Review of Communication Research
2026, Vol. 14
ISSN: 2255-4165
https://rcommunicationr.org/index.php/rcr/

Rethinking the Trade-Off: A Systematic Review of Current Research on the Privacy Calculus Model

Zhao Peng [1*] Emily S. Zhan [2] Zhehao Liang [3] Soo Young Shin [4]

[1] Ph.D., Department of Journalism, Emerson College, Boston, USA
[2] Ph.D., Department of Communication, North Dakota State University, ND, USA
[3] Ph.D., School of Political Science & Public Administration, Wuhan University, China
[4] Ph.D., Journalism & Creative Media, College of Communication & Information Sciences, University of Alabama, AL, USA
* **Corresponding Author:** zhao_peng@emerson.edu

Citation: Peng, Z., Zhan, E.S., Liang, Z. & Shin, S.Y. (2026). Rethinking the Trade-Off: A Systematic Review of Current Research on the Privacy Calculus Model. *Review of Communication Research, 14*, 84–118. https://doi.org/10.52152/RCR.V14.6

ARTICLE INFO

Received: 03 Oct 2025

Accepted: 25 Feb 2026

ABSTRACT

As one of the most popular theoretical models explaining mechanisms of information disclosure behavior, the Privacy Calculus Model (PCM) has received significant academic interest and criticism. While numerous studies have offered explanations countering criticism of the privacy calculus model, none have synthesized existing findings on benefit and cost variables or systematically reviewed moderators and other factors to address the model's limitations. Drawing on the principle of compatibility and the Privacy Process Model's four-dimensional framework of privacy context, this study conducted a systematic review of 119 PCM studies published between 2018 and 2023. Results revealed that among studies reporting non-significant cost-disclosure relationships, 66% exhibited dimensional misalignment between cost and disclosure variables, compared to only 32% among studies with significant results. Additionally, we identified inconsistencies in how disclosure behaviors, perceived risks, and privacy concerns are conceptualized and operationalized, along with an underutilization of moderating variables. Based on these findings, we propose an integrated framework recommending that future PCM research align the dimensions of costs, benefits, and disclosure variables within their specific privacy contexts to improve predictive validity.

Keywords: Privacy Calculus Model, Compatibility Principle, Four-Dimensional Framework, Privacy Concerns, Perceived Benefits.

INTRODUCTION

The privacy calculus model (PCM) is a theoretical model that has been employed to explain why people disclose personal information. It was originally developed to explain disclosure behavior in an offline context (Laufer & Wolfe, 1977). As technology advanced, it was used to explain disclosure behavior in online contexts. The PCM assumes people as active agents and postulates that people engage in rational calculation between perceived privacy costs and potential benefits of disclosure. The final disclosure behavior is determined by the cost-benefit trade-off (Dinev & Hart, 2006). The model assumes that information disclosure occurs because the benefits outweigh the costs. The potential benefits of information disclosure include entertainment, social capital, self-presentation, financial benefits, and increased convenience (Lee et al., 2013; Wang et al., 2015). The potential costs include privacy violation, security impairments, identity theft, misuse of personal information, and social criticism (Warshaw et al., 2015). The PCM has received considerable academic attention and has been employed in many empirical studies. According to Dielin (2023)'s quick search on EBSCO host, there are 297 studies using the PCM as the major theoretical framework.

The PCM is widely used across various fields, yet researchers have repeatedly found that its predictors, particularly cost variables, do not reliably predict disclosure behaviors. Several explanations have been proposed for this inconsistency. A prominent line of research challenges the PCM's fundamental premise that people are

making rational decision, arguing that disclosure decisions are driven not by rational cost-benefit calculations but by heuristics and emotions (Dienlin, 2023; Gerber et al., 2018; Kokolakis, 2017; Pomfret et al., 2020). More recently, scholars have turned attention to methodological explanations. For instance, Masur (2023) found that how privacy concerns were operationalized was the largest driver of variability in results, accounting for approximately 55% of the variance across specifications. Concern items closely matched to the specific behavior being predicted yielded stronger and more consistent effect sizes, whereas broader concern items produced smaller, more variable, and often non-significant estimates. This suggests that inconsistencies in PCM results may be partly attributed to measurement mismatches.

Building on Masur's (2023) finding that operationalization specificity significantly shapes privacy concern and disclosure outcomes, we extend this effort by refining the measurement of the Privacy Calculus Model's (PCM) core variables — costs, benefits, and disclosure. Drawing on the principle of compatibility (Fishbein & Ajzen, 2011) and Dienlin's (2014) four-dimensional privacy framework, we argue that privacy perceptions and behaviors are activated within specific privacy contexts (informational, social, psychological, and physical). Accordingly, meaningful weighing of costs and benefits is most likely to occur and most likely to predict disclosure behavior when predicting variables aligning with disclosure. To achieve this goal, we conducted a systematic review on 119 studies and examined 1) how information disclosure is conceptualized and operationalized in current PCM studies; 2) existing empirical evidence on how benefit and cost variables have been conceptualized and measured; and 3) moderators and other factors that contribute to addressing the limitations of the PCM. Based on a systematic review of 119 PCM studies, we present an integrated PCM framework (see Figure 2) that offers two key recommendations: ensuring dimensional alignment between the measurement of predictor variables (costs and benefits) and disclosure behaviors, and incorporating relevant moderators and other influential factors (e.g. trust) that influence the calculus process.

LITERATURE REVIEW

The Challenges of the PCM

The Privacy Calculus Model (PCM) is based on the assumption that individuals perform a rational mental calculus, weighing anticipated benefits against perceived risks when deciding whether to disclose personal information online (Barth & De Jong, 2017; Dienlin, 2023; Gerber et al., 2018). Within this framework, the act of information disclosure is driven by individuals engaging in a rational calculus to maximize benefits and minimize risks. Consequently, information sharing occurs when the expected gains exceed the perceived costs; conversely, when costs exceed expected gains, individuals prefer to withhold information. As the PCM is applied across diverse contexts, the specific meaning of “benefits” and “costs” vary accordingly. In the realm of social media, for instance, anticipated benefits typically manifest as the accumulation of social capital or the facilitation of relationship development (Barth & De Jong, 2017). In contrast, perceived costs are often operationalized as privacy concerns, specifically regarding identity theft or long-term reputational damage.

A growing body of empirical evidence reveals a paradoxical phenomenon that individuals disclose personal information even when reporting high levels of privacy concern (Masur, 2023). Scholars have proposed several explanations for this phenomenon, most notably by challenging the assumption of “rationality” inherent in the PCM. Critics argue that the weighing process is characterized by bounded rationality, as users often lack the requisite information (e.g., being unaware of data collection) or the cognitive capacity to comprehensively evaluate the trade-offs of disclosure (Acquisti et al., 2018; Gerber et al., 2018; Kokolakis, 2017). Consequently, rather than performing a precise calculation, individuals often rely on heuristics that can bypass the cost-benefit analysis. Also, psychological factors such as optimism bias, current emotions, and the illusion of control further inhibit the ability to engage in a strictly rational calculus, leading to disclosure behaviors that deviate from logical expectations (Gerber et al., 2018; Masur, 2019).

Beyond theoretical critiques, scholars have identified significant methodological limitations in the extant literature concerning the measurement and testing of the PCM. Notably, Kezer et al. (2022) contend that traditional analytical approaches, specifically linear regression, treat risks and benefits as discrete independent variables. This approach fails to capture the core tenet of the model: that the difference between perceived benefits and risks is the primary driver of disclosure behavior. To address this misalignment between theory and statistical application, Kezer et al. (2022) proposed the use of Response Surface Analysis (RSA), which allows for a more nuanced examination of how the congruence (or incongruence) between benefits and costs relates to self-disclosure. Furthermore, the robustness of PCM findings could also be attenuated by measurement and design constraints. Reliance on self-report measures introduces the risk of social desirability bias and recall inaccuracies, potentially skewing data (Breuer et al., 2023; Dienlin, 2023; Kokolakis, 2017). Additionally, the predominance of

cross-sectional designs in this field precludes the determination of causality.

Following the measurement issues strand, Masur (2023) found that different operationalization of dependent variables (e.g., general measure vs. specific measure) and the incompatibility between independent and dependent variables' measurement (e.g., general privacy concerns to predict specific behaviors) could easily yield unexpected and inconsistent results. Fishbein and Ajzen (2011) posited that to accurately predict a specific behavior, the measurement of the predicting variables must be at the same level of specificity with the measurement of the behavior. Using general privacy concerns to predict specific disclosure behaviors frequently produces a "privacy paradox." However, research adhering to the principle of compatibility, which requires aligned measurement specificity between predictors and outcomes, consistently identifies significant relationships (Masur, 2023).

Extending Masur's (2023) finding that paradoxical results may stem from conceptual and analytical choices, we propose that the paradoxical phenomenon is not a behavioral failure but a consequence of dimensional incompatibility within the PCM. We argue that the mental calculus is not a global evaluation but a domain-specific process; statistical significance is achieved only when costs, benefits, and disclosure align within the same conceptual dimension. To operationalize this, we apply the Privacy Process Model and its framework of four dimensions of privacy context to the PCM: informational, social, psychological, and physical.

Privacy Process Model & Four Dimensions of Privacy Context

The Privacy Process Model (PPM) is a theoretical framework proposed by Tobias Dienlin (2014) that integrates previously separate privacy theories into a single sequential model applicable to both online and offline contexts. The PPM emphasizes that privacy is a dynamic and sequential process and the model is structured around three primary factors that follow a linear process flow: privacy context, privacy perception, and privacy behavior.

According to the PPM, there are four dimensions of privacy context: informational, social, psychological, and physical, which originate from Burgoon's (1982) approach toward privacy. Informational context refers to the amount of information collected in a given situation; social context refers to the number and type of people present; psychological context refers to the extent to which people engage in intimate versus impersonal conversations; and physical context refers to the proximity of others. All four dimensions of privacy context are independent and differ from each other. According to the PPM, privacy context is an objective situation that influences people's privacy perception and subsequent privacy behaviors (Dienlin, 2014).

Although privacy context can be objectively described, it must be subjectively perceived, and people's privacy perceptions differ greatly across different privacy contexts. Hence, it is possible that perceptions of anticipated benefits and potential risks of self-disclosure are greatly influenced by privacy contexts, with specific contexts triggering corresponding perceptions of disclosure benefits and risks. For instance, when an individual downloads a new app and must provide basic identity information for service personalization, the privacy context is informational. Simultaneously, the individual's privacy perception encompasses both the personalization convenience of providing personal information (informational benefits) and concerns about unwanted data collection by the app company (informational costs). In this scenario, the individual evaluates the trade-off between convenience and unwanted data collection—two factors that exist on the same conceptual dimension.

Being on the same conceptual dimension has important implications for measurement. When dimensions are aligned between independent and dependent variables, results should match the PCM's original predictions. According to the principle of compatibility, questions used to measure attitudes, perceptions, and behaviors should align in terms of action, target, context, and time (Fishbein & Ajzen, 2010; Dienlin & Trepte, 2015). Dienlin and Trepte (2015) found that dimensionally aligning privacy attitudes with corresponding privacy behaviors (informational, social, and psychological) produced significant relationships, whereas general privacy concerns failed to predict specific behaviors. We therefore argue that aligning the dimensions of the operationalization of both predictor and outcome variables in the PCM will similarly strengthen the robustness of its prediction.

Extant PCM research overlooks the distinctions between specific types of disclosure, benefits, and concerns within their respective privacy contexts. This lack of granularity might result in paradoxical findings, as individuals struggle to evaluate trade-offs between functionally distinct dimensions. For instance, in the previously discussed application scenario, researchers may attempt to measure psychological benefits (e.g., general satisfaction) against informational costs. From a cognitive standpoint, individuals find it difficult to weigh a psychological gain against an informational loss, as these variables lack a common metric for comparison. Comparing these disparate dimensions is akin to comparing an apple with an egg; there is no shared baseline for evaluation, forcing individuals to rely on heuristics or emotional preferences rather than a strictly rational calculus. Consequently, even when users express high levels of concern regarding informational privacy, these

concerns may fail to inhibit disclosure behavior if the anticipated benefits are perceived through a different, non-competing dimension.

Therefore, we propose our central argument and overarching research question: When anticipated benefits and potential costs are measured along the same dimension as information disclosure, results will align with PCM predictions, such that benefits will positively relate to self-disclosure while costs will negatively relate to self-disclosure. Conversely, when the dimensions of predicting variables differ from information disclosure in their operationalization, results will become paradoxical, with benefits or costs showing inconsistent or unexpected relationships with disclosure behavior.

RQ1: How does the dimensional alignment between independent variables (perceived costs and perceived benefits) and disclosure behaviors separately influence the significance of the privacy calculus in predicting information disclosure?

