contexts (Epstein & Quinn, 2025), but advances the literature a step further by investigating moderating factors for this relationship on both dimensions. Findings thus contribute to the theoretical understanding of how various psychological factors *interact* to impact privacy outcomes along both dimensions, as advocated in recent research (Meier et al., 2023; Wang, Arch, et al., 2025a).

Methodologically, we followed the principle of compatibility and the contextual dependency of privacy (Dienlin & Trepte, 2015; Nissenbaum, 2010) by incorporating the multidimensionality of online privacy into our conceptualization and operationalization. Our results support the growing body of evidence that the privacy paradox does not exist on either the horizontal or vertical privacy dimension. Our findings also challenge the current understanding of the privacy paradox by revealing that high perceived benefits and high privacy cynicism could *decrease* the chance of observing a privacy paradox. As such, we join Masur (2023) in noting that future research should not expect consistent findings on the privacy paradox. Rather, it is germane for researchers to deliberate on their conceptual, operational, and analytical decisions and to recognize such impacts on "finding" the privacy paradox.

Practical Implications

Consistent with findings of previous dimensionalized research and meta-analyses (e.g., Baruh et al., 2017; Epstein & Quinn, 2025; Gruzd & Hernández-García, 2018; Kim et al., 2023; Lutz & Newlands, 2021; Masur, 2023), the effect sizes of the concern-behavior relationships on both dimensions are small. Although this finding could imply that privacy concerns play a minor role in motivating privacy protection behaviors, Funder and Ozer (2019) argue that even small effect sizes can accumulate and lead to attitudinal and behavioral changes over time. This suggests that, in practice, privacy messaging and literacy interventions should not be designed as one-shot efforts but rather delivered over time to more effectively raise privacy awareness, increase privacy concern, and ultimately motivate sustained privacy protection (e.g., Wang et al., 2026).

At the policy and design level, there remains a need to mandate greater transparency in institutional data collection and processing practices to facilitate more effective privacy management for users (e.g., advertising transparency, see Wang, Metzger, et al., 2025). Clearly communicating what types of data are collected and how they are processed can enhance user awareness, reduce information asymmetries, and motivate more active privacy protection. And at a broader societal level, evidence of a significant concern-behavioral relationship can also counter the dominant privacy paradox narratives that are often amplified in news coverage, because framing most users as indifferent or negligent toward privacy protection can undermine individual agency, cultivate privacy cynicism and fatigue, and legitimize institutional collection and (mis)use of user data.

In addition, given that benefit perceptions do not necessarily weaken the concern-behavior relationship on the horizontal dimension, and even strengthen this relationship on the vertical dimension, future message designs and literacy interventions may consider incorporating "benefit-aware" framing. That is, rather than only addressing

the negative consequences of self-disclosure and discouraging digital participation, intervention programs may highlight both rewards and risks of information sharing to facilitate more rational user considerations.

Limitations

Although the horizontal/vertical privacy distinction provides a refinement of how privacy variables have been conceptualized and measured in the literature before, it still oversimplifies the distinct privacy responses users may have against various threats from individual users and institutions *within* each dimension (see Lutz & Newlands, 2021). For example, people may have different vertical concerns vis-à-vis the government and online advertisers.

Second, our focus on the social media context limits the applicability of the findings to other online contexts. As privacy constructs are context-dependent, different findings may be observed depending on the specific platforms being used, the type of information being shared, the technological affordances, the privacy policies available, and social norms. In addition, as argued, horizontal and vertical privacy decisions may be intertwined and interdependent in social media, but in other contexts (e.g., eHealth) the horizontal/vertical discrepancy in the privacy paradox may be more observable. Future research should thus replicate these findings in other online contexts.

