Consumer Vulnerability: Understanding Transparency and Control in the Online Environment

Abstract

Purpose – In the online environment, consumers increasingly feel vulnerable due to firms' expanding capabilities of collecting and using their data in an unsanctioned manner. Drawing from gossip theory, this research focuses on two key suppressors of consumer vulnerability: transparency and control. Previous studies conceptualize transparency and control from rationalistic approaches that overlook individual experiences and present a unidimensional conceptualization. This research aims to understand how individuals interpret transparency and control concerning privacy vulnerability in the online environment. Additionally, it explores strategic approaches to communicating the value of transparency and control.

Design/methodology/approach – An interpretivism paradigm and phenomenology were adopted in the research design. Data were collected through semi-structured interviews with 41 participants, including consumers and experts, and analyzed through thematic analysis.

Findings – The findings identify key conceptual dimensions of transparency and control by adapting justice theory. They also reveal that firms can communicate assurance, functional, technical, and social values of transparency and control to address consumer vulnerability.

Originality – This research makes the following contributions to the data privacy literature. The findings exhibit multidimensional and comprehensive conceptualizations of transparency and control, including user, firm, and information perspectives. Additionally, the conceptual framework combines empirical insights from both experiencers and observers to offer an understanding of how transparency and control serve as justice mechanisms to effectively tackle the issue of unsanctioned transmission of personal information and subsequently address vulnerability. Lastly, the findings provide strategic approaches to communicating the value of transparency and control.

Keywords: Data Privacy, Consumer Vulnerability, Transparency, Control, Qualitative Research

Paper type: Research paper

1. Introduction

In the digital age, consumer vulnerability has become one of the most important topics in privacy research (Chen *et al.*, 2022; Cho, 2022; Hugl, 2011). Consumers face unsanctioned transmissions of their personal data, such as unauthorized data access, data breaches, and data misuse (Fox and James, 2021; Albashrawi and Motiwalla, 2019; Duan and Deng, 2022; Elhai *et al.*, 2017). For example, in 2023, Meta was found violating European Union (EU) data protection rules, was fined 1.2 billion euros, and was ordered to stop transferring data collected from Facebook users in the EU to the U.S. (Satariano, 2023). The Facebook–Cambridge Analytica data scandal in 2018 reveals that Facebook worked with third parties to influence voters in the U.S. by providing them with targeted information based on their demographic information and personality characteristics (Rosenberg *et al.*, 2018). In 2019, FaceApp was accused of sending users' photos to servers without their permission (Brewster, 2019). Similar incidents of unsanctioned transmission are becoming increasingly common, with more than 11 billion data breaches recorded worldwide since 2005 (Privacy Rights ClearingHouse, 2019). Such incidents raise consumers' privacy concerns and make them feel susceptible to being harmed in the online environment, leading to rising vulnerability (Muzatko and Bansal, 2023). To tackle consumer vulnerability under unsanctioned transmission of personal information, more and more firms are required to improve their data privacy practices. In the EU, the General Data Protection Regulation requires firms to provide transparent information and seek opt-in consent before data processing. Due to the significant policy changes, firms need to better understand how to manage the transmission of consumer personal information in a fair and just manner that helps mitigate consumer vulnerability.

In the data privacy literature, gossip theory is an emerging theoretical perspective (Martin *et al.*, 2017). This theory focuses on individual vulnerability that arises due to the unsanctioned transmission of personal information (i.e., gossip). It suggests that transparency and control are two crucial factors in mitigating vulnerability (Martin *et al.*, 2017). There is a need for greater conceptual clarity and consensus regarding the conceptualization of transparency and control due to the following reasons. First, previous studies mainly stem from rationalistic approaches that examine these two constructs as unidimensional with a singular focus on either user, firm, or information (e.g., Benlian and Hess, 2011; Dinev *et al.*, 2013; Esmaeilzadeh, 2020; Karwatzki *et al.*, 2017; Kim *et al.*, 2019). Exploring the meanings of these constructs in information transmissions between users and firms requires integrating angles from user, firm, and information. Additionally, prior studies empirically focus on consumers who directly engage with transparency and control mechanisms in an online environment, without considering the perspective of observers, including experts, researchers, policymakers, or external stakeholders (e.g., Hill and Sharma, 2020). Second, prior studies emphasize the significance of conveying privacy practices to address consumer vulnerability (Martin *et al.*, 2017). However, there is limited research on how to strategically communicate these practices, especially communicating the value of transparency and control underlying privacy practices.