Information Disclosure in the PCM

Information disclosure (ID) is generally defined as a behavior in which individuals reveal their information to others. As the core dependent variable in PCM, the choice of variable, conceptualization, and operationalizations vary from one study to another, each of which could result in misleading findings. Most studies that employed PCM define ID in general terms. However, advanced technologies have enriched the content and nature of information disclosure. People disclose different types of personal information across online platforms: informational data (e.g., location for service personalization), psychological content (e.g., feelings and thoughts via blogging), and social network information (e.g., friend lists on social media). While disclosure content varies across platforms, it is largely shaped by the specific privacy context (Acquisti et al., 2015; Dienlin, 2014). The uncertainties in conceptualization lead to inconsistency in operationalization. Masur (2023) found that while some scholars measure specific types of information disclosed, other scholars use a more general scale to measure ID. Given the inconsistent conceptualizations and operationalizations of ID, we propose our second research question:

RQ2(a): How did studies using PCM conceptualize and operationalize information disclosure?

In the PCM, one fundamental assumption concerning ID is that people are empowered to exercise full control of their personal information (Dinev et al., 2013). Because of that, most studies that used the PCM investigated self-disclosure behaviors. However, in today's ID environment, people's information is interconnected in many ways, and the management of privacy relies on collective actions of more than one person (De Wolf, 2020; Masure, 2023). For example, Peng (2023) proposed that the theoretical scope of PCM should be extended to non-typical disclosure behavior, such as other-generated disclosure. Other-generated disclosure refers to one's information being revealed by others, not themselves. For example, one could be unknowingly revealed or tagged in a photo posted by friends. In such a scenario, one's disclosure can cause dangers for others and the evaluation of one's own disclosure risks and benefits are different from those of others. Given the nature of current content-sharing platforms, users are encouraged and primed for other-generated disclosures. For the goal of theory development, it is imperative to know whether and how the PCM applies to non-typical disclosure behaviors.

RQ2 (b): How did studies using the PCM apply the model to disclosure behaviors other than self-disclosure?

Costs

The cost in Laufer and Wolfe's (1977) calculus of behavior emphasizes the anticipated consequences in the future, which is composed of uncertainties of the future of an individual's information management ability and the unpredictability of the ever-changing socio-historical context and technology. Dinev and Hart's (2006) took the Theory of Reasoned Action and Theory of Planned Behavior approach and narrowed down the costs to only internal subjective factors - risk beliefs and privacy concerns. Since then, Krasnova et al. (2010) and most following scholars have also used perceived risk, privacy concerns, or both as cost variables in the PCM.

Perceived Risk

Perceived risk (PR) refers to the perceived possibility of experiencing loss related to disclosure of personal information online (Dinev & Hart, 2006). In PCM, PR is negatively related to ID. In an e-commerce transaction context, PR is related to the uncertainty that arises from the potential for a seller's opportunistic actions to lead to negative consequences for the consumers (Ganesan, 1994). The opportunistic behaviors associated with disclosed personal information include selling information to parties not involved in immediate transactions (e.g. third-party marketing firms, financial institutions, government agencies), and the misuse of personal information (e.g. identity theft, insider disclosure) (Dinev & Hart, 2006). The perception that one's information could be misused makes individuals hesitant to share personal information in e-commerce transactions.

Like ID, PR is also defined in general terms, roughly referring to "the possibility of loss" caused by one's

information disclosure (Dinev & Hart, 2006, p. 63). Because of that, the measurements of PR in PCM studies tend to be broad as well. However, in different contexts, PR could include more nuanced meanings to capture contextual-specific risks. For example, Chatterjee et al. (2023) used an item "Financial transactions may fail if it is done through smartphone" to indicate perceived financial risks. PR could encompass psychological risks, such as emotional discomfort from information disclosure, or social risks like conflicts with friends due to sharing personal information (Youn, 2005).

Privacy Concerns

Similar to perceived risks, the PCM proposed that individuals with a higher degree of privacy concerns (PC) will be less willing to disclose their personal information. Dinev and Hart's (2006) definition of PC is more related to the Internet, suggesting that Internet technology induces uncertainties about who has access to the information and how it is used. The definition and scope of PC have been updated and expanded as new technology emerged. Several researchers have pointed out that the use of social media could exacerbate PC, as individuals share personal information not only with the platform itself but also with other users (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). They proposed that there are two types of privacy concerns – vertical (or institutional) privacy concern and horizontal (or social) privacy concern; the former refers to the perceived uncertainties of the service provider's way of handling disclosed data, the latter refers to the perceived uncertainties of how other users will do with the data (Bazarova & Masur, 2020; Raynes-Goldie, 2010).

Researchers rarely addressing the contextual specifics in conceptualizing and measuring PC might also be the reason leading to the divergent or contradictory empirical findings (Bartol et al., 2023). Bartol et al. (2023) found that the majority of SNS research that studies PC and ID behavior does not consider the distinction between vertical (or institutional) and horizontal (or social) PC and tends to disregard the horizontal (or social) PC, which is essential for disclosing in the SNS context. Extending the vertical (or institutional) and horizontal (or social) dimensions of PC, we propose a four-dimensional framework: informational, social, psychological, and physical. The existing vertical (or institutional) and horizontal (or social) correspond to the informational and social dimensions, respectively. Although psychological and physical privacy dimensions have not been explicitly operationalized in empirical studies, they have long been recognized as critical concerns in privacy literature. For example, Ben-Ze'ev (2003) argues that revealing emotional attitudes contradicts privacy protection by exposing one's vulnerabilities. Building on this, psychological PC can be conceptualized as individuals' anxiety about disclosing emotions, feelings, beliefs, or attitudes that render them vulnerable to others. Physical PC, meanwhile, have been implicitly measured in research on location-based services; studies examining Airbnb information sharing, for instance, assessed users' concerns that location data disclosure could facilitate physical harm (Chen et al., 2020).

Therefore, we propose the third research question:

RQ3: How did studies using PCM conceptualize and operationalize (a) privacy risks and (b) privacy concerns?

In addition to dimensional alignment between costs and disclosure behavior, prior research has identified multiple moderating variables that affect the strength and consistency of these relationships (Acquisti & Grossklags, 2007; Baek et al., 2014; Kehr et al., 2015; Kokolakis, 2017). The failure of the PCM to incorporate the impact of other factors on PC and disclosure behaviors give rise to the contradictory findings. In response to the call for a more holistic model of the mental calculus of privacy, this study examines additional significant antecedents, and moderators that have been addressed in previous papers on PCM.

RQ4: What moderators should be included in the PCM?

Perceived Benefits

The perceived benefit (PB) has been considered as the major variable that can counter the effect of perceived costs and encourage information disclosure behavior. PB generally refers to the rewards or gains one expects to receive from disclosing information. Wang et al. (2024) suggested that PB, like privacy concerns, can also be mapped onto the horizontal (e.g., social capital) and vertical (or institutional) dimensions (e.g. personalization convenience) of privacy. We propose leveraging PPM's four dimensions to conceptualize PB in a context-dependent manner: the types of benefits that motivate disclosure varies across informational, social, psychological, and physical dimensions depending on the situational context. When individuals disclose information during e-commerce transactions, the benefits encompass financial discounts or rewards, increased convenience, high-quality services, and personalization (informational) (Culnan & Armstrong, 1999; Gerber et al., 2018; Krasnova et al., 2010). When individuals share information on social media platforms, the benefits include social capital, entertainment, social support, reputation management, and relationship maintenance (social) (Chen, 2018; Krasnova et al., 2010; Trepte, 2023). During COVID-19, users sharing information with mobile tracing apps can receive multiple personal benefits, such as better quality of care, and accurate treatment options (physical) (Hong

& Cho, 2023). When people share vulnerable experiences to seek social support, they gain psychological benefits such as emotional support and empathy (psychological) (Zhu et al., 2022).

Hence, we proposed to conceptualize perceived benefit as a construct with four dimensions that depend on its context.

RQ5: How did studies using PCM conceptualize and operationalize benefits?

Although perceived benefits have been empirically tested to be effective in offsetting the influence of perceived costs on disclosure behavior, only considering perceived benefits in PCM may exclude other potential variables and fail to capture the whole picture of the disclosure behavior mechanism. In the seminal works of the PCM, other variables, such as trust and perceived control, had been proposed to be positively related to information disclosure and to mitigate the influence of perceived costs. Culnan and Armstrong (1999) found, in addition to perceived benefits such as higher quality services, trust in companies' fair information practices could encourage customers to disclose personal information. Similarly, Dinev and Hart (2006) incorporated internet trust and personal internet interest into the PCM to predict the behavior of sharing personal information in e-commerce transactions, two of which were found positively related to the disclosure behavior. Although internet trust and personal internet interest are not technically perceived benefits, they can override the influence of perceived risks on behavioral intention (Dinev & Hart, 2006). In recent publications, researchers have integrated privacy self-efficacy (Dienlin & Metzger, 2016), social influence (Fox et al., 2022), and self-enhancement (Nabity-Grover et al., 2023) in the PCM to understand the information disclosure behavior across different contexts.

As information disclosure becomes more complex, the mental calculus of privacy may extend beyond perceived costs and benefits. In response to more comprehensive PCM, this study also looks into other variables that can counter the effect of perceived costs by systematically reviewing prior studies.

RQ6: Besides perceived benefits, what other variables outweigh the influence of perceived costs in information disclosure?

METHODOLOGY

Information Sources and Search Strategy

In compliance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, we executed our literature search about the privacy calculus theory. The search process took place between April 24-27th, 2023 in the databases of Web of Science, ScienceDirect, and Scopus. Guided by the research questions, we used the Boolean "OR" to combine alternate terms regarding privacy calculus. Specifically, we applied the following search string to the metadata of the papers in each database: "privacy calculus", "privacy calculus model", "privacy calculus theory", "privacy calculus framework", "privacy calculus perspective", and "privacy calculus approach". Additionally, we intended to collect only journal articles published between January 1st, 2018, and April 27th, 2023, for the systematic review. We also used the embedded function in the websites to filter "journal articles" before downloading the sources. Our preliminary list included 800 articles using the PCM to explain information disclosure behaviors.

Screening Process

The references of 800 articles returned from the searches were exported into an Excel file. First, 219 duplicates were removed, resulting in 581 articles to be screened. Two authors participated in the title and abstract screening process. During the abstract screening, 331 more articles that did not mention PCM in the abstract or include PCM in keywords were excluded, leaving 250 articles for full-text assessment. As nine articles were not retrievable, 241 articles were downloaded for further screening. Two authors independently screened the full text of the articles and left notes when it was difficult to make decisions. After the selections, the authors discussed the unsure selection decisions to reach agreements. The final list consists of 119 articles as shown in **Figure 1**.

Coding Protocol

To study PCM, we coded the variables, including the conceptualization and operationalization of information disclosure (RQ2), benefit variables (RQ5), cost variables (RQ3), and the moderators used in the model (RQ4). To code the conceptualization and operationalization of key variables in the PCM, we thoroughly searched the entire article for the conceptual definitions and survey items of each variable. If the article provides definitions and measurement items, we copied the entire definition and measurement into our Google Sheet for further analysis. If the article does not provide conceptual definitions or measurements, we coded it as 0. We also coded whether

the cost and benefit variables were significantly related to disclosure behaviors. If the article results show a significant relationship, we coded it as 1; if not, we coded it as 0. Additionally, we recorded the general research method (e.g., survey, experiment, etc.), the platform used in the research (e.g., social media, e-commerce service, etc.), the name of the journal, and the country of the sample. The complete coding protocol can be found in the Appendix.

