Information Systems and e-Business Management (2023) 21:353–387
https://doi.org/10.1007/s10257-023-00622-6

ORIGINAL ARTICLE

Beyond the trade-offs on Facebook: the underlying mechanisms of privacy choices

Hung-Pin Shih[1] · **Wuqiang Liu**[1]

Received: 7 September 2022 / Revised: 28 November 2022 / Accepted: 5 January 2023 /
Published online: 25 January 2023

Abstract

The theory of privacy calculus in terms of the trade-offs between benefits and risks is believed to explain people's willingness to disclose private information online. However, the phenomenon of *privacy paradox*, referring to the preference-behavior inconsistency, misfits the risk–benefit analysis. The phenomenon of privacy paradox matters because it reflects an illusion of personal control over privacy choices. The anomaly of privacy paradox is perhaps attributed to cognitive heuristics and biases in making privacy decisions. We consider the stability-instability of privacy choices is better used to explain the underlying mechanisms of paradoxical relationship. A rebalanced trade-off, referring to the embeddedness of "bridging" and "bonding" social support in privacy calculus, is derived to develop the risk–benefit paradigms to explain the underlying mechanisms. In this study we address the underlying mechanisms of privacy choices in terms of self-disclosure and user resistance. To test the hypotheses (or mechanisms) of the research model, we developed the instrument by modifying previous scales. A general sample of 311 experienced Facebook users was collected via online questionnaire survey. From the empirical results, perceived benefits based on information support rather than emotion support can motivate self-disclosure willingness. In contrast, privacy risks rather than privacy concerns inhibit the willingness to disclose private information. The risk–benefit paradigms instead of the imbalanced trade-offs help to explain the instability of privacy choices where privacy calculus sticks with the stability view. Implications for the theory and practice of privacy choices are discussed accordingly.

Keywords Facebook · Privacy paradox · Privacy calculus · Social support · Embeddedness · Self-disclosure

✉ Hung-Pin Shih
2387540980@qq.com

Wuqiang Liu
13022289@qq.com

[1] Minnan Science and Technology University, Quanzhou 362332, Fujian, China

1 Introduction

Personal privacy is a general right, just as the right to property, which needs legal protection for individuals and also received concerns in the United States and most countries (Warren and Brandeis 1890). Privacy refers to "*the claim of individuals to determine for themselves when, how and to what extent information about them is communicated*," (Westin 1967). The concept of privacy for individuals was considered as a "regulatory process" to control external access to oneself and information sharing with others (Klopfer and Rubenstein 1977). Moreover, information (or personal) privacy is a concept of moral and legal right from the perspectives of regulations, policies, and commercial practices in modern countries (Clarke 1999). In the digital age, personal privacy becomes a commodity on commercial websites that make the collection, storage, transfer, processing, and re-use of private information are easy to technology suppliers and also attractive to personalized practices (Davies 1997). Hence, information privacy is more related to the ability of personal control over the information (e.g., access, storage, use, etc.) about themselves (Bélanger et al. 2002). In the name of *procedural fairness*, firms tempt consumers to disclose personal information on the exchange of free services or online transactions (Culnan and Armstrong 1999). Commercial and defaulted agreements can be regulated to meet privacy policies and look as sufficient protection for people. But information asymmetry occurs when consumers surrender personal information to get the required services from governments or make transactions from firms (Tsai et al. 2011). Collect customer purchases and profiles for better business opportunities using the Internet and mobile technologies have become the prevailing competitive strategies to effectively, i.e., the reduction of time and space barriers to recording, track people's behavioral patterns (Rust et al. 2002). Obviously, consumers rather than firms often take compromise on their privacy for the convenience of mobile applications (Hoffman et al. 1999) or online transactions (Hui et al. 2006). The phenomenon has occurred, namely *privacy paradox,* referring to the anomaly that consumers behave in a way to contradict their preferences (Sweat 2000), or the preference-behavior inconsistency in making privacy choices (Dinev and Hart 2006). The appealing to "fair exchange" of personalized services provides the reasonable explanation about why consumers express their privacy concerns, but behave in an opposite way to disclose personal information (Pavlou 2011). The phenomenon of privacy paradox matters because it reflects an illusion of personal control over the misuse of private information where online consumers or platform users just pay attention to short-term risks rather than long-term ones (Brandimarte et al. 2013). However, Barth et al. (2019) raised one question: "How much do consumers really value their data and privacy?" (p. 64).

Firms are hard to resist to the temptation of privacy invasion in which the threats to privacy penetrate through the boundary of personal privacy in collecting and re-using the profiles of consumers and the behaviors of online transactions. From online transactions to social media, people are overwhelmingly surrendering their privacy (e.g., email, mobile phone numbers) in the desire for

transaction convenience or social connection. The disclosure of personal information online is simplistic without rethinking the asymmetric return to an exchange. Social networking becomes the weapon for the technology giants that do not bear on the costs or threats to the losses of personal privacy. Social networking sites (SNSs) are human-created information artefacts that developed for human connections and the spread of influences, which probably promote the invasion of personal privacy in business contexts (Lowry et al. 2017). The wide use of SNSs, such as Facebook (or Chinese Weibo), can provide the observation lens to understand how users define their privacy boundaries and make privacy choices.

Interpersonal communication, from offline to online connections, after the Millennium was not fully predicted by Putnam (2000). Yet, Facebook's "friending" and "tagging" are expected to play as the role of social networking to rebuild people's social capital or mutual trust. Facebook users believe that they can save the time of communication and overpass the constraint of space that were considered as obvious barriers to the connections of civilization before the Internet. In 2021, the monthly active users on Facebook have reached 2.85 billion (www.facebook.com). Along with the growing trend of Facebook users associate with booming profits, the spreading of personal information may squeeze the borders of personal privacy and cause the obstacles to secured protection. Invisible invasion of personal privacy on Facebook has affected people's lives, such as privacy risks (Debatin et al. 2009). Privacy risk is a risk perception of the misuse of personal information on opportunistic behaviors (Dinev and Hart 2006). It is easy to claim that people have the control over privacy risks because the use of Facebook is a personal choice. But, the presence of privacy paradox reveals that the ability to cope with privacy risks is irrelevant (Krasnova et al. 2010). Despite the concern of personal privacy, the disclosure of personal information is irreversible after surrendering future use of personal data or having lost control over it.

People are not naive that profit-seeking high-tech giants, such as Facebook and other SNSs, have the incentives to foster unspoken misuse of user profiles and the promotion of personalized services. Previous studies often took Facebook as an example to examine the motives for personal disclosure behaviors (Chang and Heo 2014; Dienlin and Metzger 2016; Tsay-Vogel et al. 2018; Zlatolas et al. 2015). It holds obviously that Facebook users are willing to disclose personal profiles despite the threats to personal privacy. The disclosure of private information often lies in one's control over current behavior that has possible impacts on future consequences, which is often judged on the *calculus of behavior* regarding privacy rights and personal needs of socialization experience (Laufer and Wolfe 1977). Yet, the unpredictable future consequences of current behavior motivate people to overall judge privacy choices in terms of anticipated benefits and anticipated risks. Rational people are supposed to judge the disclosure of private information on a balanced trade-off between benefit beliefs and privacy risk beliefs, i.e., the theory of *privacy calculus* (Culnan and Armstrong 1999). Considering how privacy protection is hindered by the freedom of privacy choices (Clarke 1999), or the behavior of self-interested human species (Acquisti et al. 2022), the phenomenon of privacy paradox needs more evidences, such as one's cognitive biases of risk assessment (Barth and de Jong 2017). We consider the preference-behavior inconsistency of privacy

choices as the taken-for-granted phenomenon to rethink the theory of privacy calculus. The phenomenon of privacy paradox is better understood that people often overestimate their rational calculus of privacy benefits and risks, and underestimate their behavioral change (e.g., user resistance) in the ignorance of cognitive biases (Adjerid et al. 2018).

We acknowledge that people are willing to disclose personal information if interpersonal trust can help them reduce opportunistic behaviors (Krasnova et al. 2010), or because they want to sustain intimate relationships or have more intimate disclosures (Jiang et al. 2013a, b), or seek to bridge online and offline social connections (Ellison et al. 2007). Yet, social trust or social capital can enable an individual to get the support of resources from other in-group members of a networked community or group (Ellison et al. 2007). We develop an inference about the rebalance of trade-offs by embedding social support in privacy calculus to reduce the uncertainty of privacy choices, i.e., more stable social interactions and intimate relationships. Embeddedness refers to the functioning of a real world that could be understood associated with various modes of social actions on different conditions or the economic life of social beings governed by social customs and norms, which act as parts of historically derived, institutional, or social structures (Polanyi 1957). In the context of networked firms, embeddedness refers to the cultivation of long-term and cooperative relationships (Uzzi 1997). In the context of human-technology interactions, embeddedness refers to usages of information systems in work routines to sustain stable socialization process (Polites and Karahanna 2013). To extend the knowledge about personal choices of privacy uncertainty (Acquisti et al. 2015), we address the risk–benefit paradigms of self-disclosure and user resistance. The risk–benefit paradigms are developed to examine the underlying mechanisms of privacy choices, but not to eliminate the phenomenon of privacy paradox.

We take Facebook users as the target and thereby examine the fostering and inhibiting forces of privacy choices. The approach to uncover the black-box of privacy paradox is beyond the research scope. The uncertainty of privacy choices would always exist, and people try to make against it using their own ways stemming from specific beliefs that need better explanations than the existing ones from privacy calculus. In this study we address the following research questions concerning privacy choices involved in embedding digital technologies into people's life:

Question-1: What's the alternative explanation of privacy paradox and why it works?
Question-2: How to conduct a rebalanced trade-off of privacy choices on Facebook?

2 Competing views of information privacy

2.1 Social interactions on Facebook

The evolution of online connections, stemming from SNSs to multi-sided platforms for social app development, fosters Facebook to become a technology giant that

increases its influence on social media, political dispute, and advertising by collecting personal data and breaking privacy boundary (Helmond et al. 2019). Among digitalized platforms in the world, Facebook, as founded in 2004, is one of the most successful company in terms of user populations, geographical coverages, social influences, media advertisements, and business profits (Hutchinson 2020). The success of Microsoft company would remind general impressions of the importance of network effects and the war on standards for operating systems (Bresnahan 2001). New rules of digitalized platforms and strong congestion between sellers have tempted the desire for privacy protection and the business opportunities underlying social-culture dissociation (Tucker 2018). Facebook has adapted the competitive strategy via mergers and acquisitions for the past decade, from Instagram to WhatsApp, and from social connections to online advertisements and transactions (Sraders 2020). Facebook persuades people to believe that the anticipated benefits would compensate their potential losses of personal disclosure in the digital platform. The lock-in strategy of Microsoft has adapted switching costs and network effects to win the war for software competition. However, the competition in the digital economy has changed from the war on standards for compatibility (e.g., Microsoft) to the embeddedness of social capital or social support for shared interests and social connections (e.g., Facebook). Social capital or social support helps individuals connect with others and behave sticky to a community or a group (Putnam 2000). Many Facebook users knew each other offline (Ellison et al. 2007), the networking trend from offline to online would reinforce their social connections. Facebook users that engaged in social information-seeking behaviors via online and offline connection strategies are more likely to develop social support (Ellison et al. 2010).