Our cross-sectional survey data are also limited. Self-reported data may be prone to social desirability biases (Dienlin, 2023). As the privacy paradox implies a causal relationship between privacy concerns and behaviors, longitudinal (e.g., Dienlin et al., 2023) and experimental (e.g., Barth et al., 2019) research is needed to reach confident conclusions about the phenomenon. Our sample was recruited through a non-probability survey panel and thus nationally representative samples are also needed to make generalizable conclusions. Comparative studies across cultural, political contexts, and sociodemographic groups would be helpful to further understand the privacy paradox phenomenon at a macro-level.

Future Research

Future research should test the integrated model of online privacy by elaborating the dynamic processes through which social media users manage privacy and self-disclosure across the individualistic, networked, and institutional levels and their repercussions. One instance is algorithmic profiling, which may result from self-disclosure and information sharing at all three levels. For example, employment decisions can be made by biased algorithmic processing of people's social media data (institutional privacy), including analysis of a potential employee's connections to measure their social capital within a certain field (networked privacy), and content analysis of social media posts to determine personality types (individual privacy) (Madden et al., 2017).

We also encourage other novel conceptualizations and measures of online privacy to help further unpack the complicated nature of online privacy decision-making (see Baruh et al., 2017). For instance, Walker and Hargittai (2021) proposed the social versus technical distinction of privacy management. Social strategies include the appreciation of the dynamics of online information sharing and flow (e.g., not posting sensitive information), whereas technical strategies emphasize the technical aspects of controlling personal information (e.g., downloading VPN). It is possible that a privacy paradox is more likely to be observed when measuring more technical than social aspects of privacy management. Ultimately, advancing digital privacy requires not only theories that appreciate the context-dependent nature of how individuals make privacy decisions but also designs and policies that address the technological and structural barriers to successful privacy protection.

Footnotes

[1] Data for the current study were drawn from a larger project on social media privacy across different sociodemographic groups in the U.S., which employed a non-random, purposive sampling technique. See Wang and Metzger (2024) for detailed information on how the data match and/or deviate from the U.S. national sample in terms of education and income across different racial/ethnic groups. In addition, participants were recruited through Qualtrics' XM panel, an online opt-in panel aggregator that sources respondents from multiple third-party panel partners. These participants have agreed to complete market research surveys in exchange for incentives.

Because Qualtrics recruits participants through multiple external panel providers, detailed information about the overall panel composition is not publicly available.

Conflict of Interest

The authors have no conflicts of interest to declare.

Use of AI Services

The authors declare they have used AI services, specifically ChatGPT, for grammar correction and minor style refinements. They carefully reviewed all suggestions from this service to ensure the original meaning and factual accuracy were preserved.

Data Availability Statement

The data that support the findings, the items, and the code of the analyses are openly available here: https://osf.io/ufpcw.

Authors' Contribution

Laurent H. Wang: conceptualization, data curation, formal analysis, investigation, methodology, project administration, writing—original draft, writing—review & editing. **Tobias Dienlin:** formal analysis, methodology, software, visualization, writing—review & editing. **Miriam J. Metzger:** conceptualization, investigation, methodology, project administration, resources, supervision, writing—review & editing.

Acknowledgement

The data reported herein were collected under the support of the Academic Senate Faculty Research Grant at UCSB.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy enhancing technologies* (pp. 36–58). Springer. https://doi.org/10.1007/11957454_3

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Barth, S., De Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology, 36*, 118–123. https://doi.org/10.1016/j.copsyc.2020.05.004

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & De Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Brown, B. (2001). *Studying the internet experience* (HPL-2001-49). HP Laboratories Bristol. https://hplabs.itcs.hp.com/techreports/2001/HPL-2001-49.html

Chen, H. T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist, 62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691

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. C10.1089/cyber.2014.0456

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

Dienlin, T. (2023). *Privacy calculus: Theory, studies, and new perspectives*. In S. Trepte, & P. Masur (Eds.), *The Routledge handbook of privacy and social media* (pp. 70–79). Routledge.