To address the gaps, we propose the following two questions: (1) In the online environment, what do transparency and control mean in the context of consumer vulnerability? and (2) How do firms strategically communicate the value of transparency and control to address consumer vulnerability?

The remainder of this paper is organized as follows: We review the literature on consumer vulnerability and the key vulnerability suppressors (i.e., transparency and control). We then examine how previous studies conceptualize these constructs. Based on key insights, we conduct an exploratory qualitative study to identify the main dimensions of transparency and control and explore strategic approaches to communicating the value of these constructs. Finally, we conclude by presenting the theoretical contributions and practical implications of our findings followed by research limitations and directions for future research. Finally, the paper is summed up with the concluding remarks.

2. Theoretical background

In an online environment, firms expand their capability to collect and use consumer personal information to improve their marketing effectiveness. When the collection, use, or disclosure of consumers' personal information is unsanctioned and violates privacy boundaries, consumers are subject to potential privacy risks and thus feel vulnerable (Alemany *et al.*, 2021; Mpinganjira and Maduku, 2019; Cho, 2022). We draw from gossip theory, which provides insights into consumer vulnerability arising from the unsanctioned transmission of personal information. Based on this theory, we focus on reviewing the literature on two constructs, including transparency and control, which make the transmission of personal information in a just and fair manner. Finally, we review the literature on strategic communication about transparency and control in the context of privacy practice. The insights gathered from this section helped inform our main study.

2.1 Consumer vulnerability

In the consumer data privacy literature, vulnerability is a core concept describing how firms' data practices associated with the unsanctioned transmission of personal data influence consumer behavior (Janakiraman *et al.*, 2018). Our literature review summarizes the definitions and research contexts of consumer vulnerability (see Appendix A). It identifies the following interrelated characteristics of consumer vulnerability in an online environment. First, consumer vulnerability is a state of powerlessness with exposure to injury, harm, or attack (Fox and Hoy, 2019; Aguirre *et al.*, 2015). Second, consumer vulnerability is associated with rising privacy concerns when consumers engage in digital activities (Bleier and Eisenbeiss, 2015; Buglass *et al.*, 2016). Third, it involves consumers being subject to risks such as damage to their psychological and emotional state, reputation, and self-perception (Buglass *et al.*, 2016; Chen *et al.*, 2019; Dyussembayeva *et al.*, 2020; Martin and Murphy, 2017). Fourth, it occurs when consumers are not able to accomplish their goals in a consumption situation due to their powerless circumstances (Parkinson *et al.*, 2017). Fifth, it involves placing consumers in a disadvantaged position in marketplace interactions (Hill and Sharma, 2020; Kennedy *et al.*, 2019; Liyanaarachchi *et al.*, 2020). Sixth, as consumers have limited access to options and resources compared to firms, external forces that facilitate the establishment of fairness between consumers and firms can help address consumer vulnerability (O'Sullivan, 2015).

In the consumer data privacy literature, some recent studies suggest incorporating gossip theory into exploring consumers' perceptions of a firm's data privacy practices (Martin *et al.*, 2017; Chen *et al.*, 2023). Gossip broadly refers to evaluative communication that expresses the judgment of an absent third party, and, in the online environment, it refers to the unsanctioned transmission of consumer personal data (Martin *et al.*, 2017). Gossip theory provides valuable insights into consumers' responses to firms' practices of gathering and usage of consumer personal information as well as attempts to breach privacy boundaries (e.g., Martin *et al.*, 2017; Schlackl *et al.*, 2022).

Previous research suggests that gossip theory can be applied at individual, relational, and organizational levels (Wax *et al.*, 2022). At an individual level, it can be viewed to assess consumer responses such as feelings and cognitive evaluations (e.g., Chen *et al.*, 2023; Martin *et al.*, 2017; Leary and Leder, 2009). At the relational level, it can be viewed to explore the quality of interpersonal relationships such as relationships between leaders and subordinates (Cheng *et al.*, 2022). At the firm level, gossip theory can be used to help assess stock price and organization revenues (e.g., Fang *et al.*, 2023; Martin *et al.*, 2017). By applying gossip theory in an online environment, prior studies suggest that after consumers disclose their personal information to firms (Lwin *et al.*, 2016), they surrender their direct control over their personal information and thus feel vulnerable to becoming a gossip target of data breaches and unauthorized data access (Aiello *et al.*, 2020; Martin *et al.*, 2017).