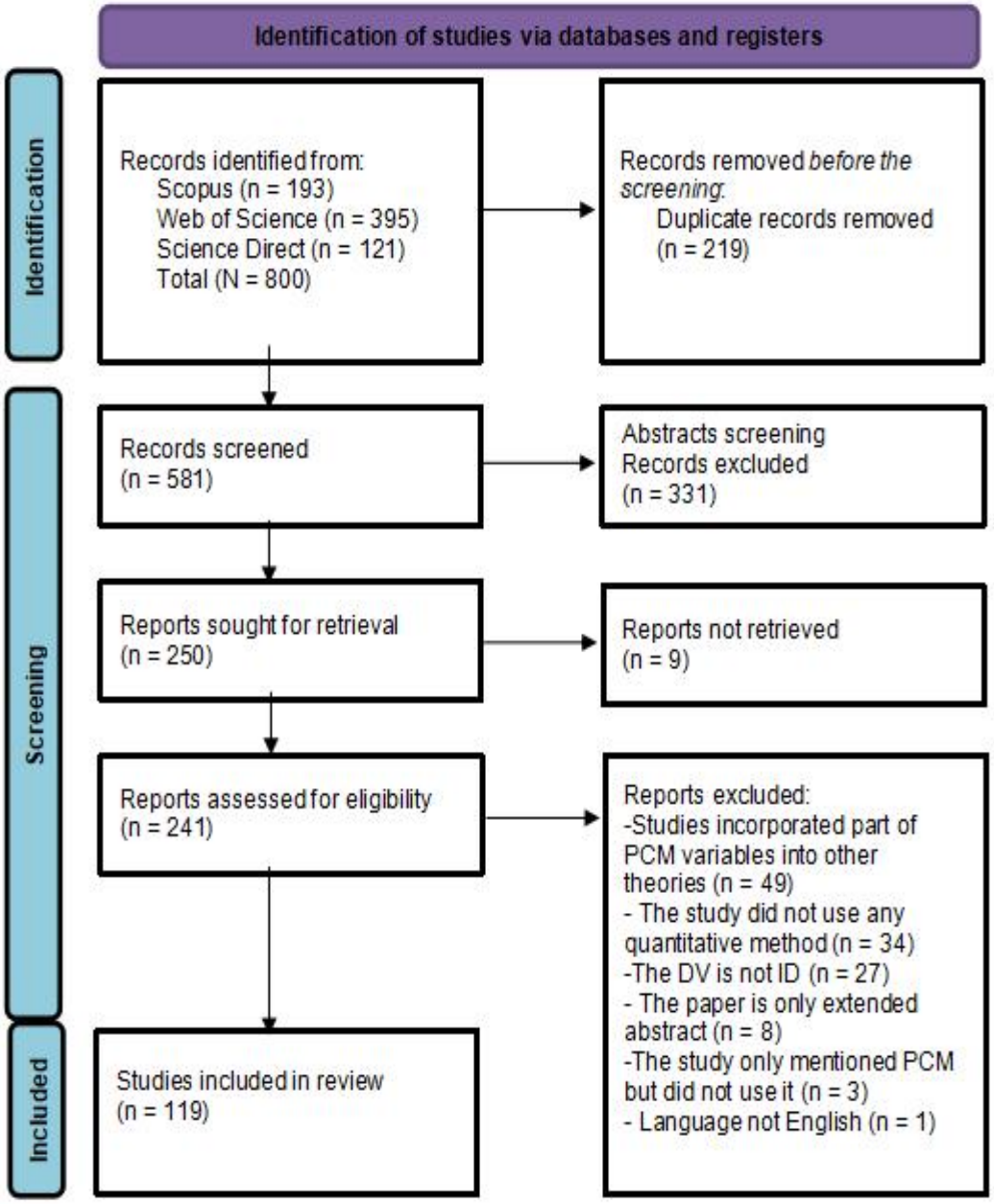

Figure 1. PRISMA Flow Diagram of Study Selection

Intercoder Reliability

After developing the initial coding protocol, the two authors tested it with a random subset of studies and revised it during coder training. During this process, they established a mutual understanding of each variable's definition, while the third author resolved any disagreements among the coders. Once the protocol was finalized, the two authors independently coded a random subset of articles (n=50) included in this review to assess inter-rater reliability. The variables' Scott's Pi, Cohen's Kappa, and Krippendorff's Alpha all exceeded 0.85. The two authors then coded additional subsets of the articles independently.

Table 1. Platforms of PCM Information Disclosure Behaviors

Information Disclosure Platform	No. of Studies
Social Media Platforms	33
Iot Services	29
Pandemic Tracing Apps	13
Mobile Apps	13
Ai-Powered Services	11
E-Commerce Platforms	7
E-Health	5
Location-Based Services	5
Wearable Technology	2
Biometric Technology	1

RESULTS

Alignment between Perceived Costs, Perceived Benefits and Self-Disclosure

RQ1 investigated whether dimensional alignment between independent variables (privacy costs/benefits) and dependent variables (disclosure behaviors) would enhance statistical relationships within the privacy calculus framework. Systematic coding of the literature yielded a noteworthy finding: among 24 articles reporting non-significant cost-disclosure relationships, dimensional misalignment characterized 16 studies (66%). Dimensional misalignment manifested in two distinct forms: (1) complete mismatch, wherein cost and disclosure variables assessed entirely different dimensions, and (2) partial mismatch, wherein variables shared one dimension while one measure incorporated additional dimensions absent from the other. For example, Lankton et al. (2020) operationalized perceived costs using both social and informational privacy dimensions, yet measured disclosure exclusively within the social dimension. Five articles have their cost variables dimensions align with their disclosure dimensions. The rest three articles did not specify their operational definition or provide measurement in their paper.

Analysis of articles with significant cost-disclosure relationships (n=95) revealed a markedly different pattern. Dimensional alignment characterized two-thirds of these studies (n=65, 68%), compared to only 32% among non-significant findings. Twenty-five articles (26%) exhibited misalignment despite obtaining significant results, while seven articles (6%) lacked sufficient measurement detail for alignment assessment.

Regarding the alignment between benefit and disclosure dimensions, only 20 of the 77 with significant relationship articles (26.0%) demonstrated alignment, while 34 articles (44.2%) did not align their benefit dimensions with their disclosure dimensions. The remaining 23 articles could not be assessed due to either unclassifiable benefit measurements (20 articles) or missing disclosure information (3 articles). These findings suggest that a substantial proportion of studies operationalize perceived benefits in dimensions that do not correspond to the type of disclosure behavior being measured.

Information Disclosure Behaviors

RQ2 (a) inquired about the conceptualization and operationalization of the information disclosure construct. The results indicated that 57 studies did not provide a definition for either the intention to disclose or ID, and 62 provided conceptual definitions. Of the remaining 62 articles with definitions, 15 were too general or described adoption/usage intentions without specifying the nature of information being disclosed. Among the 47 classifiable definitions, 34 were single-dimensional: 26 were purely informational; three were purely physical, referencing health data or the sharing of physical resources (Fernandes et al., 2023; Lutz et al., 2018; Chen et al., 2020); three were purely psychological, capturing the disclosure of feelings, emotions, or vulnerabilities (Siahaan et al., 2022; Jozani et al., 2020; Trepte et al., 2020); and two were purely social, describing online social connectivity or community participation (Choi et al., 2018; Hu et al., 2020). Thirteen definitions were multi-dimensional, with informational combined with physical being the most common pairing (six articles), frequently referencing both personal data and location or health information — largely driven by COVID-related studies. Informational combined with social appeared in three articles, while two definitions spanned three dimensions: Mwesiumo et al. (2023) (informational, physical, and social) and Ostendorf et al. (2022) (informational, psychological, and social). Overall, the informational dimension appeared in 38 of the 62 definitions (61.3%), followed by the physical dimension in 10 (16.1%), the social dimension in eight (12.9%), and the psychological dimension in six (9.7%).

Informational disclosure was measured most frequently (n=100 articles), followed by physical disclosure (n=17), social disclosure (n=14), and psychological disclosure (n=12). Regarding measurement comprehensiveness, the majority of studies employed unidimensional approaches: 89 articles (79%) measured only one disclosure dimension, while 24 articles (21%) incorporated multiple dimensions.

It also should be noted that seven studies used privacy management behaviors instead of disclosure behaviors as the dependent variable in the PCM. These privacy management behaviors encompass behaviors like misrepresentation (Tang & Ning, 2023), withholding information (Miltgen & Smith, 2019), disclosing false information (Miltgen & Smith, 2019; Tang & Ning, 2023), adjusting privacy settings (Li et al., 2019), regulating access to information (Choi et al., 2018; Li et al., 2019; Lankton et al., 2019), deleting inappropriate posts, and declining to use the service (Jiang et al., 2021). Five studies proved that privacy concerns were significantly related to privacy management behaviors, whereas all six studies proved that perceived benefits were significantly related to privacy management behaviors. This finding is in response to Dienlin and Metzger's (2016) argument that self-disclosure and self-withdrawal are no zero-sum relationship; instead, they are in dialectical tension with one another and should both be included in the PCM.

Additionally, 32 out of 119 studies used the PCM to examine self-disclosure behaviors, and 71 studies examined people's intention or willingness to disclose information. The majority of PCM studies used either the actual disclosure behavior or the intention to disclose as dependent variables. It is important to notice that there is an intention-behavior gap, and intention only explains 28% of variance in behaviors (Sheeran, 2002). Baruh et al. (2017) also found that intentions to disclose information received larger negative effects from privacy concerns than information disclosure behaviors. Thus, we suggest that future studies employing the PCM should test both intentions and behaviors to confirm the effects of PCM variables on the context-specific intentions and behaviors are in congruence.

R2(b) asked about how the PCM applies to disclosure behaviors other than self-disclosure. Unfortunately, no paper examined behaviors like other-generated behaviors with the PCM. However, it is an indisputable fact that people are socially interconnected and bonded with each other by sharing information (Kamleitner & Mitchell, 2019). Information is not individually owned but collectively owned (Peng, 2023). Privacy should not be viewed as personal but as interdependent. Everyone who holds information about other people can violate their privacy without even noticing (Kamleitner & Mitchell, 2019; Such & Craido, 2018). Therefore, the disclosure decision mechanism should not only be about how an individual independently evaluates the costs and benefits of disclosing information, but about how information owners jointly make the disclosure decision. Factors such as awareness of information co-ownership, anticipation of consequences to others, approval seeking before disclosing, and collective negotiation over disclosure should be incorporated into the PCM (Peng, 2023; Such & Craido, 2018). We call for the expansion of the PCM to encompass non-typical disclosure behaviors while integrating the aforementioned factors, in the hope of developing a more comprehensive theory that is suitable for understanding contemporary complex privacy practices.

Costs

Perceived Risks

RQ3(a) asked about how studies conceptualize and operationalize PR when using PCM. According to systematic review results, 57 articles used PR as a predictor of the PCM. Out of 57 articles, 39 provided conceptual definitions, which 18 failed to provide conceptual definitions for PR. Analysis of provided 42 definitions (three articles used two risk variables as predictors) showed that most articles defined PR as the potential loss associated with disclosing personal information, adopting the definition from Malhotra et al. (2004) or Dinev and Hart (2006). Eight definitions conceptualize PR as improper use of personal information by service providers or platforms. Three definitions emphasized unauthorized access, theft, or sharing of data (Trang & Weiger, 2021; Li et al., 2020; Esmaeilzadeh, 2019), while three defined risks as opportunistic behavior by providers or sellers (Nikkhah et al.,2020; Kummer et al., 2018; Venkatesh et al., 2021). Three articles defined risk as the expectation of the worst possible outcome, and one conceptualized it as the loss of control over personal information (Zhu et al., 2022; Jiang et al., 2022; Fan et al., 2021). Notably, these patterns frequently overlapped, with many definitions combining elements of potential loss and misuse or unauthorized access. Only a small number of articles, such as Trang (2021), Alkhalifah and Bukar (2022), Bo Hu et al. (2022), Abramova et al. (2022), and Huang and Huang (2023), explicitly incorporated multiple dimensions—including social, financial, or physical risks—into their conceptual definitions of perceived risk.

One important issue that emerges among conceptual definitions is that scholars confuse PR with PC when defining PR. However, PR conceptually differs from PC, as PR emphasizes the potential loss caused by ID whereas PC highlights the uncertain feelings of how the information will be used (Dienlin & Trepte, 2015). Given this distinction, only 17 out of the 59 studies correctly defined PR as a potential loss.

The operationalization of PR reflected the four-dimensional framework of privacy context. Of the 57 articles, 37 measured informational PR, followed by five that measured both informational and social dimensions, three that focused on the social dimension, three on the physical dimension, two that measured informational, social, and physical dimensions, and one that addressed informational and physical dimensions. The remaining six articles did not provide any measurement details. However, a significant issue emerging from these operationalizations is the mismatch between conceptual and operational definitions of perceived risk. While conceptual definitions tend to be broad in nature, the corresponding measurements often include narrowly specific risk-related items. For instance, Venkatesh et al. (2021) broadly defined PR as potential loss for customers, yet their scale measured financial risk, product-specific risks, and general risks.

Privacy Concerns

RQ3(b) also inquired about how previous PCM studies conceptualize and measure PC, with the focus on whether these studies included context-specific details in their conceptualization and measurement. According to the systematic review result, 62 studies used PC as the cost factor in the PCM. Out of the 62 studies, 44 provided conceptual definitions while 18 did not. Of the 44 definitions, 28 articles' conceptualization only focused on informational PC, encompassing concerns about the collection, use, misuse, unauthorized access or disclosure of personal information. Six definitions spanned two dimensions, all of which included the informational dimension alongside one other: two combined informational with social (Kim & Kim, 2020; Jozani et al., 2020), two combined informational with physical (Sun et al., 2019; Shin et al., 2022), and two combined informational with psychological (Willems et al., 2023; Shih & Liu, 2023). Notably, no definition was purely social or purely psychological, and only one definition — Lutz et al. (2018), which addressed physical intrusions, material losses, and infringements on the extended self.