Online social interaction is the key driving force for Facebook users from the past to the present (Acquisti et al. 2015). The use of Facebook "friending" and "tagging" to intensify the current relationship can provide explanations about why users are willing to disclose their profiles and ignore privacy concerns in the disclosure. The major sources of privacy-related threats to Facebook users mostly come from institutions and peers in which the latter is related to social privacy that probably received more concerns (Raynes-Goldie 2010). The research indicates that Facebook users are more concerned about the disclosure of private information on the peer context (Rogers 1975). But the growing trend of Facebook users (e.g., over 1 billion after 2012) seems to manifest their need for social interactions, which contradicts general impressions of privacy concerns. People's desire for social interactions and privacy protection are unlikely to be simultaneously achieved in the digital age. Owing to the spreading from offline to online social connections, we consider that Facebook users' concerns about the misuse of private information would be totally a different story that desires for a new approach to examine privacy choices (Acquisti et al. 2015, 2022).

2.2 Instability of privacy choices

Privacy choices are more related to the control over personal information, but not the restriction on social interactions (Klopfer and Rubenstein 1977). The phenomenon

of privacy paradox reveals the presence of cognitive dissonance in privacy choices, or the conflict between privacy preferences and actual disclosure. Privacy preferences concerning framing, biases, and heuristics that are not stable in different contexts in which people's lives indicate changing boundaries between private and public spheres regarding the concealment or disclosure of personal information over time or across cultures (Acquisti 2009, 2022; Brandimarte and Acquisti 2012; John et al. 2011). Personal control over private information often depends on platform self-regulation and government legislation on privacy protection (Brandimarte and Acquisti 2012), those changes in privacy boundaries would make privacy choices unpredictable or unreliable, i.e., the instability of privacy choices or the instability of behavioral outcomes. The divulgence of personal data has shaped privacy as people's concerns about online social interactions that associate with economic, legal, technical, social, and ethical issues surrounded by market opportunities and privacy intrusion (Sraders 2020).

From the selected previous work about the explanations of privacy paradox, the risk–benefit analysis of privacy calculus is rarely stable, depending on people's rational boundaries, psychological processes, or cognitive heuristics and biases (Table 1). For example, incorporating behavioral influences into rational privacy calculus of risks and benefits, the instability of privacy choices is shaped by both objective and relative perceptions, leading to the phenomenon of privacy paradox (Adjerid et al. 2018). Alternatively, the phenomenon of privacy paradox probably comes from people's self-interested choices of private information and diverse boundaries of privacy (Acquisti et al. 2022). From the previous work, the dispute of privacy choices is inconclusive and even more complicate for people to get involved in SNSs for social interactions.

Our framework of privacy choices is consistent with Westin's view that people want to restore the balance between privacy and necessary surveillance (Laughlin 1968). However, two types of uncertainty would hinder privacy choices, leading to the instability of privacy choices. First, the uncertainty of information misuses to shape privacy risks. Second, the uncertainty of information disclosure to shape anticipated benefits, such as discounting late rewards would cause overweight on the existing benefits. The instability of privacy choices, referring to the instability of underlying mechanisms, may come from possible changes of risk beliefs and/or benefit beliefs along with changing borders of privacy or different frames of reference from the existing states to the future states. Also, the trade-offs between long-term privacy risks and short-term benefits may cause the instability of privacy choices (Acquisti and Grossklags 2005).

According to privacy calculus, risk beliefs and benefit beliefs are supposed to independently affect self-disclosure intention. Building on privacy calculus, we develop the risk–benefit paradigms by taking a *relative weighing* on the comparison between perceived benefits and perceived risks of private information disclosure. A relative weighing approach to privacy choices was less examined in the literature (Adjerid et al. 2018). Using the relative weighing approach instead of the risk–benefit analysis in the literature (Keith et al. 2013; Xu et al. 2009), we assume that experienced people (e.g., existing Facebook users) perceived the risks of information disclosure prior to judging the anticipated benefits of that disclosure. Moreover,

Table 1 Selected literature about the explanations of privacy paradox

Theory	Assumption	Trade-off/context	Privacy choice	References
Procedural justice fairness	1. Fairness is a basic need for humans in justice 2. Privacy regulations or protections for fair information practices that rely on freedom of information	Procedural fairness, as regulated in policies, increasing the perceptions of fairness that weaken the tensions between the collection (giving benefits) and use (creating risks) of personal information Context: Internet commerce	Customer trust in procedural fairness would reduce privacy concern associated with disclosure	Clarke (1999), Culnan and Armstrong (1999)
Hyperbolic discounting/Psychological distortions	Hyperbolic discount functions are developed in terms of a high discount rate over short horizons and a low discount rate over long horizons. (A conflict between present and future preferences)	An inconsistency between privacy attitudes and privacy behavior Context: Interview surveys and experiments	People tend to under-discount long-term risks and losses while acting in privacy-sensitive situations	Acquisti and Grossklags (2004)
Social contract	1. The perceptions of fairness regarding the collection and use of personal information are not stable 2. The shifting dimensions of privacy concerns from offline to online are assumed to lie in fairness perceptions 3. Privacy concerns exhibited three psychometric properties, namely collection, control, and awareness, in online contexts	The trust-risk framework as shaped by privacy concerns is better to deal with the disclosure intention in an uncertain environment Context: Field surveys of Internet users from household	Less sensitive information would increase trusting beliefs and reduce risk beliefs of privacy disclosure	Malhotra et al. (2004)

Table 1 (continued)

Theory	Assumption	Trade-off/context	Privacy choice	References
Incomplete information and bounded rationality	1. People have limited ability to calculate privacy risks and disclosure benefits 2. People do not have all the information required for judging privacy risks	An imbalanced trade-off between risks and benefits of privacy	People show the dichotomy between claimed privacy concerns and their intention to disclose	Acquisti and Grossklags (2005)
Privacy calculus	1. Consumers are rational to balance anticipated risks and anticipated benefits in surrendering personal information 2. Risk perceptions are related to the uncertainty of opportunistic behavior, i.e., risk perceptions are not stable in the decision prior to privacy disclosure 3. From Internet experiences to online transactions, trust and personal interest may outweigh privacy risk perceptions	A cost–benefit analysis of privacy calculus in terms of risk beliefs and confidence and enticement beliefs are conducted to predict the disclosure behavior of personal information Context: e-commerce transactions	Internet trust and personal interest raise the willingness to disclose personal information Privacy concerns reduce disclosure intention	Dinev and Hart (2006)

Table 1 (continued)

Theory	Assumption	Trade-off/context	Privacy choice	References
Utility maximization	1. A trade-off based on consumers' utility function of benefits and costs 2. Benefit is derived through the degree of personalization 3. Cost is a function of consumer privacy concerns, previous privacy invasion, consumer-rated importance of information transparency and privacy policies	Consumers that perceive the value (or outcome utility) of online service exceeds online advertising are more willing to disclose private information Consumes perceive different values of online service and advertising associated with varying perceived benefits Context: Online personalization by a large Internet service provider	The potential benefit of the service outweighs the potential risk of privacy invasion in online personalized service The risk of an intrusion outweighs the benefit of advertising in online personalized advertising	Awad and Krishnan (2006)
Heuristic processing and routinization of behavior	1. The temporal stability of intention for planned and voluntary behavior 2. Actual disclosure behavior was less planned	A trade-off between risks and trust instead of the cost–benefit analysis Context: Marketing exchange environments	Risk perceptions hinder individuals' stated intention to disclose personal information, while trust promotes actual disclosure	Norberg et al. (2007)
Quantum theory	1. Indeterminacy: decision outcome is determined at the decision time rather than the decision-making process 2. Noncommutativity: two decisions (stated preferences and actual disclosure) are not interchangeable or compatible in privacy decision making	Stated preferences and actual disclosure behavior are necessary but mutually exclusive observations People modify their preferences in response to discomfort stemming from conflicting preferences Context: Meta-analysis	People's willingness to disclose personal data are observed to against their own privacy concerns claimed	Flender and Müller (2012)

Table 1 (continued)

Theory	Assumption	Trade-off/context	Privacy choice	References
Privacy calculus Social exchange Media richness	1. Mediated communication for intimate and social desirable relationship 2. The disclosure of private information in synchronous online social interactions	A shift from privacy calculus to social exchange Context: College students in online chat rooms	Privacy concerns reduce self-disclosure Social rewards increase self-disclosure	Jiang et al. (2013a, b)
Information boundary	The control over private and valued information in the collection and storage processes	A risk-control trade-off instead of a risk–benefit trade-off to judge psychological comfort with personalized application and the intention toward the collection of personal data Context: A field experiment of smartphone users	A tension between personalization and privacy can be reduced by technological solutions	Sutanto et al. (2013)
Privacy calculus Social exchange	1. The trade-offs between privacy and benefits of information disclosure along with the outcomes of trade-offs constitute the calculus of behavior 2. The cost-effectiveness analysis of privacy makes individuals seeking for health communication in online platforms despite the presence of privacy concerns	A trade-off between privacy concerns and positive outcomes of disclosure Context: The sample of students, faculty, staffs from southern region, as well as patients of clinics from the local hospital university in USA	High affective commitment reduces the impact of privacy concerns on the willingness to disclose High affective commitment increases the impact of positive outcomes on the willingness to disclose	Kordzadeh and Warren (2017)

Table 1 (continued)

Theory	Assumption	Trade-off/context	Privacy choice	References
Behavioral economics	1. Co-existence between normative and behavioral influences 2. Privacy preferences are unstable in privacy choices because of cognitive heuristics and biases 3. Privacy behavior is context-dependent	Consumers may overestimate their response to normative influences, while underestimate their response to behavioral influences Context: There were two samples. Participants of the first sample were recruited from Amazon Mechanical Turk for Experiments 1 and 2. Participants of the second sample were recruited from Prolific Academic for Experiment 3	Objective benefits and costs, i.e., normative influences, determine disclosure intention Relative perceptions of risks and benefits, i.e., behavioral influences, determine actual disclosure	Adjerid et al. (2018)

a rebalanced trade-off is also assumed to lie in the risk–benefit paradigms. In this study we focus on general privacy risks, but not context-specific privacy risks (Karwatzki et al. 2022). Alternatives that take self-disclosure to predict the anticipated benefits are considered, but such a causal link may violate the reasoning of user resistance, and lead to an inverse of trade-offs.