While gossip theory provides insights into individuals' responses (e.g., vulnerability) to firms' privacy policies and practices (e.g., transparency and control) of gathering and usage of their personal information, it does not explain the underlying mechanisms regarding how and why individuals develop such responses. As suggested by a recent study in data privacy (Steinhoff and Martin, 2023), our present study argues that individuals' interpretations of whether firms' privacy policies and practices are just, and fair can serve as the underlying mechanisms of their response formation. Specifically, this study argues that key characteristics of firms' privacy policies and practices (i.e., transparency and control) are conceptualized as justice mechanisms (just and fair procedure of data collection, allocation, and interactive exchange) to address gossip (i.e., unsanctioned transmission of personal information) and thus mitigate the key negative outcome of gossip, consumer vulnerability.

2.2 Consumer vulnerability key suppressors: Transparency and control

According to gossip theory, consumer vulnerability in an online environment can be mitigated by two key factors: transparency and control (Martin *et al.*, 2017). Transparency refers to consumers having information about the nature and scope of the data held by the firm and understanding how these data are utilized (Emler, 1994). Firms ensure transparency via a privacy policy or information collection disclosure statements (e.g., terms and conditions) (Martin *et al.*, 2017). Control means the extent to which consumers can manage the flow of their information (Emler, 1994). Providing such control enables consumers to manage their preferences and permission as to how the firm handles their data (Kumar *et al.*, 2014). Transparency and control collectively mitigate consumer vulnerability and further mitigate consumers' negative behavioral responses, such as negative word-of-mouth and intention to switch to other firms (Martin *et al.*, 2017).

To provide a comprehensive understanding of transparency and control, we reviewed the literature on marketing, management, and information management and summarized their conceptualizations (see Appendix B). Our literature review yields two main insights that can be applied to advance the knowledge of transparency and control. First, the exploration of transparency and control needs to be expanded beyond rationalistic approaches. Second, it is necessary to empirically explore both experiencer and observer perspectives, which provide a comprehensive understanding of individuals' vulnerable experiences concerning transparency and control. Transparency and control are elucidated in a detailed review below.

Transparency and control have been explored through rationalistic approaches stemming from quantitative methods. Specifically, research on transparency can be distinguished into three streams of information exchanges: *user-focused*, *firm-focused,* and *information-focused* (see Appendix B). *User-focused* research investigates transparency as *users'* beliefs about information related to privacy policy (e.g., Esmaeilzadeh, 2020). *Information-focused* research explores the selective exchange of sensitive information between users and firms, including disclosure, data collection, usage, distribution, and information related to the privacy policy (e.g., Benlian and Hess, 2011; Dinev *et al.*, 2013). Within the *firm-focused* stream, scholars examine a firm's ability to inform users, disclose information, and provide options (e.g., Kim *et al.*, 2019; Karwatzki *et al.*, 2017).

Previous studies about control can be distinguished as *user-focused* and *firm-focused* (see Appendix B). Within the *user-focused* stream, control primarily refers to *users'* feelings and cognition (e.g., beliefs, perceptions, judgment) regarding: users (self), privacy risk, personal information disclosure, and external interactions (e.g., Zhang *et al.*, 2017; Morimoto, 2021; Markos *et al.*, 2017; Punj, 2019; Zhao *et al.*, 2012; Dinev *et al.*, 2013; Xu *et al.*, 2012; Taylor *et al.*, 2009; Mothersbaugh *et al.*, 2012; James *et al.*, 2016; Hong and Thong, 2013; Wang, 2019). Within the *firm-focused* stream (e.g., Weydert *et al.*, 2020; Tucker, 2014; Suh and Han, 2003; Song *et al.*, 2016; Malhotra *et al.*, 2004; Ray *et al.*, 2011), control reflects the firm's ability (functions/features) to manage to whom data are sold, what is done with the data, and how users' perception of their social control and information control can be enhanced (e.g., Weydert *et al.*, 2020; Tucker, 2014; Suh and Han, 2003; Song *et al.*, 2016; Malhotra *et al.*, 2004; Ray *et al.*, 2011).

Among the above research streams adopting rationalistic approaches, scholars view transparency and control with a singular focus on either user, firm, or information perspective. Despite facilitating rationalistic operationalizations into quantitative measures, this singular focus often results in overly narrow and unidimensional descriptions that may not adequately represent the complexity of transparency and control. Moreover, researchers have suggested that individuals' interpretation of the constructs of transparency and control depends on their experiences and social contexts (Xu *et al.*, 2011). Therefore, as an alternative to the rationalistic approaches that overlook subjective interpretations, within the interpretive paradigm, the study embraced a phenomenological approach. A key feature of phenomenology is exploring concepts as lived experiences of participants which uncovers deeper insights into human experiences and their underlying meaning (Berger and Luckmann, 1967).