Thirty-nine articles only measured informational PC, followed by 12 articles measured both informational and social PC, four articles measured both informational and physical PC, two articles measured physical PC, and one article measured informational, social and physical PC. The rest two articles did not provide detailed measurement.

Moderators

RQ4 inquired about what moderators could be incorporated into the PCM. There are ten articles incorporating moderators that are significantly influencing the relationship between privacy concerns and disclosure behaviors. Some moderators are individual characteristics (n=7), whereas some moderators are contextual cues (n=3) as shown in **Table 2**.

Individual characteristic moderators include information asymmetry (Wang et al., 2019), information of privacy harms (Wang et al., 2019), privacy self-efficacy (Kang & Oh, 2023), cognitive absorption (Trang & Weiger, 2021), and personality trait like factors (Choi et al., 2018; Meier et al., 2023; Nikkhah et al., 2022). This finding is consistent with Kokolakis (2017) and Gerber et al. (2018)'s explanations and interpretations of the privacy paradox. For example, Kokolakis (2017) proposed that incomplete information and information asymmetry can affect privacy decision-making. Lacking access to relevant information about disclosure risks and benefits can bias people's judgements about the trade-offs and subsequently make seemingly irrational disclosure decisions. People's confidence in privacy knowledge and management (a.k.a privacy self-efficacy) can also optimistically bias perceptions of privacy risks, which encourages disclosure behavior and discourages the control behavior (Gerber et al., 2018; Kang & Oh, 2023). We also found that personality trait-like factors also play an important role in modulating privacy decision-making processes. Compared with privacy self-efficacy and information asymmetry, personality trait factors are more stable across various situations and can shape people's perceptions about the situation and indirectly affect their behaviors (Meier et al., 2023). For example, Nikkhah et al. (2022) found that people with higher stability traits tended to stay away from risks and disclose less information, whereas people with higher plasticity traits tended to explore new opportunities and disclose more information.

In addition to the factors mentioned above, other theoretical factors, cognitive factors (e.g., availability bias, confirmation bias), attitudinal factors (e.g., attitudes toward apps), informational factors (e.g., personal experiences of privacy violations), and emotional factors (e.g. valence effect) also require future empirical evidence to explore their roles in the privacy decision mechanism (Barth & De Jong, 2017). We also recommend future studies to explore factors like contextual cues in the PCM. Contextual cues hold equal importance to individual traits, as they can trigger specific cognitive responses or heuristics, leading individuals to make more convenient privacy decisions (Kang & Oh, 2023). For example, Trang & Weiger (2021) found that gamified services trigger people's immersion in challenge, which limits their cognitive capacity to rationally analyze the tradeoffs between costs and benefits, leading them to make short-cut decisions. Therefore, future studies can investigate how contextual cues trigger certain reactions or perceptions that influence privacy-related decisions.

Table 2. Moderators Included in the PCM

Articles	Moderating Cost Variables	Moderating Benefits Variables
Chatterjee et al.(2021)	Regulation (+)	Leadership Support (+)
Chatterjee et al. (2021)	Regulation (-)	Incentivization (+)
Wang et al. (2019)	Information Asymmetry (-), Privacy Harms (-), Disclosure Of Friends (+)	Flow Experience (+)
Choi et al. (2018)	Dispositional Privacy Concerns (-)	Dispositional Privacy Concerns (+)
Hu et al. (2020)	Trust (-)	
Kang & Oh (2023)	Privacy Self-Efficacy (+)	Privacy Self-Efficacy (+)
Nikkhah et al. (2022)	Stability (-), Plasticity (-)	Stability (-), Plasticity (+)
Ying et al. (2023)		Desire To Share Moderate The Route From Benefit Variable To Both Dvs
Trang & Weiger (2021)	Cognitive Absorption (-)	Cognitive Absorption (+)
Meier et al. (2023)		Need For Privacy (-)

Benefits

Perceived Benefits

RQ5 asked about how prior PCM studies conceptualize and operationalize PB in the PCM. According to review results, 86 studies provided conceptual definitions, whereas 33 articles did not provide conceptual definition for benefit variables. Eighty-eight articles used benefit related variables such as perceived benefit, convenience, social benefits, as perceived benefit in the PCM. The rest 31 articles used other variables such as trust, perceived control as offset variables to costs variables in the PCM. Our analysis for PB is based on the 88 articles. However, the conceptualization and operationalization vary significantly from each other.

Eighty-eight articles remained with a total of 114 benefit variables. Among these, 37 variables (32.5%) lacked a conceptual definition or were too vague to classify into any specific dimension. Of the 77 classifiable variables, 36 were purely informational, describing benefits in terms of personalization, convenience, efficiency, or service access. Fourteen variables were purely social, often referencing social connection, community belonging, or reciprocal benefits. Nine variables were purely psychological, capturing aspects such as enjoyment, self-expression, or hedonic gratification. No variable was purely physical — the physical dimension appeared in only four variables (3.5%) and always co-occurred with informational or social dimensions, typically referencing location-based value or physical movement. Eighteen variables were multi-dimensional, with informational combined with social being the most common pairing (6 variables), followed by social combined with psychological (4 variables) and informational combined with physical (3 variables). Two variables spanned three dimensions — informational, social, and psychological (Zhu et al., 2022; Wottrich et al., 2018).

At the operational definition level, 114 benefit variables were analyzed across the 88 articles. Of these, 30 variables (26.3%) could not be classified because the operational definitions was not provided or provided items too vague to categorize. Among the 84 classifiable variables, 35 were purely informational — typically measured through items related to personalization, convenience, efficiency, or service usefulness. Fifteen variables were purely social, often capturing relationship building, community belonging, or reciprocal benefits. Eleven variables were purely psychological, measured through items reflecting enjoyment, self-expression, self-presentation, life documentation, or emotional satisfaction. Only one variable was purely physical (Alkhalifah et al., 2022). Twenty-two variables were multi-dimensional, with informational combined with social, informational combined with physical, and social combined with psychological each appearing four times as the most common pairings. Three variables spanned informational, social, and psychological dimensions (Kezer et al., 2022; Trepte et al., 2020; Ashuri et al., 2018), and one captured physical, social, and informational dimensions (Ying et al., 2023). Compared to the conceptual definitions, operational definitions revealed higher representation of the psychological dimension (n = 19) and the physical dimension (n=7), suggesting that actual measurement items often capture more nuanced aspects of benefits than the broader conceptual framing indicates.

Other Factors

Besides perceived benefit as the primary variable that may override the effects of cost variables (RQ6), we

also found other variables were also included in the privacy calculus model, such as trust (n=22), personal interest (n=5), perceived control (n=5), social norms (n=4), privacy self-efficacy (n=2), perceived security (n=1), perceived transparency (n=1).

Trust, as the variable most frequently included in the PCM, refers to users' willingness to be vulnerable to some actions because they believe the website, SNS, providers, or apps will be reliable and confidentially handle their personal information (Bol et al., 2022, Dinev & Hart., 2006a). Of 22 papers that used trust, 19 papers empirically validated that trust is an important and positive variable associated with the information disclosure behavior or intention: when users consider the technology will exhibit ethical behaviors of protecting their personal information from improper access or unauthorized second use, they are more likely to share information on the technology. Moreover, trust has also been found to have a significant impact on offsetting privacy concerns or privacy risks, especially when privacy concerns or risks are associated with disclosing information on a platform (Duan & Deng, 2022; Jiang et al., 2022; Siahaan et al., 2022). In fact, trust is conceptually opposite to privacy concerns. Trust emphasizes the belief that a system or others will protect disclosed information, whereas privacy concerns emphasize the anxiety that a system or others will misuse the information. Therefore, based on the results of our systematic review regarding the influence of trust on disclosure behaviors and privacy concerns, we recommend that scholars incorporate trust as the opposite variable to privacy concerns within the PCM.

The goal of the present study is to systematically review 119 studies that employed the PCM to examine information disclosure behaviors and to propose an integrated model that addresses the dimensional misalignment issue between predictor and outcome variables. Although we proposed that information disclosure also encompasses other-generated disclosure, our evidence and results are based entirely on self-disclosure behaviors. Results revealed that dimensional alignment between cost and disclosure variables significantly influenced the detection of significant relationships. Specifically, 66% of studies with non-significant cost-disclosure results had misaligned dimensions, compared to only 26% among significant studies, suggesting that many null findings may reflect measurement misalignment rather than theoretical failure. This pattern did not hold on the benefit side, where only 26% of significant studies demonstrated alignment, indicating that benefit variables may operate more diffusely across privacy dimensions. The review also uncovered considerable inconsistency in the conceptualization and operationalization of core PCM variables. Disclosure, cost, and benefit constructs were predominantly operationalized within the informational dimension, while social, psychological, and physical dimensions remained underrepresented. Based on these findings, we propose an integrated model as shown in **Figure 2,** that emphasizes dimensional alignment across costs, benefits, and disclosure variables within the four-dimensional privacy framework (informational, social, psychological, and physical).

DISCUSSION

More Contextual-Specific Conceptualization and Operationalization of Disclosure, Costs, and Benefits

Privacy is context-dependent (Acquisti et al., 2015). Privacy-related behaviors and perceptions should be understood, discussed, and investigated within the framework of their context (Nissenbaum, 2010). Privacy perceptions and behaviors are all influenced by the same contextual factors. Instead of using broad operationalizations to measure costs, benefits, and disclosure behaviors, we propose that future studies consider contextual factors and align the dimensions of variables' conceptualization and operationalization with the context in the PCM. Our systematic review revealed that aligning cost and disclosure dimensions was more likely to yield significant relationships, which strongly suggests that non-significant cost-disclosure results may reflect measurement misalignment rather than theoretical failure: respondents may have been considering concerns in one dimension while researchers measured disclosure in another. Our findings support Dienlin and Trepte's (2015) proposition that aligning the dimensions of privacy perceptions and privacy behaviors can improve the rate of significant results.

It is interesting to find that only 26% (n = 20) of significant result studies aligned benefit and disclosure dimensions, while 44% (n = 34) misaligned the two, suggesting that alignment between benefits and disclosure is not as crucial for producing significant results. Given half of these studies (n = 16) used multidimensional measurement, one explanation is that benefit variables are more generalizable and transferable across dimensions than cost variables. Also, nine articles used benefit variables like enjoyment or satisfaction, it is possible that when benefit variables are affective in nature, such as enjoyment, gratification, or hedonic pleasure, affective heuristics may play a significant role in the disclosure decision, with individuals relying on their emotional states rather than deliberate analysis to guide behavior (Gerber et al., 2018). This raises an important theoretical consideration: when perceived benefits are primarily affective, scholars should consider whether a dual-process framework

might better capture the privacy calculus, as perceived benefits and perceived costs may not be processed through the same cognitive route. Specifically, affective benefits may be processed through a fast, automatic, and holistic route (System 1), whereas perceived costs may be processed through a more deliberate, analytical route (System 2). When System 1 is activated, dimensional alignment may have less influence on the outcome, as individuals rely primarily on affective heuristics to guide their disclosure decisions. However, when System 2 is activated, individuals engage in deliberative evaluation of costs and benefits, making dimensional alignment a more critical factor in determining disclosure behavior. Future research should empirically examine whether affective benefits (e.g., enjoyment, gratification) differ from non-affective benefits (e.g., personalization, convenience) in their influence on disclosure behaviors.

Although our systematic review focused on self-disclosure and found no studies that have examined other-generated disclosure using the PCM, we strongly recommend that future research address this gap. Other-generated disclosure is not a new concept; since the context collapse brought by social media (Marwick & Boyd, 2011), individuals' information can be inevitably shared by others, and the process of negotiating privacy boundaries with those who possess one's information differs fundamentally from self-disclosure. The four-dimensional framework of privacy context is equally applicable to other-generated disclosure scenarios. For example, when parents share their children's information online, this form of disclosure involves informational, social, and physical privacy contexts. Accordingly, the costs associated with such disclosure span multiple dimensions, including informational concerns (e.g., unauthorized collection of children's personal data), social concerns (e.g., reputational damage to the child), and physical concerns (e.g., increased risk of kidnapping or stalking). Applying the dimensional alignment framework to other-generated disclosure could yield valuable insights into how privacy trade-offs operate when the discloser and the information subject are different individuals.