The phenomenon of privacy paradox is better understood by the stability-change dichotomy in which mechanisms and outcomes of human-technology interactions (e.g., social interactions on Facebook) are often assumed complementary but not mutually exclusive. We consider stability and change (or instability) as two essential elements to explain the underlying mechanisms of paradoxical relationship, such as the paradoxical relationship between privacy concerns and information disclosure (Acquisti and Grossklags 2004, 2005). Stability and change are *fundamentally interdependent or contradictory but mutually enabling and constituting each other*, i.e., the duality view (Farjoun 2010). According to the duality view, the change of mechanisms enables stability outcomes, while the stability of mechanisms enables change outcomes. The approach to consider privacy calculus as the two-sided forces (e.g., risks and benefits) for either constraining or enabling self-disclosure is inconsistent with the phenomenon of privacy paradox. From the duality view, we consider the proposed risk–benefit paradigms as two-sided factors that are conditionally balanced to enable the resistance and willingness toward privacy disclosure. The examination of user resistance helps to address the potential instability of privacy choices.

According to psychological reactance (Brehm and Brehm 1981), people that enjoy their behavioural freedom would achieve a negative emotion response to the threats to behavioral freedom. The restoring of behavioral freedom is called reactance. Facebook users may not consider the disclosure of private information as the threats to behavioral freedom given that the disclosure freedom is not completely eliminated or restricted, such as partial disclosure of sensitive information (Core 2001). We adopt "resistance toward information disclosure" to define people's psychological reaction to the concern on negative behavioral outcomes (the weaker reaction) or the violation of personal autonomy (the stronger reaction) but not the notion of negative emotional response. For consumers, resistance to use an innovation mostly stems from functional barriers (e.g., incompatibility) and/or psychological barriers (e.g., conflicting with belief structure) (Ram and Sheth 1989). For Facebook users, we consider user resistance mostly stems from psychological barriers to privacy disclosure. People often resist to an innovation in the way of rejection, postponement, or opposition in order to avoid, reduce, or control the uncertainty of behavioral outcomes, respectively (Szmigin and Foxall 1998). In the context of privacy choices, the fear of losses and the willingness to against privacy risks may cause people's resistance toward privacy disclosure (Hirschheim and Newman 1988; Klaus and Blanton 2010).

2.3 A trade-off between risks and benefits

The boundary of privacy between private (e.g., incomes) and public (e.g., honours) information would define personal privacy (Petronio 2002), and also define the red

lines of privacy invasion for an individual. Privacy is a concern for individuals and linked to the ability to the control of private information on making privacy protections or valuable exchanges in specific contexts (Smith et al. 2011). Privacy calculus refers to the *calculus of behavior* conducted on personal information processing in the context of changing environments, unpredictable behavioral outcomes, and new technologies that emerge at various stages of the life (Laufer and Wolfe 1977). Privacy calculus also refers to the disclosure of private information in exchange for an individual's economic and social benefits (Culnan and Armstrong 1999). According to Dinev et al. (2008), the information asymmetry between people and government under institutional surveillance rendering privacy risks about the abuse of personal information by the government. Likewise, the phenomenon of information asymmetry exists in which Facebook users lose the control about the processing of their disclosed profiles behind the platform. According to privacy calculus theory, people would develop the beliefs of risk–benefit analysis of information disclosure under the influence of privacy concerns and privacy risks (Dinev and Hart 2006). Privacy concern is a specific belief driven by experience and context (Culnan and Armstrong 1999). Privacy risk is a general belief of one's expected losses from the disclosure of personal sensitive information (Xu et al. 2011a, b). Privacy concern is more related to one's perceived ability to control the disclosure of personal information, privacy risk is more related to the possibility of loss in information disclosure (Dinev and Hart 2006). Privacy concerns reflect perceived control over privacy choices according to one's confidence in specific contexts, while privacy risks are considered as perceived losses from privacy disclosure according to the estimation of probabilities. From the information privacy framework (Ozdemir et al. 2017), privacy concerns and privacy risks differ in term of antecedents and outcomes.

Privacy calculus theory that develops based on a risk–benefit analysis has been widely used to predict consumers' willingness toward private information disclosure in online transactions (Dinev and Hart 2006), online chat rooms (Jiang et al. 2013a, b), mobile applications (Kehr et al. 2015; Wang et al. 2016), location-based services (Xu et al. 2011a, b; Xu et al. 2009), virtual health communities (Kordzadeh and Warren 2017), SNSs (Dienlin and Metzger 2016), and ride-sharing services (Cheng et al. 2021). In sum, privacy calculus was used to address how to make the trade-offs between perceived benefits and perceived risks. The early privacy calculus model examined the balance between privacy risk beliefs (e.g., privacy risks and concerns) and confidence-enticement beliefs (e.g., trust and personal interest) regarding online disclosure of personal information (Dinev and Hart 2006). The reality of Internet privacy for the majority of people is far from the balance between privacy concerns and personal interests because individual needs of privacy protection and social environments of personal life are constantly interacting and changing (Acquisti et al. 2015). People may perceive the rewards outweigh the risks of information disclosure, i.e., an imbalanced trade-off, when they focus on the value of relationship intimacy by minimizing the risk beliefs of self-disclosure (Jiang et al. 2013a, b). Privacy calculus theory takes an exchange view to address whether consumers are willing to disclose private information (e.g., anticipated risks) to get the return of value (e.g., anticipated benefits) in the personalization (Xu et al. 2011a, b). However, the calculation of privacy in the disclosure of private information is beyond

the trade-offs framework because anticipated benefits and anticipated risks are not evaluated on the same time point. For example, mobile phone users tend to exhibit dichotomous attitudes toward the disclosure of privacy in the imbalanced risk–benefit trade-offs (Goes 2013). The theory of hyperbolic discounting explains that people prefer an early reward to a late reward (Ainslie 2002). Beyond a rational trade-off, prior habits provide the reason to explain the irrational disclosure of private information (Fernandes and Pereira 2021). The disclosure of personal information looks like a context-dependent decision-making process (Acquisti et al. 2015; Punj 2019; Yu et al. 2020). The underlying assumptions of privacy calculus such as rational (e.g., cost–benefit analysis) and irrational (e.g., the embeddedness of habits), as well as context-dependence of privacy concerns (Acquisti et al. 2015), may overlook the stability of privacy choices in theory development. Moreover, the assumption of stable preferences for privacy calculus does not fit the reality of privacy choices (Adjerid et al. 2018). We thus address the anomaly of privacy paradox that lies in the stability-instability dichotomy of privacy decisions.

2.4 Embeddedness of social support

Social capital refers to public resources in a community, such as information, social relationship and capacity, that can be shared with people for better collective actions or social outcomes (Coleman 1988; Paxton 1999; Woolcock and Narayan 2000). The concepts of social capital help individuals to achieve a stable balance between private and collective benefits. There are two forms of social capital, "bridging" social capital that enables individuals to access the information from external ties (Nahapiet and Ghoshal 1998), and "bonding" social capital that helps individuals pursue cohesive relations through internal ties (Adler and Kwon 2002). The influence of external and internal ties on social interactions and human behaviors provides possible incentives to foster the use of social networks for personal benefits (Newell et al. 2004). Bridging social capital refers to loose connections between networked members that can provide and receive useful information (Ellison et al. 2007), which rely on the approach to promote casual acquaintances and connections of view via information support (Claridge 2018). Bonding social capital refers to strong ties between networked members or those members holding emotionally close relationships (Ellison et al. 2007), which rely on the approach to reinforce intimate interpersonal relationship via emotion support (Claridge 2018).

Compared with offline communication, online communication is more crucial to the competition among profit-seeking SNSs. Facebook has adapted social information-seeking and relational communication strategies to embed social capital in the structure of networks and the habit of individuals (Ellison et al. 2007, 2010; Valenzuela et al. 2009). Social capital is localized at individuals to reinforce their belongingness to a group or a community (Adler and Kwon 2002). The development of social capital helps people produce positive social outcomes, such as civic trust, mutual cooperation, and behave reciprocity in social life (DeFilippis 2001; Ellison et al. 2007). Facebook users that have developed their social ties would also extend their online connections. For Facebook users, such online connections help to

develop their social support that can be directly personalized to meet personal interests. Compared with the three-dimension framework of social capital that focused on both personal and collective goals and actions (Treacy et al. 2017; Wasko and Faraj 2005), we adopt "social support" instead of "social capital" to address how Facebook users develop their online connections to pursue the individual preference of benefits and whether the support from information and emotion can work (Liang et al. 2011; Taylor et al. 2004).

People can easily find the current benefits of personal decisions, but feel the difficulty or perceive the uncertainty to judge future benefits of personal choices. Hence, people tend to discount future benefits of personal choices. The disclosure of private information on Facebook is a good example to explain why people need "social support" or "social trust" to against privacy risks or the uncertainty of personal control over information abuse. It is not surprising that people "need" (e.g., rely on, use, develop) social communication or interpersonal relationship even in the risks of privacy invasion or information abuse. According to privacy calculus, people are supposed to take privacy risks as an exchange of the existing benefits. Obviously, the risk estimate of information disclosure is not completely reduced by the borders of privacy. It is overconfident on the estimation of privacy risks according to the frequency of past privacy invasion events (Knight 1921). The misuse and misinformation on profit-seeking SNSs to invade the boundaries of privacy may cause unexpected losses of privacy (Smyth 2019). The unstable states between "existing benefits" and "future benefits", the estimate of uncertainty in terms of "current risks" and "future risks" in information disclosure, and thereby the imbalance between risk and benefit beliefs would cause the instability of privacy choices. Using a risk–benefit analysis to make the decision to disclose or withhold privacy, the benefits of emotion support and instrumental support are better to maximize social support and thereby encourage the disclosure of private information (Kingsley Westerman et al. 2022). Without the instability of privacy choices, instrumental support and information support are good measures of social support. Building on *the risk–benefit paradigms*, we consider the embeddedness of "bridging" and "bonding" social support in privacy calculus is better to reduce the instability of privacy choices given that human behaviors are enabled and constrained by the current social systems (Giddens 1979).