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

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, *25*(5), 1043-1064. https://doi.org/10.1177/14614448211016316

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712–728. https://doi.org/10.1080/1369118X.2018.1428652

Draper, N. A., Hoffmann, 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

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, *6*(2). https://doi.org/10.1177/2056305120916853

Epstein, D., & Quinn, K. (2025). A dimensionalised privacy behaviour model: An empirical test of a conceptual proposition. *Behaviour and Information Technology*, *44*(15), 3621–3641. https://doi.org/10.1080/0144929x.2024.2443523

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. Psychology Press. https://doi.org/10.4324/9780203838020

Funder, D. C., & Ozer, D. J. (2019). Evaluating effect size in psychological research: Sense and nonsense. *Advances in Methods and Practices in Psychological Science*, *2*(2), 156-168. https://doi.org/10.1177/2515245919847202

Gottfried, J., Ježek, S., Králová, M., & Řiháček, T. (2022). Autocorrelation screening: A potentially efficient method for detecting repetitive response patterns in questionnaire data. *Practical Assessment, Research, and Evaluation, 27*(2), Article 2. https://doi.org/10.7275/VYXB-GT24

Gruzd, A., & Hernández-García, Á. (2018). Privacy concerns and self-disclosure in private and public uses of social media. *Cyberpsychology, Behavior, and Social Networking*, *21*(7), 418–428. https://doi.org/10.1089/cyber.2017.0709

Gruzd, A., Jacobson, J., Mai, P., & Dubois, E. (2018*). Social media privacy in Canada* (V1; UNF:6:T9u/atUzgpVvdlRvbejvgg== [fileUNF]) [Data set]. Borealis. https://doi.org/10.5683/SP/JVOT0S

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

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

Kang, H., & Oh, J. (2023). Communication privacy management for smart speaker use: Integrating the role of privacy self-efficacy and the multidimensional view. *New Media & Society*, *25*(5), 1153–1175. https://doi.org/10.1177/14614448211026611

Kezer, M., Dienlin, T., & Baruh, L. (2022). Getting the privacy calculus right: Analyzing the relations between privacy concerns, expected benefits, and self-disclosure using response surface analysis. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(4), Article 1. https://doi.org/10.5817/CP2022-4-1

Kim, Y., Kim, S. H., Peterson, R. A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. *Technological Forecasting and Social Change*, *196*, Article 122789. https://doi.org/10.1016/j.techfore.2023.122789

King, J., Gonzales, A. L., & Wang, L. H. (2026). Depressed individuals' support seeking in online communities: The role of anonymity, self-disclosure, and privacy skills. *Computers in Human Behavior*, *176*, Article 108863. https://doi.org/10.1016/j.chb.2025.108863

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. https://doi.org/10.1007/s12394-009-0019-1

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

Lin, L., & Wang, L. H. (2026). From screens to sensors: A contextual integrity approach to understanding privacy norms across mobile health contexts. *Journal of Computer-Mediated Communication, 31*(1), Article zmaf022. https://doi.org/10.1093/jcmc/zmaf022

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, *37*(3), 147–162. https://doi.org/10.1080/01972243.2021.1897914

Lutz, C., & Ranzini, G. (2017). Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media + Society*, *3*(1). https://doi.org/10.1177/2056305117697735

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

Madden, M. (2017, September 27). *Privacy, security, and digital inequality.* Data & Society Research Institute. https://datasociety.net/research-library/privacy-security-and-digital-inequality/

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53–125. https://journals.library.wustl.edu/lawreview/article/id/3193/

Marwick, A., Fontaine, C., & Boyd, D. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among Low-SES youth. *Social Media + Society*, *3*(2). https://doi.org/10.1177/2056305117710455

Masur, P. K. (2023). Understanding the effects of conceptual and analytical choices on 'finding' the privacy paradox: A specification curve analysis of large-scale survey data. *Information, Communication & Society*, *26*(3), 584–602. https://doi.org/10.1080/1369118X.2021.1963460

Masur, P. K., Hagendorff, T., & Trepte, S. (2023). Challenges in studying social media privacy literacy. In S. Trepte & P. Masur (Eds.), *The Routledge handbook of privacy and social media* (pp. 110–123). Routledge.