While most studies use general definitions and operationalizations of these constructs, some have adopted a more context-specific approach. **Table 3** provides an overview of variables used in PCM studies, including granular and context-specific variables. For instance, in the context of social media platforms, perceived benefits extend beyond the general benefits of information disclosure to include concepts such as social rewards, social capital, and self-enhancement, all of which can be categorized as social benefits. Similarly, perceived risks in the social media context encompass not only general concerns like information loss but also psychological risks such as cyberbullying.

Table 3. Benefits and Cost Variables Used in Different Platforms

Benefit Variables	Cost Variables	Platforms
• Perceived Benefits • Trust • Personal Interest • Social Capital • Social Rewards • Number Of Friends • Privacy Self-Efficacy • Self-Expression/Self-Enhancement/Self-Presentation • Life Documentation • Efficiency • Perceived Usefulness • Co-Created Value • Perceived Controllability	• Perceived Risk • Privacy Concerns • Information Security • Perception Of Losses • Institutional Privacy Concerns • Social Privacy Concerns • Cyberbullying Risk • Perceived Intrusion	Social Media Platforms
• Perceived Benefits • Personalization Value • Trust • Conditional Value • Ease Of Use • Convenience	• Privacy Concerns • Perceived Risk • Perceived Physical Privacy Risks • Perceived Informational Privacy Risks	Iot Services
• Social Benefits • Economic Benefits/Monetary	• Perceived Cost	

Benefit Variables	Cost Variables	Platforms
• Social Benefits • Benefits • Perceived Control		
• Perceived Benefits • Perceived Usefulness • Perceived Security • Trust • Perceived App Value • Enjoyment • Satisfaction	• Privacy Concerns • Perceived Risk • App Intrusiveness	Mobile Apps
• Perceived Benefits • Perceived Usefulness • Trust • Privacy Self-Efficacy • Social Influence • Novelty • Convenience	• Privacy Concerns • Perceived Risks • Financial Risk	Ai-Powered Services
• Perceived Benefits • Personal Interest • Utilitarian Benefits • Hedonic Benefits	• Privacy Concerns • Perceived Risks • Perceived Losses	E-Commerce Platforms
• Perceived Benefits • Trust • Health Benefits • Social Influence • Individual Benefits/Social Benefits • Social Interaction • Reciprocal Benefits	• Privacy Concerns • Perceived Risks • Individual Privacy Risk • Social Privacy Risk	Pandemic Tracing Apps
• Perceived Benefits • Information Support • Emotional Support	• Privacy Concerns • Perceived Risks • Lack Of Privacy Control • Health Information Privacy Concerns	E-Health
• Benefits Of Disclosing Information • Advertising Value • Personalization • Monetary Rewards	• Privacy Concerns • Perceived Risks • Perceived Intrusiveness • Reasons Against Location Tracking	Location-Based Services
• Perceived Benefits • Perceived Value	• Privacy Concerns • Perceived Risks	Wearable Technology
• Personalization	• Privacy Concerns	Biometric Technology

Actual behavior or Intention

Besides the issue that using specific privacy concerns to predict general disclosure behavior might lead to inconsistent results, we found that predicting disclosure intention or willingness instead of actual behavior might also be the reason that leads to unexpected outcomes. We found that of 44 insignificant results (including costs variables and benefits variables), 29 papers used disclosure intention or willingness as the dependent variable instead of the actual disclosure behavior as mentioned in (see appendix **Table 1** & **Table 2)**. However, the intention does not guarantee the realization of corresponding actions. Norberg et al. (2007) found that people disclose more information than they intended to. Given the limited empirical evidence showing the discrepancy between intended and actual behavior in existing PCM studies, we suggest that future scholars examine both disclosure intention and actual disclosure behaviors and compare the influence of PCM on these two variables separately.

Making the Privacy Trade-off Commensurable

As a typical cognitive trade-off, the PCM also has a fundamental incommensurable problem created by the absence of a common scale for translating competing values into each other (Tetlock et al., 2000). A reasonable trade-off requires an interdimensional comparison to enable people to reliably evaluate the benefits and costs. For an individual, it is easier to compare risks of reputation damage and benefits of making new friends resulting from the behavior posting one's photos on social media than to compare the misuse of information by a company with financial benefits, as the former share a common framework for assessing the values of loss and gain. Therefore, we propose that the trade-off in the PCM should overcome the incommensurable obstacle and rely on a unified framework that allows for the assessment of benefits and costs within the same conceptual dimension.

Building on previous research and our findings, we propose applying the PPM's four-dimensional privacy framework (informational, social, psychological, and physical) to the core variables of the PCM (see Table 4). When employing the PCM to examine a disclosure behavior, scholars should first identify which privacy dimensions are salient within the disclosure context, then incorporate dimension-specific perceptions into the model. For example, an individual developing a friendship with an AI companion, engaging in frequent conversations and disclosing personal feelings and secrets, operates within both social and psychological privacy contexts. The individual is likely to consider psychological costs (e.g., concern that the AI might exploit disclosed secrets to manipulate or harm the individual) and social costs (e.g., fear that intimate disclosures could be exposed to others), as well as corresponding benefits such as psychological gains (e.g., receiving emotional support and a sense of being understood) and social gains (e.g., companionship and a sense of relational connection). Critically, the operationalization of cost and benefit variables should be dimensionally aligned with the disclosure behavior being predicted, reducing the risk of attenuated relationships due to dimensional misalignment.

Table 4. Recommended Conceptualizations and Operationalizations of Each Variable in the PCM

Variables	Definition	Dimensions
Information Disclosure	Information Disclosure (ID) refers to the act of revealing personal or sensitive information by individuals in various contexts, influenced by advanced technologies and social practices. In the context of PCM, ID reflects the competing needs and motivations that individuals navigate during disclosure. This multifaceted concept encompasses the dynamic management of information flow, balancing general behavior of disclosure, trade-offs involving information goods, manipulation and refusal of information, as well as social and altruistic purposes. In interdependent privacy context, information disclosure also refers to disclosure of others' information.	Informational Disclosure
		Social Disclosure
		Psychological Disclosure
		Physical Disclosure
Privacy Concerns	Privacy concerns refer to the uncertainties and apprehensions individuals have about the handling of their personal information.	Informaitonal Concerns
		Social Concerns
		Psychological Concerns
		Physical Concerns
Trust	Trust refers to users' confidence that service providers or other individuals will reliably and securely handle their disclosed information. Trust can be divided into two categories: vertical (or institutional) trust, which pertains to trust in service providers, and horizontal (or social) trust, which pertains to trust in other users.	Horizontal (Or Social)
		Vertical (Or Institutional)
Perceived Risks	Perceived risk refers to the perceived possibility of experiencing loss related to the disclosure of personal information online.	Informational Risk
		Social Risk
		Psychological Risk

Variables	Definition	Dimensions
		Physical Risk
Perceived Benefits	Perceived benefits refer to the rewards or gains individuals expect to receive from disclosing personal information.	Informational Benefit
		Social Benefit
		Psychological Benefit
		Physical Benefit

Toward an Integrated PCM Model

One of the biggest criticisms faced by the PCM is that it assumes the information disclosure process is guided by rational cost-benefit calculations, in which people are analytical and conscious when maximizing benefits and minimizing risks. Many studies have provided empirical evidence to prove that heuristic thinking, immediate gratification, incomplete information, personal habits, and contextual cues can all bias people's decision-making and distort the rational cost-benefit calculation (Barth & De Jong, 2017; Kokolakis, 2017). Therefore, we encourage future scholars to actively incorporate other factors proposed by previous studies in the PCM to improve the theory's precision in prediction and explanation. For instance, Wang et al.(2019) integrated the perspective of heuristic shortcuts into the PCM to explain the self-disclosure behavior, which not only addresses the PCM's limitations concerning heuristic thinking but also enhances the theory's precision in predicting disclosure behavior.

Out of 119 reviewed studies, only 10 studies incorporated moderators, and 40 papers incorporated other factors that can also override privacy concerns. Therefore, we think more attempts should be made to achieve a more comprehensive PCM. Future researchers can test possible factors or moderators from four perspectives: psychological or cognitive biases, contextual cues, and information types. Seven out of 10 studies focused on incorporating cognitive factors. More attention and efforts can be concentrated on contextual cues and information types (Barth & de Jong, 2017; Kokolakis, 2017). Privacy behavior is highly influenced by disclosing context (Morando et al., 2014). People could have different disclosure behaviors in different contexts. Instead of generalizing results across various contexts, more empirical studies should be conducted to find the privacy behavior pattern in certain contexts. Also, different types of information will be treated differently. Sensitivity of information could be a critical moderator, which, however, is not observed in reviewed studies. Therefore, future researchers can look into how information types and properties influence the privacy disclosure mechanism

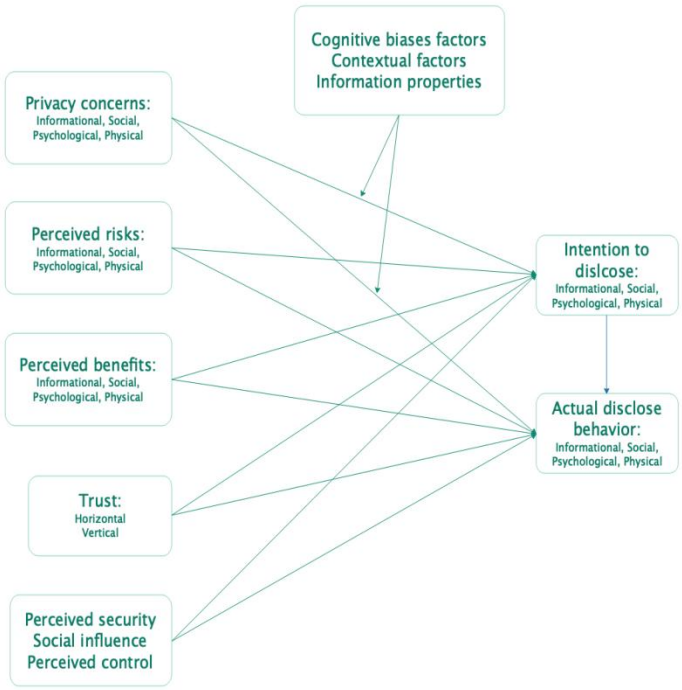

Figure 2. An Integrated Framework of the PCM Incorporating Dimensional Alignmenta and Additional Factors

CONCLUSION

The purpose of this study is to address the limitations of the PCM and improve its predictability by conducting a systematic review of 119 existing studies. Drawing on the principle of compatibility and the Privacy Process Model's four-dimensional framework, we proposed that dimensional alignment between independent variables (e.g., costs, benefits) and dependent variables (e.g., disclosure behaviors) can improve the predictability of the PCM. The systematic review results partially corroborated our hypothesis, especially on the cost side: a substantial share of null findings in the PCM literature reflect dimensional misalignment between predictor and outcome variables. Beyond measurement issues, the review highlighted the underuse of moderating variables and the limited scope of PCM research, which has yet to engage with other-generated disclosure behaviors. Based on these findings, we propose an integrated framework recommending that future PCM research align the dimensions of independent variables and disclosure behaviors with their specific privacy contexts in measurement, incorporate trust as a structural counterpart to privacy concerns, and expand the model to account for moderators, cognitive heuristics, and the increasingly complex landscape of information sharing enabled by emerging technologies.

LIMITATIONS

This study has two limitations that should be acknowledged. First, our paper primarily provides a theoretical discussion on the conceptualization and operationalization of variables within the Privacy Calculus Model (PCM). While we offer insights and recommendations, further empirical studies are necessary to determine which measurements should be used and to test the effectiveness of the alignment in measurements of variables. Second, our review only covers studies published between 2018 and 2023. With the emergence of generative AI, the context and behaviors surrounding information disclosure are likely to evolve significantly. Therefore, future research should focus on the implications of AI advancements on information disclosure, ensuring that the PCM remains relevant in the face of rapid technological change. More attention and discussion are needed to address these evolving contexts and behaviors in the privacy literature.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology: The Official Journal of the Society for Consumer Psychology, 30*(4), 736–758. https://doi.org/10.1002/jcpy.1191

Abramova, O., Wagner, A., Olt, C. M., & Buxmann, P. (2022). One for all, all for one: Social considerations in user acceptance of contact tracing apps using longitudinal evidence from Germany and Switzerland. *International Journal of Information Management, 64*, 102473.

Alkhalifah, A., & Bukar, U. A. (2022). Examining the prediction of COVID-19 contact-tracing app adoption using an integrated model and hybrid approach analysis. *Frontiers in Public Health, 10*, 847184 .

Baek, Y. M., Kim, E.-M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 31*, 48–56. https://doi.org/10.1016/j.chb.2013.10.010

Barth, S., & De Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartol, J., Vehovar, V., & Petrovčič, A. (2023). Systematic review of survey scales measuring information privacy concerns on social network sites. *Telematics and Informatics, 85*, 102063. https://doi.org/10.1016/j.tele.2023.102063

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

Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior, 19*(4), 451–467.