3 Research model and hypothesis development

We address self-disclosure willingness rather than actual disclosure because the latter is often hidden by platform regulations. Moreover, actual disclosure is more related to the behavior of context-dependent privacy choices. Privacy calculus is the underlying theory adopted to develop the theoretical lens (Fig. 1). We develop the risk–benefit paradigms to extend the anticipated risks to encompass privacy concerns and privacy risks. The perceived benefits stem from information support and emotion support are conducted on the view of social support. Given the influence route from offline to online connections between Facebook users (Ellison et al. 2007), we assume that information support and emotion support have been

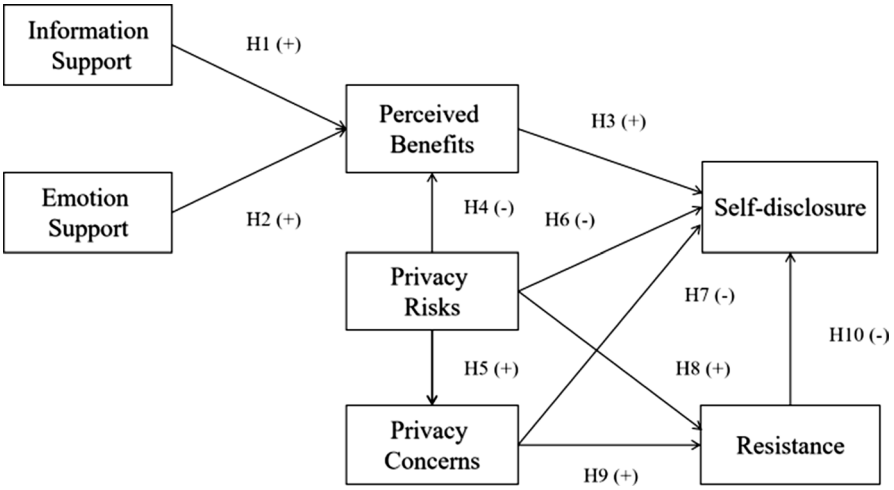

Fig. 1 Research model of self-disclosure

embedded in online social interactions, i.e., *the structuration process of technology* (Orlikowski 1992). Previous studies considered Internet trust or trusting beliefs as an enabler of self-disclosure (Dinev and Hart 2006; Malhotra et al. 2004). But, other research argued that the disclosure of private information would make people to trust in interpersonal relationship (Schoenbachler and Gordon 2002).

Users develop their beliefs of system usages, including internally (e.g., human–computer interactions) and externally (e.g., system functions) oriented beliefs of the system. Cenfetelli (2004) defines enablers and inhibitors as those external beliefs of system usages that would encourage and discourage adoption behavior, respectively. Hence, enablers and inhibitors are not opposites of one another; meanwhile, both beliefs differ in terms of causes and effects. Resistance to a change in either organizational routines or personal habits seems to act as an inhibitor of innovation (Bovey and Hede 2001; Mani and Chouk 2017). From the study of physician's resistance behaviors (Lapointe and Rivard 2005), the interaction with new technology would lead to the perception of threats or stresses, and individual user might respond with resistance behaviors, from passive to active, as well as from individual-level to group-level. A threat is an external stimulus (Witte 1992). A fear emerges from a threat in which individuals respond with fear-inducing perceptions of the threat (Rogers 1975). Taken together, fears and perceived threats from privacy invasion may cause behavioral change. Bhattacherjee and Hikmet (2007) took resistance to change as an external inhibitor under the threat condition. In contrast, we consider user resistance as an internal inhibitor of self-disclosure under the uncertainty of losses in information misuse in which people would make against the misuse. User resistance is a psychological reaction to the situation that individuals skin to frustration of personal control over the misconduct of private information and the threats to privacy in the data-driven algorithms (Hirschheim and Newman 1988). We take privacy risks and privacy concerns rather than perceived threats as the

antecedents of user resistance toward information disclosure. User resistance was less examined in prior work, it is more related to one's implicit unwillingness based on conscious thoughts that should be detailed in the study of privacy choices.

3.1 Information and emotion support

Social support is a human need that exists along with social relationships, and defined as the accumulated experience of mutual assistance and obligations that contribute to well-being lives (Wills 1991). Information support, instrumental and emotional support are three norms of social support that can help to sustain social relationships (Taylor et al. 2004). Facebook users are motivated to share information and sustain close relationship on the platform (Waters and Ackerman 2011). Information support and emotion support are believed to reinforce reciprocal motivation to share information and receive the support from others, respectively (Liang et al. 2011). Facebook users may consider information support and emotion support as the "metaphor" of switching costs if they leaving intimate members or losing social identities on the platform. Information support is one of the motivations for Facebook users that need advices or encounter problems. Emotion support is crucial to those people that need the support from friends or the sharing of interests in online connections. The reciprocity of social interactions or the norm of social support in terms of either information support or emotion support would increase the benefit beliefs of mutual trust (Ellison et al. 2007; Woolcock and Narayan 2000). In converting social resources to meet the preference for benefits, "bridging" and "bonding" influences of social support should be examined independently (Newell et al. 2004). We posit that:

H1 Information support of Facebook use would positively affect users' perceived benefits of online disclosure.

H2 Emotion support of Facebook use would positively affect users' perceived benefits of online disclosure.

3.2 Perceived benefits

The anticipated benefits of personalized services mostly encompass the support for information and entertainment would promote users to access online personalization (Xu et al. 2009). People that desire for intimate relationship, social identity, and social support would perceive the stable benefits of social support. People may trust a digital platform, depending on the promise that the support of positive social outcomes can be converted to meet personal interests in against the uncertainty of information misuse (Krasnova et al. 2010). Facebook users would perceive the benefits of disclosure that come from information support and emotion support, such as the ability to share thoughts and feelings with others (Acquisti et al. 2015). Compared with privacy risks, the desire for personal interests, such as relationship intimacy and social identity, would encourage personal disclosure (Dienlin and Metzger

2016). We consider perceived benefits that develop on personal interests would play the role as an enabler of information disclosure. We thus posit that:

H3 Perceived benefits of disclosure would positively affect Facebook users' willingness toward self-disclosure.

3.3 Privacy risks

Privacy is a concept of self-right that individuals perceived the control over personal information in which others have limited access to the information. Facebook has incentives to break the self-right of users and persuade them to build profiles online. Online disclosure of private information may tempt opportunistic behavior because of low costs of privacy invasion, such as unauthorized access, identity theft, and selling consumer database. For individuals, the disclosure of private information is judged on the benefits of a close relationship, as well as the potential of privacy risks and privacy concerns that across the borders of privacy (Culnan and Armstrong 1999).

Privacy risks refer to general beliefs of vulnerability or loss in the misuse of personal information (Dinev and Hart 2006). Privacy concerns refer to specific beliefs of personal control over private information based on technological capabilities (Dinev and Hart 2006). Facebook users that perceive privacy risks in online connections would perceive possible losses in information abuse, leading to mitigate their benefit evaluation of the platform. According to Dinev and Hart (2006), privacy risks and privacy concerns are distinct factors, but work as related beliefs of privacy calculus theory. Regarding the disclosure of private information, the risk beliefs of privacy would increase Facebook users' privacy concerns about the control over personal information. Facebook users that perceive the risks of privacy in the abuse of personal information would less likely to disclose their profiles online. In sum, we posit that:

H4 Privacy risks would negatively affect Facebook users' perceived benefits of online disclosure.

H5 Privacy risks would positively affect Facebook users' privacy concerns of online disclosure.

H6 Privacy risks would negatively affect Facebook user' willingness to disclose private information.

3.4 Privacy concerns

Facebook users that have concerns about their control over the spreading of private information online are supposed to have low levels of ability to control their profiles on the platform. The reason is obvious that most Facebook users want to minimize the negative outcomes of information abuse or illegal access. According to privacy

calculus theory (Dinev and Hart 2006), privacy concerns mitigate consumers' willingness to disclose personal information online. From the phenomenon of privacy paradox (Pavlou 2011), and the temptation of privacy invasion, this study examines whether privacy concerns can mitigate the willingness to disclosure on Facebook. We thus posit that:

H7 Privacy concerns would negatively affect Facebook users' willingness to disclose private information.

3.5 Antecedents of resistance

External and internal influences provide the reasons about why user resistance occurs (Martinko et al. 1996). External influence refers to the threats that associate with behavioral change (Marakas and Hornik 1996), internal influence refers to personal control over behavioral change (Martinko et al. 1996). The perspective of status quo biases can provide the explanation for people's user resistance toward misuse of personal information (Samuelson and Zeckhauser 1988). People want to maintain current status or situation because a change may increase the costs and lose the control. Perceived benefits of switching did not provide the incentive to reduce user resistance toward the implementation of a new information system (Kim 2011). Hence, we consider that "perceived benefits" is not a significant antecedent of user resistance. People resist to using a new technology that is considered a threat to possible losses or personal control over resources (Bhattacherjee and Hikmet 2007), or because the new technology does against their habits or routines (Mani and Chouk 2017). The antecedents of user resistance include external and internal factors (Hirschheim and Newman 1988). A general belief of privacy risks referring to the unpredictable loss of information misuse that would play the role as an external factor of user resistance. A specific belief of privacy concerns referring to personal control over information misuse that would play the role as an internal factor of user resistance. We thus posit that:

H8 Privacy risks would positively affect Facebook users' resistance toward information disclosure.

H9 Privacy concerns would positively affect Facebook users' resistance toward information disclosure.

3.6 Outcomes of resistance

Consumers may resist to using an innovation because of functional and psychological barriers (Ram and Sheth 1989). Compared with functional barriers, we consider that psychological barriers are better to explain why people resist to disclosing private information online. Knowing that self-disclosure behavior is irreversible and out of personal control once exposed, people are supposed sensitive to the disclosure. Bhattacherjee and Hikmet (2007) have emphasized, "*resistance is not the*

mirror opposite of IT acceptance, but a possible antecedent of IT acceptance" (p. 728). Resistance and adoption coexist in user behaviors (Mani and Chouk 2017). Likewise, resistance and self-disclosure may coexist to shape Facebook users' privacy choices. The psychological reaction to privacy as caused by psychological barriers would likely inhibit Facebook users from disclosing personal information. We thus posit that:

H10 Facebook users' resistance toward information disclosure would negatively affect their willingness to disclose private information on the platform.

4 Method

4.1 The instrument

The measurement items were mostly conducted by modifying prior measures with wording change to meet the survey of Facebook users, but not benefit-oriented consumers ("Appendix"). People's beliefs of privacy risk and privacy concern differ between online transactions and social interactions because the former is activated by technology-push solutions, while the latter is activated by need-pull connections (Debatin et al. 2009; Dienlin and Metzger 2016; Dinev and Hart 2006). We modified previous scales of privacy risks adopted from Malhotra et al. (2004) and previous scales of privacy concerns adopted from Awad and Krishnan (2006) for reflecting the core elements of beliefs in online social interactions, but not the beliefs developed based on the type of information (Xu et al. 2009). The modified measures of privacy concerns focus on the lose of confidence and control, and the threats to information disclosure. The modified measures of privacy risks focus on risk beliefs about the potential for losses and unexpected outcomes in privacy disclosure. Information support and emotion support were measured by modifying previous scales (Liang et al. 2011). We measured perceived benefits in terms of social rewards, such as relationship intimacy, social identity (or acceptance), and social support (Ellison et al. 2007; Jiang et al. 2013a, b). Self-disclosure was examined using the scales in terms of users' willingness to disclose specific private information. Two scales of Bovey and Hede (2001) and one self-developed scale were adopted to measure user resistance. All measurement items of the instrument were anchored using five-point Likert scales and translated from English to Chinese, as well as improved before lunching the formal survey.