Masur, P. K., & Trepte, S. (2021). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research*, *47*(1), 49-74. https://doi.org/10.1093/hcr/hqaa012

Meier, Y., Meinert, J., & Krämer, N. C. (2023). One-time decision or continual adjustment? A longitudinal study of the within-person privacy calculus among users and non-users of a COVID-19 contact tracing app. *Media Psychology*, *26*(1), 36–53. https://doi.org/10.1080/15213269.2022.2092750

Meier, Y., Schäwel, J., Kyewski, E., & C. Krämer, N. (2020, July). Applying protection motivation theory to predict Facebook users' withdrawal and disclosure intentions. In *SMSociety'20: International Conference on Social Media and Society* (pp. 21–29). Association for Computing Machinery. https://doi.org/10.1145/3400806.3400810

Memarian, S., Malgonde, O. S., & Kim, D. J. (2025). Unraveling the privacy paradox: A comprehensive review of factors behind the discrepancy in online concerns and disclosure behavior. *Information Systems Frontiers*, *28*(2), 675–696. https://doi.org/10.1007/s10796-025-10617-y

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

Park, Y. J. (2021). Why privacy matters to digital inequality. In E. Hargittai (Ed.), *Handbook of digital inequality* (pp. 284–295). Edward Elgar Publishing. https://doi.org/10.4337/9781788116572.00028

Petro, G., & Gonzales, A. L. (2025). Young women's perceptions of cooperative privacy threats through the lens of abortion in the United States. *New Media & Society*, Advance online publication. https://doi.org/10.1177/14614448251403196

Quinn, K., & Epstein, D. (2023). Dimensionalizing privacy to advance the study of digital disempowerment. *Big Data & Society*, *10*(2). https://doi.org/10.1177/20539517231221739

Quinn, K., Epstein, D., & Moon, B. (2019). We care about different things: Non-Elite conceptualizations of social media privacy. *Social Media + Society*, *5*(3). https://doi.org/10.1177/2056305119866008

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). https://doi.org/10.5210/fm.v15i1.2775

Reynolds, B., Venkatanathan, J., Gonçalves, J., & Kostakos, V. (2011). Sharing ephemeral information in online social networks: privacy perceptions and behaviours. In *IFIP Conference on Human-Computer Interaction* (pp. 204–215). Springer. https://doi.org/10.1007/978-3-642-23765-2_14

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). The Guilford Press.

Rohrer, J. M. (2018). Thinking clearly about correlations and causation: Graphical causal models for observational data. *Advances in Methods and Practices in Psychological Science*, *24*(2), 27–42. https://doi.org/10.1177/2515245917745629

Segijn, C. M., Kim, E., & Van Ooijen, I. (2024). The role of perceived surveillance and privacy cynicism in effects of multiple synced advertising exposures on brand attitude. *Journal of Current Issues & Research in Advertising*, *45*(4), 506–522. https://doi.org/10.1080/10641734.2024.2318711

Schwartz-Chassidim, H., Ayalon, O., Mendel, T., Hirschprung, R., & Toch, E. (2020). Selectivity in posting on social networks: the role of privacy concerns, social capital, and technical literacy. *Heliyon*, *6*(2), Article e03298. https://doi.org/10.1016/j.heliyon.2020.e03298

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36. https://doi.org/10.1177/0270467607311484

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

Vanhove, J. (2021). Collinearity isn't a disease that needs curing. *Meta-Psychology*, *5*. https://doi.org/10.15626/MP.2021.2548

Vimalkumar, M., Sharma, S. K., Singh, J. B., et al. (2021). "Okay Google, what about my privacy?": User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior 120*, Article 106763. https://doi.org/10.1016/j.chb.2021.106763