Breuer, J., Weller, K., & Kinder-Kurlanda, K. (2023). The role of participants in online privacy research: Ethical and practical considerations. In *The Routledge handbook of privacy and social media* (pp. 314–323). Routledge.

Bol, N., & Antheunis, M. L. (2022). Skype or skip? Causes and consequences of intimate self-disclosure in computer-mediated doctor-patient communication. *Media Psychology, 25*(5), 706–723.

Burgoon, J. K. (2012). Privacy and communication. In *Communication Yearbook 6* (pp. 206–249). Routledge.

Chatterjee, S., Chaudhuri, R., Vrontis, D., & Hussain, Z. (2023). Usage of smartphone for financial transactions: From the consumer privacy perspective. *Journal of Consumer Marketing, 40*(2), 193–208. https://doi.org/10.1108/jcm-03-2021-4526

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, J. V., Biamukda, S., & Tran, S. T. T. (2020). Service providers' intention to continue sharing: The moderating role of two-way review system. *Industrial Management & Data Systems, 120*(8), 1543–1564.

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

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

De Wolf, R. (2020). Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society, 22*(6), 1058–1075. https://doi.org/10.1177/1461444819876570

Dienlin, T. (2014). The privacy process model. *Medien und Privatheit*, 105–122.

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

Dienlin, T. (2023). Privacy calculus. In *The Routledge handbook of privacy and social media* (pp. 70–79). Routledge.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

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.

Duan, S. X., & Deng, H. (2022). Exploring privacy paradox in contact tracing apps adoption. *Internet Research, 32*(5), 1725–1750. https://doi.org/10.1108/intr-03-2021-0160

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics, 65*, 101717.

Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. Psychology Press.

Fox, G., Van Der Werff, L., Rosati, P., Takako Endo, P., & Lynn, T. (2022). Examining the determinants of acceptance and use of mobile contact tracing applications in Brazil: An extended privacy calculus perspective. *Journal of the Association for Information Science and Technology, 73*(7), 944–967.

Fox, G., Clohessy, T., Van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior, 121*, 106806. https://doi.org/10.1016/j.chb.2021.106806

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing, 58*(2), 1. https://doi.org/10.2307/1252265

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Hong, S. J., & Cho, H. (2023). Privacy management and health information sharing via contact tracing during the COVID-19 pandemic: A hypothetical study on AI-based technologies. *Health Communication, 38*(5), 913–924.

Hu, T., Wang, K. Y., Chih, W., & Yang, X. H. (2020). Trade off cybersecurity concerns for co-created value. Journal *of Computer Information Systems, 60*(5), 468–483.

Ingber, A. S. (2026). Screenshots in human communication research: Protecting privacy in light of law, ethics and user expectations. *New Media & Society*, 14614448251413695.

Jiang, X., Goh, T.-T., & Liu, M. (2022). On students' willingness to use online learning: A privacy calculus theory approach. *Frontiers in Psychology, 13*, 880261. https://doi.org/10.3389/fpsyg.2022.880261

Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*, 106260.

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing, 38*(4), 433–450. https://doi.org/10.1177/0743915619858924

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

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635. https://doi.org/10.1111/isj.12062

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).

Kim, B., & Kim, D. (2020). Understanding the key antecedents of users' disclosing behaviors on social networking sites: The privacy paradox. *Sustainability, 12*(12), 5163.

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

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

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research, 126*, 221–238. https://doi.org/10.1016/j.jbusres.2020.12.006

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

Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2020). Understanding the antecedents and outcomes of Facebook privacy behaviors: An integrated model. *IEEE Transactions on Engineering Management, 67*(3), 697–711. https://doi.org/10.1109/tem.2019.2893541

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 862–877. https://doi.org/10.1016/j.ijhcs.2013.01.005

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

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society, 21*(10), 1472–1492.

Ma, X., Qin, Y., Chen, Z., & Cho, H. (2021). Perceived ephemerality, privacy calculus, and the privacy settings of an ephemeral social media site. *Computers in Human Behavior, 124*, 106928. https://doi.org/10.1016/j.chb.2021.106928

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

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

Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 114–133.

Miltgen, C. L., & Smith, H. J. (2019). Falsifying and withholding: Exploring individuals' contextual privacy-related decision-making. *Information & Management, 56*(5), 696–717. https://doi.org/10.1016/j.im.2018.11.004

Morando, F., Iemma, R., & Raiteri, E. (2014). Privacy evaluation: What empirical research on users' valuation of personal data tells us. *Internet Policy Review, 3*(2). https://doi.org/10.14763/2014.2.283

Mwesiumo, D., Halpern, N., Budd, T., Suau-Sanchez, P., & Bråthen, S. (2021). An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns. *Journal of Business Research, 136*, 63–75. https://doi.org/10.1016/j.jbusres.2021.07.027

Nabity-Grover, T., Cheung, C. M., & Thatcher, J. B. (2023). How COVID-19 stole Christmas: How the pandemic shifted the calculus around social media self-disclosures. *Journal of Business Research, 154*.

Nikkhah, H. R., & Sabherwal, R. (2022). Information disclosure willingness and mobile cloud computing collaboration apps: The impact of security and assurance mechanisms. *Information Technology & People, 35*(7), 1855–1883. https://doi.org/10.1108/itp-12-2019-0630

Nikkhah, H. R., Sabherwal, R., & Sarabadani, J. (2022). Mobile cloud computing apps and information disclosure: The moderating roles of dispositional and behaviour-based traits. *Behaviour & Information Technology, 41*(13), 2745–2761. https://doi.org/10.1080/0144929x.2021.1946591

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48.

Ostendorf, S., Meier, Y., & Brand, M. (2022). Self-disclosure on social networks: More than a rational decision-making process. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(4).

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International Business Review, 29*(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717

Peng, Z. (2023). A privacy calculus model perspective that explains why parents sharent. *Information,* Communication *& Society*, 1–24. https://doi.org/10.1080/1369118x.2023.2285462

Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: Socio-demographic and attitudinal influences on privacy and disclosure choices. *Journal of Marketing Management, 36*(5–6), 519–549. https://doi.org/10.1080/0267257x.2020.1715465

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

Sheeran, P. (2002). Intention–behavior relations: A conceptual and empirical review. *European Review of Social Psychology, 12*(1), 1–36. https://doi.org/10.1080/14792772143000003

Shin, D., Kee, K. F., & Shin, E. Y. (2022). Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms? *International Journal of Information Management, 65*, 102494.

Siahaan, M. N., Handayani, P. W., & Azzahro, F. (2022). Self-disclosure of social media users in Indonesia: The influence of personal and social media factors. *Information Technology & People, 35*(7), 1931–1954. https://doi.org/10.1108/itp-06-2020-0389

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Such, J. M., & Criado, N. (2018). Multiparty privacy in social media. *Communications of the ACM, 61*(8), 74–81. https://doi.org/10.1145/3208039

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability, 11*(12), 3311.

Tang, Y., & Ning, X. (2023). Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems, 165*, 113881. https://doi.org/10.1016/j.dss.2022.113881

Tetlock, P. E., Lupia, A., McCubbins, M. D., & Popkin, S. L. (2000). Coping with trade-offs: Psychological constraints and political implications. In *Elements of reason: Cognition, choice, and the bounds of rationality* (pp. 239–263).

Trang, S., & Weiger, W. H. (2021). The perils of gamification: Does engaging with gamified services increase users' willingness to disclose personal information? *Computers in Human Behavior, 116*, 106644. https://doi.org/10.1016/j.chb.2020.106644

Trepte, S. (2023). *The Routledge handbook of privacy and social media*. Routledge.

Trepte, S. (2021). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory, 31*(4), 549–570. https://doi.org/10.1093/ct/qtz035

Venkatesh, V., Hoehle, H., Aloysius, J. A., & Nikkhah, H. R. (2021). Being at the cutting edge of online shopping: Role of recommendations and discounts on privacy perceptions. *Computers in Human Behavior, 121*, 106785.

Wang, L., Hu, H.-H., Yan, J., & Mei, M. Q. (2019). Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management, 33*(2), 353–380. https://doi.org/10.1108/jeim-05-2019-0121

Wang, N., Zhang, B., Liu, B., & Jin, H. (2015). Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*.

Warshaw, J., Matthews, T., Whittaker, S., Kau, C., Bengualid, M., & Smith, B. A. (2015). Can an algorithm know the "real you"? Understanding people's reactions to hyper-personal analytics systems. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 797–806).

Widmer, G., & Kubat, M. (1996). Learning in the presence of concept drift and hidden contexts. *Machine Learning, 23*(1), 69–101. https://doi.org/10.1007/bf00116900

Willems, J., Schmid, M. J., Vanderelst, D., Vogel, D., & Ebinger, F. (2023). AI-driven public services and the privacy paradox: Do citizens really care about their privacy? *Public Management Review, 25*(11), 2116–2134.

Wottrich, V. M., Van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52.

Ying, S., Huang, Y., Qian, L., & Song, J. (2023). Privacy paradox for location tracking in mobile social networking apps: The perspectives of behavioral reasoning and regulatory focus. *Technological Forecasting and Social Change, 190*, 122412.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110. https://doi.org/10.1207/s15506878jobem4901_6

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*.

Zhu, X., Cao, Q., & Liu, C. (2022). Mechanism of platform interaction on social media users' intention to disclose privacy: A case study of TikTok app. *Information (Basel), 13*(10), 461. https://doi.org/10.3390/info13100461

APPENDIX

Table 1. Studies with Insignificant Relationships Between Id and Cost Variables

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
Jiang X.; Goh T.-T.; Liu M.	On Students' Willingness to Use Online Learning: A Privacy Calculus Theory Approach	willingness to use online learning	—	privacy perception	privacy perception is the degree to which an individual perceives their right to control personal information.	1. I think of privacy as a right that I can control and use. 2. Controlling privacy is very important to me. 3. I think it's very important to know how my personal information is being used. 4. When an online learning platform asks me to provide personal information, I need to weigh the risk.
Liu J.; Skoric M.M.; Li C.	Disentangling the relation among trust, efficacy and privacy management: a moderated mediation analysis of public support for government surveillance during the COVID-19 pandemic	public support for government surveillance	surveillance support: means to relinquish control over their personal information and subject oneself to others' action.	perceived cost of info disclosure	refer to the expected negative outcomes of information disclosure which often motivate people to take privacy protection behaviours or reduce self-disclosure (Dienlin and Metzger 2016; Wu et al. 2012).	respondents were asked to indicate their level of concern for below items regarding data privacy when they perform online activities on 7-point scale (1 = 'not concerned at all' to 7 = 'very concerned'):(1) your identity being used by somebody else; (2) being asked for your personal information when registering or making online purchases; (3) someone accessing your medical records electronically; (4) someone stealing of your credit card details when making online purchases.
Fernandes T.; Costa M.	Privacy concerns with COVID-19 tracking apps: a privacy calculus approach	willingness to disclose personal information	willingness to disclose health information refers to the extent to which one is likely to voluntarily share his/her personal health-related data through COVID-19 contacttracing apps while opt-in intention refers to the actual adoption and usage of the technology	lack of privacy control	the level of control one perceives to have over factors that might interfere with certain behaviors	1. I believe I have no control over … who can get access to the health information I disclose through a COVID-19 tracking app 2. what health information disclosed through a COVID-19 tracking app will be released 3. how the health information I disclose through a COVID-19 tracking app will be used
Habich-Sobiegalla S.; Kostka G.	Sharing is caring: willingness to share personal data through contact tracing apps in China, Germany, and the US	willingness to share data via CTAs	the willingness of individuals to share health information, relative location, real-time location and identity	disclosure risks	Perceived negative CTA consequences	Do you believe that the use of COVID-19 tracing apps would result in any of the following? 1 = fewer COVID-19 infections, 2 = isolating infected people, 3 = making it safer to go out, 4 = better health information, 5 = privacy violations, 6 = discrimination against people who

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
						test positive for COVID-19, 7 = government surveillance, 8 = use of data for commercial purposes, 9 = other, 10 = none.
Shih H.-P.; Liu W.	Beyond the trade-offs on Facebook: the underlying mechanisms of privacy choices	self-disclosure	—	privacy concerns	Privacy concerns refer to specific beliefs of personal control over private information based on technological capabilities (Dinev and Hart 2006).	1. Disclose private information on Facebook is a concern for me. (dropped) 2. Disclose private information on Facebook looks like a lose of control for me. 3. Disclose private information on Facebook looks like a threat to me.
Meier Y.; Krämer N.C.	The Privacy Calculus Revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels	self-disclosure intention	Participants' intention to disclose personal information	perceived privacy risks	—	Respondents' perception of privacy risks was assessed with six items (e.g., "I think that this website tracks my Internet activities") on a 7-point Likert scale from 1 = I do not agree at all to 7 = I totally agree.
Aboulnasr K.; Tran G.A.; Park T.	Personal information disclosure on social networking sites	information disclosure	Information disclosure refers to personal information a consumer shares with others on social networking sites, which may include any information "that refers to the self, including personal states, dispositions, events in the past and plans for the future" (R. Chen & Sharma, 2013).	perceived risk	—	Four items were adapted from Uilenberg (2015)tomeasure perceived risks of information disclosure.
Lutz C.; Hoffmann C.P.; Bucher E.; Fieseler C.	The role of privacy concerns in the sharing economy	sharing frequency	the sharing of material goods and services through online communities via contractual renting or leasing, as in the case of, for example, Airbnb.	online privacy concerns; physical privacy concerns	Physical privacy concerns associated with sharing can be suitably conceptualized based on Belk's(1988) notion of the extended self, as physical intrusions, damages and material losses all constitute infringements on the extended self.	The measures for online and physical privacy concerns were based on previous studies (Malhotra et al., 2004; Stutzman, Capra, & Thompson, 2011), but they were adapted to cover both institutional and social privacy threats in the context of a sharing service. | The measures for online and physical privacy concerns were based on previous studies (Malhotra et al., 2004; Stutzman, Capra, & Thompson, 2011), but they were adapted to cover both institutional and social privacy threats in the context of a sharing service.