4.2 The sample survey

According to NapoleonCat website (www.napoleoncat.com), Facebook users in Taiwan have reached eighty percent of the population (19 million) in 2019. The survey targeted at experienced Facebook (Taiwan) users—those users with daily use (Table 2), they may disclose their private information on the platform even though they consider the abuse of disclosed information as potential concerns and risks

Table 2 Profiles of the respondents (N = 311)

Characteristics	Count (%)
Gender	
Male	139 (44.7%)
Female	172 (55.3%)
Age	
18–24	5 (1.6%)
25–34	120 (38.6%)
35–44	124 (39.9%)
45–54	48 (15.4%)
55 or above	14 (4.5%)
Education level	
High school	39 (12.5%)
Junior college	58 (18.7%)
College/University	172 (55.3%)
Graduate school	42 (13.5%)
Job categories	
Students	5 (1.6%)
House wife/husband	15 (4.8%)
Public administrations	48 (15.4%)
Private sectors	235 (75.6%)
Others	8 (2.6%)
Daily use time (hours)	
< 0.5	81 (26.0%)
$0.5 \leq \sim < 1$	95 (30.6%)
$1 \leq \sim < 2$	70 (22.5%)
$2 \leq \sim < 3$	33 (10.6%)
$3 \leq$	32 (10.3%)

of privacy. This study collected a general sample of voluntary Facebook users via online questionnaire survey, and received a total of 311 completed questionnaires in the survey (Table 2). Regardless of the levels of utilization experience in Facebook, we consider those users or groups of users that have adopted and continued use of Facebook as a general sample.

4.3 Reliability, validity, and goodness-of-fit

The factor analysis (Table 3) indicates all higher factor loadings for the measurement items of the corresponding construct compared with lower cross-loadings for other items, exceeding the 0.60 threshold (Hair et al. 2010), and thus achieving convergent validity. The Cronbach's alphas and the composite reliability (Table 4) of each construct significantly exceeded the 0.70 threshold (Nunnally 1978), achieving acceptable reliability (Fornell and Larcker 1981). From Table 4, the average variance extracted for each construct significantly exceeded the 0.50 threshold (Fornell

Table 3 Factor analysis—factor loadings and cross-loadings of measurement items

Item	ES	PR	R	IS	PB	PC	SD
ES1	**0.859**	0.044	−0.034	0.223	0.020	0.063	0.015
ES2	**0.895**	0.093	0.025	0.202	0.026	0.010	0.144
ES3	**0.861**	0.046	−0.010	0.270	−0.012	0.003	0.037
ES4	**0.867**	0.058	0.023	0.306	0.018	0.024	−0.017
PR1	0.057	**0.834**	0.222	0.101	−0.081	0.164	−0.117
PR2	0.091	**0.862**	0.130	0.047	−0.144	0.268	−0.095
PR3	0.106	**0.833**	0.121	0.133	−0.069	0.274	−0.165
R1	0.028	0.053	**0.830**	−0.023	0.050	0.092	−0.020
R2	0.001	0.180	**0.853**	0.033	−0.040	−0.023	−0.107
R3	−0.030	0.157	**0.882**	0.043	−0.091	0.045	−0.094
IS1	0.400	0.077	0.020	**0.813**	0.092	0.104	0.035
IS2	0.461	0.122	0.038	**0.826**	0.056	0.037	0.176
IS3	0.452	0.121	0.012	**0.827**	−0.051	0.072	0.182
PB2	0.001	−0.168	−0.036	0.033	**0.929**	−0.035	0.149
PB3	0.044	−0.068	−0.031	0.102	**0.916**	−0.090	0.215
PC2	0.090	0.296	0.075	−0.016	−0.061	**0.873**	−0.065
PC3	0.025	0.364	0.045	0.072	−0.074	**0.839**	−0.120
SD1	0.010	−0.159	−0.212	0.007	0.198	−0.066	**0.851**
SD3	0.085	−0.150	−0.021	−0.006	0.175	−0.104	**0.882**
Eigenvalue	3.651	2.546	2.336	2.335	1.839	1.683	1.674
Cumulative variance (%)	19.215	32.614	44.909	57.197	66.877	75.736	84.548

It is better that the factor loading of bold items should exceed 0.7. The score of diagonal elements should exceed that of off-diagonal elements

and Larcker 1981). The square root of the average variance extracted for each construct significantly exceeded the correlation between that and other constructs (Table 4), achieving acceptable discriminant validity (Fornell and Larcker 1981). From the seven goodness-of-fit indexes associated with the cut-off scores (Bagozzi et al. 1991), the measurement model and the structural model have passed the goodness-of-fit tests (Table 4).

4.4 Common method variance

To examine common method variance (CMV), we adopt a *post-hoc* approach to test the self-reported data. First, we adopted Harmon's one-factor test, the largest variance explained by one factor, i.e., the "emotion support" factor, was under 20% (Table 3). Hence, the factor did not explain the majority of the variance (Podsakoff and Organ 1986). Second, we examined the inter-construct correlations (Table 4), the highest correlation (0.695) between information support and emotion support was far below the threshold of 0.90 (Bagozzi et al. 1991). Third, we examined the

Table 4 Tests of reliability, validity and goodness-of-fit

Var	Mean	SD	α	CR	IS	ES	PB	PC	PR	R	SD
IS	3.58	0.70	0.94	0.96	**0.822**						
ES	3.54	0.65	0.93	0.96	0.695	**0.871**					
PB	2.91	0.84	0.90	0.92	0.119	0.049	**0.922**				
PC	3.53	0.72	0.84	0.90	0.115	0.125	−0.190	**0.856**			
PR	3.92	0.65	0.90	0.95	0.241	0.182	−0.258	0.602	**0.843**		
R	3.78	0.80	0.84	0.86	0.058	0.016	−0.110	0.166	0.338	**0.855**	
SD	2.26	0.89	0.80	0.81	0.015	0.068	0.411	−0.259	−0.349	−0.240	**0.867**

Diagonal elements represent the square roots of the AVEs of the constructs, while the other matrix elements represent the inter-construct correlations

Goodness-of-fit indexes (the measurement model): χ^2/df = 1.588; SRMR = 0.02; RMSEA = 0.04; GFI = 0.93; AGFI = 0.90; NFI = 0.95; CFI = 0.98

Goodness-of-fit indexes (the structural model): χ^2/df = 2.615; SRMR = 0.03; RMSEA = 0.07; GFI = 0.98; AGFI = 0.94; NFI = 0.95; CFI = 0.97

Cut-off scores of goodness-of-fit indexes (Bagozzi and Yi 1988): Chi-square/degree of freedom ($\chi^2/df \leqq 3.00$); standardized root mean square residual (SRMR ≦ 0.05); root mean square error of approximation (RMSEA ≦ 0.08); goodness-of-fit index (GFI ≧ 0.90); adjusted goodness-of-fit index (AGFI ≧ 0.80); normed fit index (NFI ≧ 0.90); comparative fit index (CFI ≧ 0.90)

α, Cronbach's α; CR, Composite reliability

It is better that the factor loading of bold items should exceed 0.7. The score of diagonal elements should exceed that of off-diagonal elements

correlation between a marker variable, i.e., a theoretically unrelated variable (e.g., "fake disclosure"), and the seven constructs (Lindell and Whitney 2001). The average correlation coefficient of the marker variable with other constructs was small (0.075). In sum, we consider CMV is not a concern of this study.

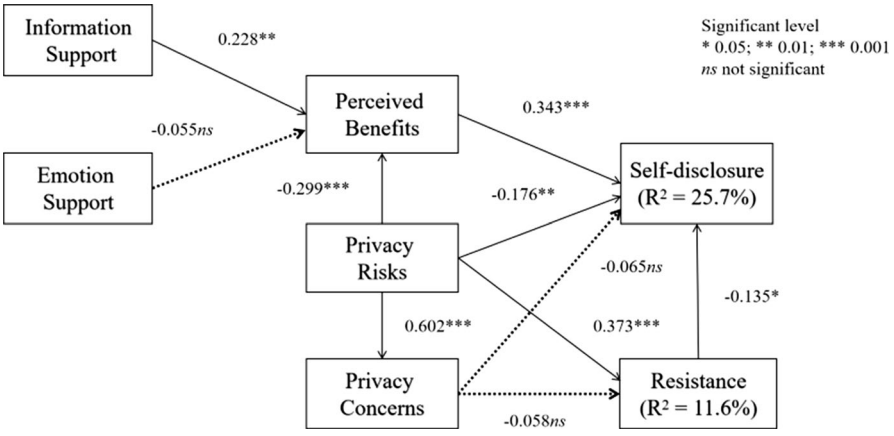

Fig. 2 Empirical results of Facebook users

4.5 Hypothesis testing

From the empirical results (Fig. 2), we have found that the positive effect of information support on perceived benefits (hypothesis H1), the positive effect of perceived benefits on self-disclosure (hypothesis H3), the negative effect of privacy risks on perceived benefits (hypothesis H4), the positive effect of privacy risks on privacy concerns (hypothesis H5), the negative effect of privacy risks on self-disclosure (hypothesis H6), the positive effect of privacy risks on resistance (hypothesis H8), and the negative effect of resistance on self-disclosure (hypothesis H10) are all significant. In contrast, hypotheses H2, H7, and H9 are not supported. Re-examine the effect of perceived benefits on resistance, the path coefficient (−0.017) is insignificant in the study. The research model accounted for 25.7% of variances in self-disclosure and 11.6% of variances in user resistance.

5 Discussion and conclusions

5.1 Implications for theory

The occurrence of privacy risks is inevitable on Facebook, but the anticipated benefits of social interactions and relationship intimacy can be used to encourage users' self-disclosure. The embeddedness of social support to explain the disclosure of private information was less examined in the literature (Martin and Murphy 2017). The embeddedness of information support and emotion support is expected to reduce the instability of privacy choices underlying changing privacy preferences in rational calculus. People, including Facebook users, are not totally rational in privacy choices (Table 1). In this study, the embeddedness of "bridging" social support in privacy calculus has been found to reshape the risk–benefit paradigms to foster users' willingness to disclose online by stabilizing the desire for information support or inhibiting the change in privacy preferences (Farjoun 2010). The first implication is that we adapt the risk–benefit paradigms to explain why privacy calculus should be stabilized underlying the uncertainty of information misuse, and how the trade-offs are rebalanced via the embeddedness of information support instead of rational calculus-grounded theories (Adjerid et al. 2018).