Walker, A. M., & Hargittai, E. (2021). Drills and spills: Developing skills to protect ones privacy online. In E. Hargittai (Ed.), *Handbook of digital inequality* (pp. 358–372). Edward Elgar Publishing. https://doi.org/10.4337/9781788116572.00033

Wang, L. H. (2026). Privacy cynicism as a product of structural constraints and a form of social privilege: A precarious protection hypothesis. In C. Lutz, C. Hoffmann, & A. Tamò Larrieux (Eds.), *Advancing the study of privacy cynicism, apathy and resignation in the digital society* (pp. 81–96). Edward Elgar Publishing.

Wang, L. H., & Metzger, M. J. (2023). The role of culture in privacy management on social media among emerging adult children and their parents. *Journal of International and Intercultural Communication*, *16*(2), 162–190. https://doi.org/10.1080/17513057.2021.1993966

Wang, L. H., & Metzger, M. J. (2024). The online privacy divide: Testing resource and identity explanations for racial/ethnic differences in privacy concerns and privacy management behaviors on social media. *Communication Research.* https://doi.org/10.1177/00936502241273157

Wang, L. H., Arch, D. N., & Metzger, M. J. (2025). Not the average user: A latent profile analysis of privacy protection appraisals in targeted advertising. *New Media & Society*, Advance online publication. https://doi.org/10.1177/14614448251393913

Wang, L. H., Metzger, M. J., Liu, X., & Qi, L. (2025). Seeing ad transparency more clearly: Public perception, use of ad transparency tools, and responses to dataveillance. *Journal of Advertising, 54*(2), 213–232. https://doi.org/10.1080/00913367.2025.2451993

Wang, L. H., Miller, L. B., Metzger, M. J., & Nabi, R. L. (2026). The pulse of privacy: The role of efficacy framing and discrete emotion in combating privacy powerlessness and motivating online privacy protection. *Communication Research*, Advance online publication. https://doi.org/10.1177/00936502261415680

Xu, S., & Li, W. (2022). A tool or a social being? A dynamic longitudinal investigation of functional use and relational use of AI voice assistants. *New Media & Society*, *26*(7), 3912–3930. https://doi.org/10.1177/14614448221108112

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

About Authors

Laurent H. Wang (Ph.D., UC Santa Barbara) is an Assistant Professor in the Stan Richards School of Advertising and Public Relations, Moody College of Communication, at the University of Texas at Austin. He studies communication technology, privacy, and social inequality. Specifically, he employs quantitative and qualitative methods to examine how users 1) negotiate privacy decisions in various technological contexts and 2) navigate digital inequality challenges.

https://orcid.org/0000-0002-6795-3039

Tobias Dienlin (Ph.D., University of Hohenheim) is Professor of Empirical Communication and Media Studies in the Department of Communication and Media Research at the University of Zurich, Switzerland. Using both quantitative and qualitative methods, in his research, Dr. Dienlin analyzes how users manage their privacy online, how using digital media affects well-being, and how research can be improved using open science practices.

https://orcid.org/0000-0002-6875-8083

Miriam J. Metzger (Ph.D., University of Southern California) is a Professor in the Department of Communication at the University of California, Santa Barbara. Dr. Metzger's research seeks to understand the individual and societal effects of using information and communication technology by studying the forces that shape people's trust of and perceptions about online information. Her work employs quantitative social science methods to study the ways in which digital communication technologies challenge users' ability to evaluate the credibility of information online and negotiate privacy decisions.

https://orcid.org/0000-0001-8433-8604

✉ **Correspondence to**
Laurent H. Wang, Stan Richards School of Advertising and Public Relations, Moody College of Communication, University of Texas at Austin, 300 W Dean Keeton St, Austin, TX 78712, USA, laurent.wang@austin.utexas.edu