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
Najjar M.S.; Dahabiyeh L.; Algharabat R.S.	Users' affect and satisfaction in a privacy calculus context	intention to allow access	—	perceived risks	The perceived risk of allowing access to personal information is based on an individual's belief that a high potential for loss would result from allowing this access (Malhotra et al., 2004).	1. In general, it would be risky to allow access to my personal information to this mobile app 2. There would be high potential for privacy loss associated with allowing access to my personal information to this mobile app 3. My personal information could be inappropriately used by this mobile app 4. Allowing this mobile app to access my personal information would involve many unexpected problems
Kim B.; Kim D.	Understanding the key antecedents of users' disclosing behaviors on social networking sites: The privacy paradox	user's disclosing behaviors	—	privacy concerns	SNSs because of the uncertainty regarding the privacy and security of personal information [2,5]. Privacy concerns include the unauthorized sharing of personal information, disclosure of customers' political behavior, and spamming through personalized advertisements [2,13,53].	Privacy concerns were assessed with scales developed by Malhotra et al. [55].
Chen J.V.; Biamukda S.; Tran S.T.T.	Service providers' intention to continue sharing: the moderating role of two-way review system	intention to continue	Service provider's intention to continue sharing their personal accommodation via a given channel	perceived physical privacy risks	The degree to which a service provider believes that a high potential for loss is associated with acceptance of people to their private space	1. When I share my accommodation via Airbnb, I am afraid that guests might damage or dirty my personal belongings (e.g. furniture) 2. When I share my accommodation via Airbnb, I am afraid that guests might snoop through my personal belongings (e.g. pictures) 3. When I share my accommodation via Airbnb, I am afraid that guests might enter areas that they should not access (e.g. bedroom) 4. When I share my accommodation via Airbnb, I am afraid that guests might use items that they should not use (e.g. bedclothes, pillows, personal hygiene products)
Princi E.; Krämer N.C.	Acceptance of smart electronic monitoring atwork as a result of a privacy calculus decision	acceptance of IoT-system	—	privacy concerns; perceived risks	—	Privacy concerns were assessed on a seven-point Likert-scale (from 1 = I do not agree at all to 7 = I totally agree) via 10 items (e.g., "I'm concerned that companies are

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
						collecting too much personal information about me") developed by Smith, Milberg and Burke [53] | perceived risks were assessed by the measurement from Bol et al. [10] on a seven-point Likert-scale (from 1 = I do not agree at all to 7 = I totally agree)
Harborth D.; Pape S.	Empirically investigating extraneous influences on the "apco" model—childhood brand nostalgia and the positivity bias	Use Behavior	—	concerns for information privacy	Privacy concerns are considered as the central construct of the study whereas the operationalization Concerns for Information Privacy (CFIP) [14] as a second-order construct [15] is used.	The sub-dimensions of CFIP (collection, error, improper access and unauthorized secondary use) were unalteredly taken from the original paper.
Abbas H.	Religion and spirituality as determinants of privacy and benefits to use mobile applications: An application of privacy calculus theory	intention to use mobile apps	The behavioral intention to use mobile apps is the degree of willingness to provide personal information	perceived privacy concerns	—	1. It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by mobile applications providers 2. It usually bothers me when mobile applications ask me for personal information 3. It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by mobile applications
Lankton N.K.; McKnight D.H.; Tripp J.F.	Understanding the Antecedents and Outcomes of Facebook Privacy Behaviors: An Integrated Model	1. privacy setting use 2. limiting disclosure 3. network size 4. use frequency	—	privacy risk	perceived privacy risks assess what could happen to general OSN users' personal information	1. MySNW.com entries and posts could be sold to third parties? 2. Personal information submitted could be misused? 3. Personal information could be made available to unknown individuals or companies without your knowledge? 4. Personal information could be made available to government agencies?
Brusch I.; Brusch M.	Influence of privacy and communication factors on online behavior	willingness to provide photos on the Internet	—	Internet privacy concerns; Perceived Internet privacy risk	—	—
Lünich M.; Marcinkowski F.; Kieslich K.	It's now or never! future discounting in the application of the online privacy calculus	usage behavior of the actual applications	—	perceived losses	—	four items addressed benefits and four addressed losses. An example of a risk item was "[Data context] is of disadvantage for

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
						me."
Meier Y.; Schäwel J.; Krämer N.C.	The shorter the better? Effects of privacy policy length on online privacy decision-making	self-disclosure behavior	—	privacy risk likelihood	—	The seven items were based on the content of the privacy policies and consisted of a first part ('How likely do you think it is...') and a varying second part (e.g., '...that the SNS passes on your personal data to third parties' or '... of being exposed to privacy risks by using the SNS').
Vimalkumar, M; Sharma, SK; Singh, JB; Dwivedi, YK	'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants	behavioral intention	—	perceived privacy concerns; perceived risk	privacy concern is the assessment of the loss. | Privacy risk can be defined as the degree of loss a consumer associates with the potential disclosure of personal information by the users in genera	1. I am concerned that the information I submit to (PDA) could be misused. 2. I am concerned that a person can find private information about me through PDA. 3. I am concerned about submitting information to PDA, because what others might do with it. 4. I am concerned about submitting information to PDA, because it could be used in a way I did not foresee | 1. PDA data may be sold to third parties? 2. Personal Data in PDA may be misused? 3. PDA data could be given to unidentified persons or companies without my consent 4. PDA Data could be made available to government agencies?
Ashuri, T; Dvir-Gvisman, S; Halperin, R	Watching Me Watching You: How Observational Learning Affects Self-disclosure on Social Network Sites?	self-disclosure behavior	Self-disclosure refers to the "process of making the self known to others" (Jourard & Lasakow, 1958, p. 91).	perception of losses	emotional distresses like jealousy in others' supposedly "good life" life (Muise, Christofides, & Desmarais, 2009), and envy in the rewards they receive online (e.g., rewards like getting support in the form of receiving "Likes"), and other losses associated with undesired usage of the information disclosed that the discloser cannot fully control (Altman, 1975).	1. Information I want to share with specific people will find its way to other people 2. People will share information about me without my consent, for example by tagging me in pictures 3. I will often be exposed to information I don't care about 4. Commercial companies will use information I share to my disadvantage, for example by bombarding me with irrelevant advertisements 5. Commercial companies will sell my information to third parties without my knowledge or consent 6. The state will know more about

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
						me than I want it to 7. Hackers will steal my information
Dongyeon Kim, Kyuhong Park, Yongjin Park, Jae-Hyeon Ahn,	Willingness to provide personal information: Perspective of privacy calculus in IoT services	willingness to provide personal information	willingness or intent to provide personal information to e-commerce vendors, social networking services, online video services, and location-based services	perceived privacy risk	perceived privacy risk is the degree to which people believe there is a potential for loss associated with the release of personal information	What do you believe is the risk due to the possibility that personal information tracked by this IoT service. 1. ... could be sold to third parties? 2. ... could be misused? 3. ... could be made available to unknown individuals or companies without your knowledge? 4. ... could be made available to governmental agencies? 5. ... could be jeopardized by hacking activities?
Anrong Fan, Qiao Wu, Xiaofei Yan, Xiaotong Lu, Yue Ma, Xue Xiao,	Research on Influencing Factors of Personal Information Disclosure Intention of Social Media in China	personal information disclosure intention	Posey, Lowry, Roberts and Ellis (2010) stated that the self-disclosure behavior of online community users refers to the behavior of users leaking personal information when registering or using mobile social networks.	Perceived risk	Perceived risk refers to the loss that may be caused by the users' personal information disclosure behavior due to social media's illegal or improper use of information, and it is the user's prediction of the worst outcome	1. Disclosure of personal information to social media may lead to disclosure of personal information. 2. In general, there are risks in disclosing personal information to social media.
John T. Gironda, Pradeep K. Korgaonkar,	iSpy? Tailored versus Invasive Ads and Consumers' Perceptions of Personalized Advertising	personalized advertising intention	Defined personalized advertising, but did not clearly define what is perception of personalized advertising	Privacy concerns	Concerns about a possible loss of privacy as a result of voluntary or surreptitious information disclosure	1. I am concerned that personalized advertisers are collecting too much information about me. 2. I am concerned that the information collected about me for PA could be misused. 3. I am concerned about collection of my information by personalized advertisers, because of what others might do with it. 4. All things considered, I believe that my privacy is seriously threatened by personalized advertising.
Athina Ioannou, Iis Tussyadiah, Yang Lu,	Privacy concerns and disclosure of biometric and behavioral data for travel	Willingness to Share Behavioral Information. Willingness to Share Biometric Information	businesses focusing on offering unique personalized travel experiences are highly dependent on the collection of consumers' personal information.	privacy concerns	A central construct that has been widely used is privacy concerns, which represent individuals' perceptions of what will happen to the information they provide to different providers (Dinev & Hart, 2006).	Travelers' online privacy concerns
Alkhalifah A.; Bukar U.A.	Examining the Prediction of COVID-19 Contact-Tracing App Adoption Using an Integrated Model	Tawakkalna behavior intention (BI) use	This study defines BI as the extent to which an individual will adopt or continue to use	privacy risk; social risk	Internet-related perceived privacy risk refers to the extent to which internet users are concerned about	It bothers me when health authorities track my location through my Tawakkalna mobile

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
	and Hybrid Approach Analysis		Tawakkalna in the future (71).		how and to what extent an online entity collects and uses their personal information | Although perceived risk has been conceptualized as a multidimensional term encompassing financial, performance, physical, physiological, and social risk (13, 60). This study focuses on social risk as a particularly prominent component in the contact-tracing application.	contact-tracing app. I am concerned that health authorities are collecting too much location information about me through my Tawakkalna mobile contact-tracing app. It bothers me if health authorities collect my mobile location and I cannot alter the location settings. It bothers me when I do not have control over how my mobile location is used by health authorities. 13 98 | I am concerned that my movement may be restricted if I do not use Tawakkalna. I am concerned that I may not be allowed to visit places without Tawakkalna installed on my phone. I am concerned that my family and friends will not allow me to visit them if I am not using Tawakkalna. I am concerned that if Tawakkalna indicates that I am a suspected case, I will be forced to self-isolate. 13
Huang & Huang	Privacy Calculus Theory in the Digital Government Context: The Case of Taiwan's New eID Policy	the willingness to authorize personal information via new eID	—	privacy risk	Privacy risk could be elucidated as the cost of potential privacy violation (Keith et al., 2013), such as financial damage and mental anxiety due to intensive fraud or harassment.	1. RISK1 using new eID to authorize the government agencies with my personal data would involve many unexpected problems 2. RISK2 there would be high potential for loss in authorizing my personal information to the government agencies via new eID 3. RISK3 overall, it would be risky to authorize my personal information to the government agencies via new eID
Nguyen	Continuance Intention in Traffic-Related Social Media: A Privacy Calculus Perspective	continuance intention to provide traffic information	—	privacy concerns	—	1. I am concerned with my personal information that I submit on the Waze could be misuse. 2. I am concerned about put my personal information on Waze because of what other people might do with it. 3. I am concerned with submitting my information on Waze as it might be used in a way I did not predict. 4. I am quiet sensitive with how

Authors	Titles	Labels of DV	Disclosure Definition	Cost Variables	CV Conceptual Definition	CV Operational Definition
						Waze handle my personal information. 5. I am concerned about threats to my privacy in Waze.