From the empirical results, perceived benefits, privacy risks, and user resistance are three antecedents of self-disclosure willingness, privacy risk is the antecedent of user resistance. Hence, user resistance and self-disclosure are not located at the opposite ends of the same conceptual spectrum according to the inconsistent antecedents. User resistance and self-disclosure would coexist in the presence of privacy risks. Perceived benefits can encourage self-disclosure, but cannot affect user resistance. In contrast, privacy risks inhibit self-disclosure, but enable user resistance. A possible explanation is that an enabler is better to encourage behavioral intention, while an inhibitor is easy to cause psychological reaction. The appealing to anticipated benefits is a better route to enable self-disclosure willingness, while the threatening to anticipated risks is more influential to enable user resistance toward information disclosure. The second implication is the risk–benefit paradigms instead of

the imbalanced trade-offs would enable self-disclosure willingness and user resistance via distinct routes, leading actual disclosure to become more unpredictable.

Previous studies verified that privacy risks and privacy concerns would reduce consumers' willingness to disclose private information in online transactions or mobile services (Dinev and Hart 2006; Keith et al. 2013; Li et al. 2011). In contrast to the information privacy framework (Ozdemir et al. 2017), the empirical results of this study indicate that privacy risks rather than privacy concerns would reduce the willingness toward self-disclosure on Facebook. The effect of privacy concerns is probably reduced when individuals surrender partial control over personal information. The change of context, from online transactions to SNSs, may provide stronger incentives to loosen personal control over privacy. Facebook users tend to perceive lower ability of control over personal information than shoppers because they need intimate relationships. Pavlou (2011) explains that the presence of information privacy attitudes would mitigate the effect of privacy concerns on self-disclosure willingness. The presence of an external factor, such as privacy risks, probably enables the internal factor, such as privacy concerns, to become a weak inhibitor of self-disclosure. Another possible explanation is the potential losses of personal disclosure that can be compensated by the benefits of that disclosure, coinciding with earlier findings that trust can compensate privacy risks and thereby encourages self-disclosure (Ozdemir et al. 2017). The third implication is that external and internal factors differ in making the trade-offs of self-disclosure.

5.2 Implications for practice

Policymakers believe that "default settings" or "nudge" can help people make better choices, such as organ donation or retirement saving (Thaler and Sunstein 2008). Digital platforms, such as Facebook and Pinduoduo (China), are professional about how to use "default settings" to encourage information disclosure and how to manipulate the desire for free lunch. It is not surprising that "default settings" can help digital platforms "legally" collect more visible profiles despite the fact that users are either aware or unaware of the surrender of their privacy in exchange for free lunch (Acquisti et al. 2015). We highlight the empirical findings of this study for Facebook users and the likes of whom. Privacy paradox does always exist once perceived benefits can satisfy the desire for free information and perceived risks are believed to be controlled under privacy protection policies. Platform users need privacy protection policies, but platform owners and creators define the rules of game—play or not. Policymakers want people to believe the trade-offs of life or an exchange of privacy, but the judgment on the risk and uncertainty of information disclosure is driven by the conflicts of belief in one's privacy choices. Yet, we echo the view that contexts matter in privacy preferences and behaviors (Acquisti et al. 2015). We proceed one more step that privacy choices are determined by the boundaries of the risk–benefit paradigms, i.e., the conflicts of privacy beliefs can be used to examine the stability and instability of privacy preferences and behaviors.

Previous studies focused on guiding firms to provide technological solutions and develop information privacy policies (Bélanger and Crossler 2011), teaching people

to protect personal privacy (Chen and Rea 2004), or paying for privacy protection (Rust et al. 2002). From the risk–benefit paradigms, one rule is derived that benefit beliefs of information support rather than emotion support will win the war on personalization. In contrast to information support, the spreading of emotion support mostly relied on intimate relationships that develop on trusting beliefs. Probably, the high correlation between information support and emotion support reveals that Facebook users might take the latter as a metaphor of social support, or consider it as the connection with "advice" or "information", but not the "bonding" connection. Hence, Facebook users are more likely to perceive more benefits of information support than the benefits of emotion support. Facebook is easily to foster information support via online connection strategies (Ellison et al. 2010). But online connections indicate "perceived publicness" (Bateman et al. 2011), which is not a core element of emotion support for Facebook users that need privacy protection. The effect of emotion support may probably depend on social contexts or specific grouping. The first implication is about the transparency and control of information sharing, which are better than the spreading of emotion support to meet the preferences for privacy choices (Acquisti et al. 2015).

In the context of cooperative work, "bonding" connection is considered as a prerequisite for converting "bridging" influence of social capital to benefit both individual and collective goals (Newell et al. 2004). However, it is not true in our study of privacy disclosure because Facebook users are motivated by the needs of the individual. A trade-off between benefits and risks for judging Facebook users' privacy disclosure is unlikely to be balanced underlying the conflicts of interest in rational calculus. However, the balance between personalization and privacy is crucial in digital marketing, which would render a trade-off between convenience and control for people in the coming era of artificial intelligence. Privacy protection and data collection are believed to be balanced on the proposition that less privacy concerns would encourage more disclosure of personal information (Liu et al. 2021). However, our study does not support the causal link. It is helpful for policymakers to focus on the boundary of personal information disclosure instead of the restriction of information disclosure in the design of privacy policy. The second implication is that the connection strategies drawn upon information support and emotion support should be aligned with external and internal ties of social networks, respectively.

Compared with a few (Wang et al. 2016), previous studies of privacy choices widely examined the enabling and hindering forces of personal information disclosure on Facebook were widely conducted in the United States and/or the sampling survey of college students (Dinev and Hart 2006; Jiang et al. 2013a, b; Jiang et al. 2013a, b; Keith et al. 2013; Kordzadeh and Warren 2017; Li et al. 2011; Ozdemir et al. 2017; Xu et al. 2011a, b; Xu et al. 2011a, b). Respond to the suggestion called for sample diversity (Bélanger and Crossler 2011), the survey of general sample of Facebook (Taiwan) exhibits different cultures from the United States. In the context of Facebook, privacy risks tend to reinforce user resistance and reduce the willingness toward self-disclosure. The strong effect (0.373) of privacy risks on user resistance might verify the force-reaction patterns underlying the moral norms and legal rights of privacy. The third implication is the risk–benefit paradigms that built on privacy calculus and social support are better than the trade-offs that built on

rational calculus to examine the psychological-behavioral tension in terms of user resistance and self-disclosure. For policymakers, the connection between personal benefits and social benefits may look as the boundary between "good" and "bad" in a society (Leclercq-Vandelannoitte and Aroles 2020). People are often asked to judge what's the good or bad, as well as for whom to get it. From the study of user resistance toward information disclosure, policymakers should learn that self-disclosure willingness may not guarantee actual disclosure.

5.3 Concluding remarks and limitations

We surveyed experienced Facebook users to answer the two questions about privacy paradox and privacy choices, which were previously examined using distinct theoretical frameworks, but exhibiting the conflicts of view (Table 1). Respond to the first question, we have found that privacy concerns did not significantly mitigate Facebook users' willingness to disclose private information, exhibiting the phenomenon of privacy paradox that users express their privacy concerns (or psychological reaction) but still intend to disclose. The phenomenon of privacy paradox can also be explained by the reasoning that privacy concerns and self-disclosure willingness are motivated by distinct factors. Our risk–benefit paradigms that built on a relative weighing approach to the comparison between anticipated risks and anticipated benefits in which the former is more likely to foster user resistance toward information disclosure, while the latter is better to foster self-disclosure. Hence, privacy is often exposed when the uncertainty of benefits is believed to be reduced.

The approach from the trade-offs between perceived risks and perceived benefits is simplistic, without examining why causes the instability of privacy choices, such as the co-existence between self-disclosure and user resistance toward information disclosure. To examine the instability of privacy choices, we develop the risk–benefit paradigms where risk and benefit beliefs are initially judged on imbalanced trade-offs. The risk–benefit paradigms are theoretically conducted on the embeddedness of social support (e.g., information support and emotion support) to develop the underlying mechanisms of privacy choices. Respond to the second question, the underlying mechanisms of privacy choices that embed "bridging" social support in privacy calculus can be conducted upon a rebalanced trade-off by stabilizing the perceived benefits of self-disclosure. In contrast, privacy risks would cause the instability of privacy choices. The risk–benefit paradigms help to address how the resistance and willingness toward information disclosure are interlocked to judge people's privacy choices.

This study is subjected to few limitations that should be examined in future research. First, user willingness (or intention) to disclose private information is not a good measure of actual self-disclosure behavior (Keith et al. 2013). The average user willingness toward self-disclosure ($\overline{u} = 2.26$) is far below the midpoint of 'neutral' in the questionnaire. The descriptive statistics indicate that the average perceived benefits ($\overline{u}_1 = 2.91$) did not exceed the average privacy risks ($\overline{u}_2 = 3.92$), which provide a good explanation of lower average self-disclosure. Second, the measurement of social support in terms of information support and emotion support is reasonable,

but might not meet the multi-dimensional framework of online social interactions and thus should be extended for the future. Third, partial disclosure and full disclosure on SNSs should be examined in future study. Fourth, cultural difference might shape people's risk beliefs of privacy disclosure, suggesting a direction for the future. Fifth, the extension of this study to other digital platforms (e.g., twitter or WeChat) should consider contextual disparity between work and entertainment. Sixth, slightly lower amount of variance explained in the model of self-disclosure and user resistance should be improved. Last but not the least, our sample may not represent the population of Facebook users in different nations. The limitation of our sampling should be considered in explaining the empirical results.

Appendix: The measurement items of research constructs

Information support (IS)

IS1 On Facebook, some people would offer suggestions when I needed help.
IS2 When I encountered a problem, some people on Facebook would give me information to help me overcome the problem.
IS3 When faced with difficulties, some people on Facebook would help me with suggestions.

Emotion support (ES)

ES1 When faced with difficulties, some people on Facebook are on my side with me.
ES2 When faced with difficulties, some people on Facebook would encourage me.
ES3 When faced with difficulties, some people on Facebook listened to me talk about my feelings.
ES4 When faced with difficulties, some people on Facebook expressed interests and concerns in my well-being.

Perceived benefits (PB)

PB1 Self-disclosure on Facebook is beneficial to sustain intimate relationship. (dropped)
PB2 Self-disclosure on Facebook is beneficial to build my social identity within a group.
PB3 Self-disclosure on Facebook is beneficial to get social support from others.

Privacy risks (PR)

PR1 Disclose private information on Facebook is risky for me.

PR2 Disclose private information on Facebook would bring with the potential of losses.
PR3 Disclose private information on Facebook would produce unexpected outcomes.

Privacy concerns (PC)

PC1 Disclose private information on Facebook is a concern for me. (dropped)
PC2 Disclose private information on Facebook looks like a lose of control for me.
PC3 Disclose private information on Facebook looks like a threat to me.

Resistance toward information disclosure (R)

Regarding the disclosure of private information on Facebook, my reaction to the disclosure is …

R1 Very unlikely … Very Likely (opposition)
R2 Strongly unwilling to … Strongly willing to (obstruct)
R3 Very impossible … Very possible (resistance)

Willingness toward self-disclosure (SD)

Regarding the use of Facebook, …

SD1 I am willing to disclose my mobile phone number on my profile.
SD2 I am willing to reveal very detailed thoughts and experiences in my profile. (dropped)
SD3 I am willing to post my email information on my profile.

Acknowledgements The authors thank the two anonymous referees for their valuable comments and suggestions on earlier versions of this paper.

Funding This research received partial financial support from Social Science Foundation of Fujian Province, China, under Project No. FJ2021B166. The authors do not have any personal relationships with other people or organizations that could inappropriately influence this research.

Declarations

Conflict of interest The authors declare that they have no known conflicts of interest or personal relationships that could influence the work reported in this manuscript.

References

Acquisti A (2009) Nudging privacy: the behavioral economics of personal information. IEEE Secur Priv 7(6):82–85. https://doi.org/10.1109/MSP.2009.163

Acquisti A, Grossklags J (2004) Privacy attitudes and privacy behavior. In: Camp LJ, Lewis S (eds) Economics of information security. Advances in information security, vol 12. Spring, Boston, pp 165–178. https://doi.org/10.1007/1-4020-8090-5_13

Acquisti A, Grossklags J (2005) Privacy and rationality in individual decision making. IEEE Secur Priv 3(1):24–30. https://doi.org/10.1109/MSP.2005.22

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

Acquisti A, Brandimarte L, Hancock J (2022) How privacy's past may shape its future. Science 375(6578):270–272. https://doi.org/10.1126/science.abj0826

Adjerid I, Peer E, Acquisti A (2018) Beyond the privacy paradox: objective versus relative risk in privacy decision making. MIS Q 42(2):465–488. https://doi.org/10.25300/MISQ/2018/14316

Adler PS, Kwon S-W (2002) Social capital: prospects for a new concept. Acad Manag Rev 27(1):17–40. https://doi.org/10.5465/amr.2002.5922314

Ainslie G (2002) The effect of hyperbolic discounting on personal choices. *Keynote speech to the thematic* session, "Personal choice and change". Annual convention of the American Psychological Association, Chicago. http://picoeconomics.org/Articles/APA.pdf

Awad NF, Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q 30(1):13–28. https://doi.org/10.2307/25148715

Bagozzi RP, Yi Y (1988) On the evaluation of structural equation models. J Acad Mark Sci 16(1):74–94

Bagozzi RP, Yi Y, Phillips L (1991) Assessing construct validity in organizational research. Adm Sci Q 36(3):421–458. https://doi.org/10.2307/2393203

Barth S, de Jong M (2017) The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior: a systematic literature review. Telematics Inform 34(7):1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth S, de Jong M, Junger M, Hartel PH, Roppelt JC (2019) Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics Inform 41(C):55–69. https://doi.org/10.1016/j.tele.2019.03.003

Bateman PJ, Pike JC, Butler BS (2011) To disclose or not: publicness in social networking sites. Inf Technol People 24(1):78–100. https://doi.org/10.1108/09593841111109431

Bélanger F, Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. MIS Q 35(4):1017–1041. https://doi.org/10.2307/41409971

Bélanger F, Hiller JS, Smith WJ (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. J Strat Inf Syst 11(3/4):245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bhattacherjee A, Hikmet N (2007) Physicians' resistance toward healthcare information technology: a theoretical model and empirical test. Eur J Inf Syst 16(6):725–737. https://doi.org/10.1057/palgrave.ejis.3000717

Bovey WH, Hede A (2001) Resistance to organizational change: the role of defense mechanisms. J Manag Psychol 16(7):534–548. https://doi.org/10.1108/EUM0000000006166

Brandimarte L, Acquisti A (2012) The economics of privacy. In: Peitz M, Waldfogel J (eds) Handbook of the digital economy. Oxford University Press, New York

Brandimarte L, Auquisti A, Loewenstein G (2013) Misplaced confidences privacy and the control paradox. Soc Psychol Personal Sci 4(3):340–347. https://doi.org/10.1177/1948550612455931

Brehm JW, Brehm SS (1981) Psychological reactance: a theory of freedom and control. Academic Press, San Diego
Bresnahan TF (2001) Network effects and Microsoft. Stanford University, Working paper
Cenfetelli RT (2004) Inhibitors and enablers as dual factor concepts in technology usage. J Assoc Inf Syst 5(11):472–492. https://doi.org/10.17705/1jais.00059
Chang C-W, Heo J (2014) Visiting theories that predict college students' self-disclosure on Facebook. Comput Hum Behav 30:79–86. https://doi.org/10.1016/j.chb.2013.07.059
Chen K, Rea AI (2004) Protecting personal information online: a survey of user privacy concerns and control techniques. J Comput Inf Syst 44(4):85–92
Cheng X, Hou T, Mou J (2021) Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. Inf Manag 58(6):103450. https://doi.org/10.1016/j.im.2021.103450
Claridge T (2018) Functions of social capital–bonding, bridging, linking
Clarke R (1999) Internet privacy concerns confirm the case for intervention. Commun ACM 42(2):60–67. https://doi.org/10.1145/293411.293475
Coleman JS (1988) Social capital in the creation of human capital. Am J Sociol 94:S95-120. https://doi.org/10.1086/228943
Core JE (2001) A review of the empirical disclosure literature: discussion. J Account Econ 31(1–3):441–456. https://doi.org/10.1016/S0165-4101(01)00036-2
Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness, impersonal trust: an empirical investigation. Org Sci 10(1):104–115. https://doi.org/10.1287/orsc.10.1.104
Davies SG (1997) Rethinking the right to privacy: how privacy has been transformed from a right to a commodity. In: Agre PE, Rotenberg M (eds) Technology and privacy: the new landscape. MIT Press, Cambridge, pp 143–165
Debatin B, Lovejoy JP, Horn A-K, Hughes BN (2009) Facebook and online privacy: attitudes, behaviors, and unintended consequences. J Comput Mediat Commun 15(1):83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x
DeFilippis J (2001) The myth of social capital in community development. Hous Policy Debate 12(4):781–806. https://doi.org/10.1080/10511482.2001.9521429
Dienlin T, Metzger MJ (2016) An extended privacy calculus model for SNSs: analyzing self-disclosure and self-withdrawal in a representative U.S. sample. J Comput Mediat Commun 21(5):368–383. https://doi.org/10.1111/jcc4.12163
Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. Inf Syst Res 17(1):61–80. https://doi.org/10.1287/isre.1060.0080
Dinev T, Hart P, Mullen MR (2008) Internet privacy concerns and beliefs about government surveillance: an empirical investigation. J Strat Inf Syst 17(3):214–233. https://doi.org/10.1016/j.jsis.2007.09.002
Ellison NB, Steinfield C, Lampe C (2007) The benefits of Facebook "Friends:" social capital and college students' use of online social network sites. J Comput Mediat Commun 12(4):1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x
Ellison NB, Steinfield C, Lampe C (2010) Connection strategies: social capital implications of Facebook-enabled communication practices. New Media Soc 13(6):873–892
Farjoun M (2010) Beyond dualism: stability and change as a duality. Acad Manag Rev 35(2):202–225. https://doi.org/10.5465/amr.35.2.zok202
Fernandes T, Pereira N (2021) Revisiting the privacy calculus: why are consumers (really) willing to disclose personal data online. Telematics Inform 65(2):101717. https://doi.org/10.1016/j.tele.2021.101717
Flender C, Müller G (2012) Type indeterminacy in privacy decisions: the privacy paradox revisited. In: International symposium on quantum interaction Q1, pp 148–159
Fornell C, Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. J Mark Res 18(1):39–50
Giddens A (1979) Central problems in social theory: action, structure and contradiction in social analysis. University of California Press, Berkeley
Goes PB (2013) Editor's comments: information systems research and behavioral economics. MIS Q 37(3):iii–viii
Hair JF, Black WC, Babin BJ, Anderson RE (2010) Multivariate data analysis, 7th edn. Prentice Hall, Upper Saddle River

Helmond A, Nieborg DB, van der Vlist FN (2019) Facebook's evolution: development of a platform-as-infrastructure. Internet Hist 3(2):123–146. https://doi.org/10.1080/24701475.2019.1593667
Hirschheim R, Newman M (1988) Information systems and user resistance: theory and practice. Comput J 31(5):398–408. https://doi.org/10.1093/comjnl/31.5.398
Hoffman DL, Novak TP, Peralta MA (1999) Information privacy in the marketplace: implications for the commercial uses of anonymity on the Web. Inf Soc 15(2):129–139. https://doi.org/10.1080/019722499128583
Hui K-L, Tan BCY, Goh C-Y (2006) Online information disclosure: motivators and measurements. ACM Trans Internet Technol 6(4):415–441. https://doi.org/10.1145/1183463.1183467
Hutchinson A (2020) Facebook closes in on new milestone of 3 billions total users across its platform. Social Media Today. https://www.socialmediatoday.com/news/facebook-closes-in-on-new-milestone-of-3-billion-total-users-across-its-pla/577048/. Accessed Feb 2021
Jiang LC, Bazarova NN, Hancock JT (2013a) From perception to behavior: disclosure reciprocity and the intensification of intimacy in computer-mediated communication. Commun Res 40(1):125–143
Jiang Z, Heng CS, Choi BCF (2013b) Privacy concerns and privacy-protective behavior in synchronous online social interactions. Inf Syst Res 24(3):579–595. https://doi.org/10.1287/isre.1120.0441
John LK, Acquisti A, Loewenstein G (2011) Strangers on a plane: context-dependent willingness to divulge sensitive information. J Consum Res 37(5):858–873. https://doi.org/10.1086/656423
Karwatzki S, Trenz M, Veit D (2022) The multidimensional nature of privacy risks: conceptualisation, measurement and implications for digital services. Inf Syst J 32(6):1126–1157. https://doi.org/10.1111/isj.12386
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. Inf Syst J 25(6):607–635. https://doi.org/10.1111/isj.12062
Keith MJ, Thompson SC, Hale J, Lowry PB, Greer C (2013) Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. Int J Hum Comput Stud 71(12):1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016
Kim H-W (2011) The effects of switching costs on user resistance to enterprise systems implementation. IEEE Trans Eng Manag 58(3):471–482
Kingsley Westerman CY, Haverkamp EM, Zeng C (2022) Understanding disclosure of health information to workplace friends. Behav Sci 12(10):355. https://doi.org/10.3390/bs12100355
Klaus T, Blanton JE (2010) User resistance determinants and the psychological contract in enterprise system implementations. Eur J Inf Syst 19(6):625–636. https://doi.org/10.1057/ejis.2010.39
Klopfer PH, Rubenstein DI (1977) The concept privacy and its biological basis. J Soc Issues 33(3):52–65. https://doi.org/10.1111/j.1540-4560.1977.tb01882.x
Knight FH (1921) Risk, uncertainty, and profit. University of Chicago Press, Chicago. https://ssrn.com/abstract=1496192
Kordzadeh N, Warren J (2017) Communicating personal health information in virtual health communities: an integration of privacy calculus and affective commitment. J Assoc Inf Syst 18(1):45–81. https://doi.org/10.17705/1jais.00446
Krasnova H, Spiekermann S, Koroleva K (2010) Online social network: why we disclose. J Inf Technol 25(2):109–125
Lapointe L, Rivard S (2005) A multilevel model of resistance to information technology implementation. MIS Q 29(3):461–491. https://doi.org/10.2307/25148692
Laufer RS, Wolfe M (1977) Privacy as a concept and s social issue: a multidimensional development theory. J Soc Issues 33(3):22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x
Laughlin Jr. SK (1968) Westin: privacy and freedom. Michigan Law Rev 66(5): 1064. https://repository.law.umich.edu/mlr/vol66/iss5/12
Leclercq-Vandelannoitte A, Aroles J (2020) Does the end justify the means? Information systems and control society in the age of pandemics. Eur J Inf Syst 29(6):746–761. https://doi.org/10.1080/0960085X.2020.1820912
Li H, Sarathy R, Xu H (2011) The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decis Support Syst 51(3):434–445. https://doi.org/10.1016/j.dss.2011.01.017
Liang T-P, Ho Y-T, Li Y-W, Turban E (2011) What drives social commerce: the role of social support and relationship quality. Int J Electron Commer 16(2):69–90. https://doi.org/10.2753/JEC1086-4415160204