*0 means studies did not provide relevant information

Table 2. Studies with Insignificant Relationships Between Id and Benefit Variables

Authors	Titles	Labels of DV	Disclosure Definition	Benefit Variables	BV Conceptual Definition	BV Operational Definition
Carlsson Hauff J.; Nilsson J.	Individual costs and societal benefits: the privacy calculus of contact-tracing apps	Willingness to use Contacttracing apps	—	perceived utilitarian usefulness	they may be general and utilitarian, such as promoting economic and informational solutions for the user and implying increased productivity	1. Using my smartphone would allow me to get information about stores and products 2. Using my smartphone would allow me to access product price comparisons 3. Using my smartphone would allow me to get useful information to make better shopping decisions 4. Using my smartphone would allow me to do my shopping at a lower financial cost 5. Using my smartphone would allow me to save money 6. Using my smartphone would allow me to take advantage of promotional offers
Lutz C.; Hoffmann C.P.; Bucher E.; Fieseler C.	The role of privacy concerns in the sharing economy	sharing frequency	the sharing of material goods and services through online communities via contractual renting or leasing, as in the case of, for example, Airbnb.	social-hedonic benefits	—	both social-hedonic and monetary benefits (Bucher et al., 2016) were also taken from previous studies.
Najjar M.S.; Dahabiyeh L.; Algharabat R.S.	Users' affect and satisfaction in a privacy calculus context	intention to allow access	—	perceived benefits	—	1. I think this mobile app is useful in my daily life 2. I think using this mobile app makes my life easier 3. I think using this mobile app enables me to accomplish tasks more quickly 4. Overall, I find using this mobile app useful
Kim B.; Kim D.	Understanding the key antecedents of users' disclosing behaviors on social networking sites: The privacy paradox	user's disclosing behaviors	—	trust	Trust refers to users' willingness to be vulnerable to some actions based on the expectation that others will exhibit ethical behaviors	—
Princi E.; Krämer N.C.	Acceptance of smart electronic monitoring atwork as a result of a privacy calculus decision	acceptance of IoT-system	—	rescue value	—	The scale from a long-term study by Trepte and Masur [47] contained 11 items such as "The protection of privacy should be enshrined in the constitution" on a seven-point Likert-scale (from 1 = I do not agree at all to 7 = I totally agree).
Hassandoust F.; Akhlaghpour S.; Johnston A.C.	Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational	intention to install contact tracing app	—	trusting beliefs	rusting beliefs refer to the degree to which individuals believe that the PHA releasing and controlling a CTMA is reliable in guarding their personal information collected	—

Authors	Titles	Labels of DV	Disclosure Definition	Benefit Variables	BV Conceptual Definition	BV Operational Definition
	privacy calculus perspective				through a CTMA.	
Brusch I.; Brusch M.	Influence of privacy and communication factors on online behavior	willingness to provide photos on the Internet	—	personal Internet interest	—	—
Zareef A. Mohammed, Gurvirender P. Tejay,	Examining the privacy paradox through individuals' neural disposition in e-commerce: An exploratory neuroimaging study	PII Disclosure (personally identifiable information)	—	Personal Interest	—	Condition 4 reflected personal interest, which allowed subjects to choose a product they can obtain online of their choice that they were personally interested in. A few survey items on a seven-point Likert Scale was asked for manipulation check purpose, but the items were not disclosed by the authors.
Dongyeon Kim, Kyuhong Park, Yongjin Park, Jae-Hyeon Ahn,	Willingness to provide personal information: Perspective of privacy calculus in IoT services	willingness to provide personal information	willingness or intent to provide personal information to e-commerce vendors, social networking services, online video services, and location-based services	perceived privacy risk	perceived privacy risk is the degree to which people believe there is a potential for loss associated with the release of personal information	What do you believe is the risk due to the possibility that personal information tracked by this IoT service.
Teagen Nabity-Grover, Christy M.K. Cheung, Jason Bennett Thatcher,	How COVID-19 stole Christmas: How the pandemic shifted the calculus around social media Self-Disclosures	Online Self-Disclosure (three dimensions)	the communication of personal information to others online (Nabity-Grover et al., 2020, Nabity-Grover, 2020) – during the COVID-19 pandemic	self-presentation	Self-presentation is the behavior of individuals to intentionally regulate their image as perceived by others (Wang et al., 2016).	1. Using [Facebook/Instagram], I can accurately express my identity. 2. Using [Facebook/Instagram], I can portray the image I want. 3. Using [Facebook/Instagram], I am able to present myself in the way that I want. 4. Using [Facebook/Instagram], I can adequately convey information about who I am. 5. Using [Facebook/Instagram], I am able to project my desired identity. 6. Using [Facebook/Instagram], others will view me in the way that I want.
Deodat Mwesiumo, Nigel Halpern, Svein Bråthen, Thomas Budd, Pere Suau-Sanchez,	Perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports	Willingness to provide personal data	this study defines personal data as "any piece of information related to an identified or identifiable person, including name, identification number, location data and an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person". Therefore, the willingness to provide personal data is defined in this paper as	Benefits of disclosure	—	BD1. Providing personal data would help airports to serve me better BD2. Providing personal data would improve my experience with digital services at airports BD3. Overall, I feel that providing personal data would be beneficial for passengers

Authors	Titles	Labels of DV	Disclosure Definition	Benefit Variables	BV Conceptual Definition	BV Operational Definition
			the readiness of an individual to offer any piece of information specified in Article 4 of the GDPR.			
Karl van der Schyff, Stephen Flowerday,	The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO	Intention to self-disclose	—	trust in provider	—	1. Is open and receptive to the needs of its members. 2. Makes good-faith efforts to address most member concerns. 3. Is interested in the wellbeing of its members, not just its own. 4. Is honest in its dealings with me. 5. Keeps its commitments to its members. 6. Is trustworthy.
Taewoo Nam,	What determines the acceptance of government surveillance? Examining the influence of information privacy correlates	surveillance acceptability	—	privacy control	"A perceptual construct reflecting an individual's beliefs in his or her ability to manage the release and dissemination of personal information" (Xu et al., 2011: 804)	"As you go through a typical day, how much control do you feel you have over how much information is collected about you and how it is being used?"
Bo Hu, Yu-li Liu, Wenjia Yan,	Should I scan my face? The influence of perceived value and trust on Chinese users' intention to use facial recognition payment	Intention to use	—	novelty	Novelty refers to the extent of the newness and uniqueness of a product or a service that makes it different from others (Im et al., 2015).	—
Alkhalifah A.; Bukar U.A.	Examining the Prediction of COVID-19 Contact-Tracing App Adoption Using an Integrated Model and Hybrid Approach Analysis	Tawakkalna behavior intention (BI) use	This study defines BI as the extent to which an individual will adopt or continue to use Tawakkalna in the future (71).	social interaction	0 by revealing location-based information or health status to authorities, individuals may benefit from physical movement (4, 16), which may increase the number of users inclined to use the contact-tracing app. On the other hand, location-based information is viewed as highly sensitive (16) by users who perceive this information as intrusive, who do not want their social activities to be threatened by authorities due to COVID-19 risk exposure, or who are fearful of being forced to self-isolate.	By using Tawakkalna, I will be allowed to move freely, without any restrictions. By using Tawakkalna, I will visit places, anywhere and at any time. By using Tawakkalna, I will visit places, anywhere and at any time.
Smink et al.	Try online before you buy: How does shopping with augmented reality affect brand responses and personal data disclosure	willingness to share personal data	—	perceived enjoyment	—	Trying the colors of lipstick on the website was... 1. enjoyable* 0.95 2. fun* 0.97 3. pleasant* 0.97 4. interesting*
Venkatesh et al.	"Being at the cutting edge of	purchase intention	—	trust; information	Trust in the seller is considered one of the	1. This retailer is trustworthy. 2. I trust this retailer keeps my

Authors	Titles	Labels of DV	Disclosure Definition	Benefit Variables	BV Conceptual Definition	BV Operational Definition
	online shopping: Role of recommendations and discounts on privacy perceptions"			richness	enablersthat can offset customers' concerns about shopping online and is the belief that the seller does not behave opportunistically | Information richness is defined as the capability of the information on shopping sites to facilitate understanding of products and services	best interests in mind. 3. This retailer's behavior meets my expectations. | 1. My interaction with the online site was close to an actual face-to-face interaction. 2. My interaction with the online site felt like a face-to-face interaction. 3. Shopping at the online site felt like an in-person interaction.

METHOD

The method that is used in the paper. If the paper used more than one method, please search for the one that is used for the privacy calculus model. If a survey is used in the study, please code 1; if an experiment is used in the study, please code 2; please other methods are used in the study, please code 3 and provide the name of the method right after 3. If the author used a mixed method, please look into which method the author used to test the privacy calculus theory. If both methods are used to test the theory, please code 4 and leave a note of the two methods' names in the Note column.

Sample Size

The number of individual samples measured or observations used in the study.

Platform

The platform or device where the authors study use the privacy calculus theory. Please use the original description of the platform from the paper.

Journal Name

The journal where the paper is published.

Country

The country where the study is conducted.

Dependent Variable

(*Note: In PCM, the information disclosure is not limited to revealing one's information. Behaviors, such as using an app, becoming a subscriber, adopting a technology etc, that involves users giving up their information fall into the category of information disclosure. Please refer to the original text and see how authors define or conceptualize the behavior.*)

Labels of DV

Labels author(s) used to describe the dependent variables. For example, in some articles, researchers use *privacy disclosure or apps adoption* to describe the DV.

Information Disclosure Conceptual Definition

An abstract description of the meaning of information disclosure the author(s) provide to clarify the boundaries of what it does and does not entail. If the author does not provide conceptual definition, please code this variable as 0.

Information Disclosure Operational Definition

Scale items the author(s) provide to specify how they will measure or observe information disclosure in the study. If the author(s) did not provide scale items, please see if they provide an item example or the citation from which they borrow or adapt scale items. If the author does not provide any of the above, please code this variable as 0.

Costs Variables

(*Note: In PCM, the cost refers to the consequences or loss an individual perceives they will face after disclosing information (Dinev et al., 2006). Cost variables are factors that directly influence information disclosure behaviors or intentions. Negative variables that are not directly related to information disclosure are not considered as benefits variables. Please refer to the hypothesis section in the original paper and see if this variable is introduced in the PCM section.*)

Cost Variable Conceptual Definition

An abstract description of the meaning of the cost variable the author(s) provide to clarify the boundaries of what the variable does and does not entail. If the author does not provide conceptual definition, please code this variable as 0.

Cost Variable Operational Definition

Scale items the author(s) provide to specify how the cost variable will be measured or observed in the study. If the author does not provide operational definition, please code this variable as 0. If the author(s) did not provide scale items, please see if they provide an item example or the citation from which they borrow or adapt scale items. If the author does not provide any of the above, please code this variable as 0.

CV Sig or Not

The statistical result of the cost variable author(s) report in the Result section. If authors report the cost variable is significantly related to the information disclosure, please code as 1; if not, please code as 0. If the author tested the theory on different platforms, samples, countries, contexts, etc, and got mixed results of different situations, please code as 2 and leave a note of the mixed results in the Note column.

Benefits Variables

(*Note: In PCM, benefits refers to tangible/intangible rewards an individual expects or perceives they will get from information disclosure (Kokolakis, 2017). Benefit variables are factors that directly influence information disclosure behaviors or intentions. Positive variables that are not directly related to information disclosure are not considered as benefits variables. Please refer to the hypothesis section in the original paper and see if this variable is introduced in the PCM section.)*

Benefit Variable Conceptual Definition

An abstract description of the meaning of the benefit variable the author(s) provide to clarify the boundaries of what the variable does and does not entail. If the author does not provide conceptual definition, please code this variable as 0.

Benefit Variable Operational Definition

Scale items the author(s) provides to specify how the cost variable will be measured or observed in the study. If the author does not provide operational definition, please code this variable as 0. If the author(s) did not provide scale items, please see if they provide an item example or the citation from which they borrow or adapt scale items. If the author does not provide any of the above, please code this variable as 0.

BV Sig or Not

The statistical result of the benefit variable author(s) report in the Result section. If authors report the benefit variable is significantly related to the information disclosure, please code as 1; if not, please code as 0. If the author tested the theory on different platforms, samples, countries, contexts, etc, and got mixed results of different situations, please code as 2 and leave a note of the mixed results in the Note column.

Moderators

Variables that significantly affect the strength of the relationship between cost, or benefit, variables and information disclosure behaviors.