Lindell MK, Whitney DJ (2001) Accounting for common method variance in cross-sectional research design. J Appl Psychol 86(1):114–121. https://doi.org/10.1037/0021-9010.86.1.114
Liu B, Pavlou PA, Cheng X (2021) Achieving a balance between privacy protection and data collection: a field experimental examination of a theory-driven information technology solution. Inf Syst Res 33(1):203–223. https://doi.org/10.1287/isre.2021.1045
Lowry PB, Dinev T, Willison R (2017) Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. Eur J Inf Syst 26(7):546–563. https://doi.org/10.1057/s41303-017-0066-x
Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355. https://doi.org/10.1287/isre.1040.0032
Mani Z, Chouk I (2017) Drivers of consumers' resistance to smart products. J Mark Manag 33(1–2):76–97. https://doi.org/10.1080/0267257X.2016.1245212
Marakas GM, Hornik S (1996) Passive resistance misuse: overt support and covert recalcitrance in IS implementation. Eur J Inf Syst 5(3):208–219. https://doi.org/10.1057/ejis.1996.26
Martin KD, Murphy PE (2017) The role of data privacy in marketing. J Acad Mark Sci 45:135–155. https://doi.org/10.1007/s11747-016-0495-4
Martinko MJ, Henry JW, Zmud RW (1996) An attributional explanation of individual resistance to the introduction of information technologies in the workplace. Behav Inf Technol 15(5):313–330. https://doi.org/10.1080/014492996120085a
Nahapiet J, Ghoshal S (1998) Social capital, intellectual capital, and the organizational advantage. Acad Manag Rev 23(2):242–266. https://doi.org/10.5465/amr.1998.533225
Newell S, Tansley C, Huang J (2004) Social capital and knowledge integration in an ERP project team: the importance of bridging and bonding. Br J Manag 15(S1):43–57. https://doi.org/10.1111/j.1467-8551.2004.00399.x
Norberg PA, Horne DR, Horne DA (2007) The privacy paradox: personal information disclosure intentions versus behavior. J Consum Affairs 41(1):100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
Nunnally J (1978) Psychometric theory, 2nd edn. McGraw-Hill, New York
Orlikowski WJ (1992) The duality of technology: rethinking the concept of technology in organizations. Org Sci 3(3):398–427. https://doi.org/10.1287/orsc.3.3.398
Ozdemir ZD, Smith HJ, Benamati JH (2017) Antecedents and outcomes of information privacy concerns in a peer context: an exploratory study. Eur J Inf Syst 26(6):642–660. https://doi.org/10.1057/s41303-017-0056-z
Pavlou PA (2011) State of the information privacy literature: where are we now and where should we go? MIS Q 35(4):977–988. https://doi.org/10.2307/41409969
Paxton P (1999) Is social capital declining in the United States? A multiple indicator assessment. Am J Sociol 105(1):88–127
Petronio S (2002) Boundaries of privacy: dialectics of disclosure. SUNY Press, New York
Podsakoff PM, Organ DW (1986) Self-reports in organizational research: problems and prospects. J Manag 12(4):531–544
Polanyi K (1957) The great transformation: the political and economic origins of our time. Beacon Press, Boston
Polites GL, Karahanna E (2013) The embeddedness of information systems habits in organizational and individual level routines: development and disruption. MIS Q 37(1):221–246. https://doi.org/10.25300/MISQ/2013/37.1.10
Punj GN (2019) Understanding individuals' intentions to limit online personal information disclosure to protect their privacy: implications for organizations and public policy. Inf Technol Manag 20(3):139–151. https://doi.org/10.1007/s10799-018-0295-2
Putnam RD (2000) Bowling alone: the collapse and revival of American community. Simon and Schuster, New York
Ram S, Sheth JN (1989) Consumer resistance to innovations: the marketing problem and its solution. J Consum Mark 6(2):5–14. https://doi.org/10.1108/EUM0000000002542
Raynes-Goldie K (2010) Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook. First Money. https://doi.org/10.5210/fm.v15i1.2775
Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. J Psychol 91(1):93–114. https://doi.org/10.1080/00223980.1975.9915803
Rust RT, Kannan PK, Peng N (2002) The customer economics of Internet privacy. J Acad Mark Sci 30(4):455–464

Samuelson W, Zeckhauser R (1988) Status quo bias in decision making. J Risk Uncertain 1(1):7–59. https://doi.org/10.1007/BF00055564
Schoenbachler DD, Gordon GL (2002) Trust and consumer willingness to provide information in database-driven relationship marketing. J Interact Mark 16(3):2–16. https://doi.org/10.1002/dir.10033
Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Q 35(4):989–1015. https://doi.org/10.2307/41409970
Smyth SM (2019) The Facebook conundrum: is it time to usher in a new era of regulation for big tech? Int J Cyber Criminol 13(2):578–595
Sraders A (2020) History of Facebook: facts and what's happening. The Street-Technology. https://www.thestreet.com/technology/history-of-facebook-14740346
Sutanto J, Palme E, Tan C-H, Phang CW (2013) Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Q 37(4):1141–1164. https://doi.org/10.25300/MISQ/2013/37.4.07
Sweat J (2000) Privacy paradox: customer want control and coupons. Information week, 781, April, 52
Szmigin I, Foxall G (1998) Three forms of innovation resistance: the case of retail payment methods. Technovation 18(6/7):459–468. https://doi.org/10.1016/S0166-4972(98)00030-3
Taylor SE, Sherman DK, Kim HS, Jarcho J, Takagi K, Dunagan MS (2004) Culture and social support: who seeks it and why? J Personal Soc Psychol 87(3):354–362. https://doi.org/10.1037/0022-3514.87.3.354
Thaler RH, Sunstein CR (2008) Nudge: improving decisions about health, wealth, and happiness. Yale University Press, London
Treacy S, Feller J, O'Flaherty B, Nagle T (2017) Competitive market innovation contests and social capital: diametrically opposed, or inherently linked? In: Proceedings of the 25th European conference on information systems (ECIS), Guimarães, Portugal, pp 1695–1712. http://aisel.aisnet.org/ecis2017_rp/109
Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The effect of online privacy information on purchasing behavior: an experimental study. Inf Syst Res 22(2):254–268. https://doi.org/10.1287/isre.1090.0260
Tsay-Vogel M, Shanahan J, Signorielli N (2018) Social media cultivating perceptions of privacy: a 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media Soc 20(1):141–161
Tucker C (2018) Network effects and market power: what have we learned in the last decade? Antitrust 32(2):72–79
Uzzi B (1997) Social structure and competition in interfirm networks: the paradox of embeddedness. Adm Sci Q 42(2):35–67. https://doi.org/10.2307/2393808
Valenzuela S, Park N, Kee KF (2009) Is there social capital in a social network site? Facebook use and college students' life satisfaction, trust, and participation. J Comput Mediat Commun 14:875–901. https://doi.org/10.1111/j.1083-6101.2009.01474.x
Wang T, Duong TD, Chen CC (2016) Intention to disclose personal information via mobile applications: a privacy calculus perspective. Int J Inf Manag 36(4):531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003
Warren SD, Brandeis LD (1890) The right to privacy. Harvard Law Rev 4(5):193–220
Wasko MM, Faraj S (2005) Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. MIS Q 29(1):35–57. https://doi.org/10.2307/25148667
Waters S, Ackerman J (2011) Exploring privacy management on Facebook: motivations and perceived consequences of voluntary disclosure. J Comput Mediat Commun 17(1):101–115. https://doi.org/10.1111/j.1083-6101.2011.01559.x
Westin A (1967) Privacy and freedom. Atheneum, New York
Wills TA (1991) Social support and interpersonal relationships. In: Clark MS (ed) Review of personality and social personality. Prosocial behavior, vol 12. Sage Publication, Thousand Oaks, pp 265–289
Witte K (1992) Putting the fear back into fear appeals: the extended parallel process model. Commun Monogr 59(4):329–349. https://doi.org/10.1080/03637759209376276
Woolcock M, Narayan D (2000) Social capital: implications for development theory, research, and policy. World Bank Res Obs 15(2):225–249
Xu H, Teo H-H, Tan BCY, Agarwal R (2009) The role of push-pull technology in privacy calculus: the case of location-based services. J Manag Inf Syst 26(3):135–173. https://doi.org/10.2753/MIS0742-1222260305
Xu H, Dinev T, Smith J, Hart P (2011a) Information privacy concerns: linking individual perceptions with institutional privacy assurances. J Assoc Inf Syst 12(12):798–824. https://doi.org/10.17705/1jais.00281

Xu H, Luo X, Carroll JM, Rosson MB (2011b) The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decis Support Syst 51(1):42–52. https://doi.org/10.1016/j.dss.2010.11.017

Yu L, Li H, He W, Wang F-K, Jiao S (2020) A meta-analysis to explore privacy cognition and information disclosure of internet users. Int J Inf Manag 51:102015. https://doi.org/10.1016/j.ijinfomgt.2019.09.011

Zlatolas LN, Welzer T, Heričko M, Hölbl M (2015) Privacy antecedents for SNS self-disclosure: the case of Facebook. Comput Hum Behav 45(C):158–167. https://doi.org/10.1016/j.chb.2014.12.012