Additionally, previous studies mainly empirically view control and transparency from an experiencer's perspective, with a primary focus on vulnerability that individuals identify, feel, and experience (e.g., Taylor *et al.*, 2009; Zhang *et al.*, 2017; Hong and Thong, 2013; Dinev *et al.*, 2013; Zhao *et al.*, 2012; Wang, 2019; Punj, 2019; Hajli and Lin, 2016; Ray *et al.*, 2011; Markos *et al.*, 2017; Morimoto, 2021; Song *et al.*, 2016; Suh and Han, 2003; Tucker, 2014; Xu *et al.*, 2012). The experiencer perspective refers to individuals who directly engage in transparency and control mechanisms in an online environment. It exhibits a user's experiential and subjective viewpoint, intentions, cognitions, behaviors, and interaction with such mechanisms. Importantly, the literature review exhibits that limited research about transparency and control focuses on the perspective of observers (see Appendix B). The observer perspective involves experts, researchers, policymakers, or external stakeholders who undertake an objective and external point of view which allows for an assessment of the effectiveness, ethical considerations, and broader implications of these mechanisms (Hill and Sharma, 2020; Baker *et al.*, 2005). Additionally, the observer perspective provides valuable insights because they focus on the full experience of experiencers and are aware of experiencers' behaviors in their social contexts (Baker *et al.*, 2005; Baker *et al.*, 2007).

Experiencer and observer perspectives reveal different ways in which individuals experience transparency and control, with varying intensities of these constructs related to vulnerability. Scholars could more fully understand these constructs by empirically evaluating both experiencers and observers, rather than just one perspective in isolation (Hill and Sharma, 2020). Thus, it is imperative to incorporate both experiencer and observer perspectives as they provide empirically distinct viewpoints that contribute to a comprehensive understanding of the two constructs aiding theory development.

2.3 Strategically communicating the value of transparency and control

Firms need to provide explanations and justifications for their privacy practices to consumers when collecting data from them (Hui *et al.*, 2007; Pollach, 2005). Gossip theory acknowledges that communication is an important aspect of information exchange (Martin *et al.*, 2017). From a communication perspective, firms should first examine what consumers value and then communicate this value to them to make them feel less vulnerable (Norberg and Horne, 2014). Based on this notion, the present study argues that communicating the value of privacy practices can effectively mitigate consumer vulnerability. However, there is limited research investigating how to communicate the value of transparency and control to make consumers feel less vulnerable. We aim to fill this gap through our research.

To summarize, drawing on insights from gossip theory, this study aims to explore two key suppressors of consumer vulnerability, namely transparency and control. It aims to advance the conceptualization of transparency and control by adopting phenomenology (interpretative approach) as an alternative to rationalistic approaches and incorporating the experiencer and observer perspectives empirically. This study also aims to offer insights into the strategic communication of the value of transparency and control as a means to address consumer vulnerability.

3. Methodology

The main objective of this study is to explore the role of transparency and control in understanding consumer vulnerability in an online environment. Specifically, it addresses two research questions: 1) *In the online environment, what do transparency and control mean in the context of consumer vulnerability?* and 2) *How do firms strategically communicate the value of transparency and control to address consumer vulnerability?* To discuss the findings, the study adopts a justice theory perspective to gather deep insights into individuals' interpretations of transparency and control. Justice theory provides a comprehensive framework for understanding justice, fairness, and equity to mitigate consumer vulnerability in consumer online interactions (Ashworth and Free, 2006; Bies, 2001). Specifically, by focusing on the online context, this study explores how individuals interpret the meaning of transparency and control, using just and equitable mechanisms for addressing the unauthorized transmission of personal data and mitigating consumer vulnerability.

Within the interpretive paradigm, the study embraces a phenomenological approach that views reality as socially constructed. The meaning of reality is derived from participants' experiences (Sandberg, 2005). In adopting this approach, researchers are exposed to the complex lived experiences and perceptions of participants (Creswell, 2014). This study argues that the meanings of transparency and control are subjective and depend on participants' experiences of privacy practices. The phenomenological approach lets us explore the lived experiences of individuals in their role as either consumers or experts and allows a conceptual framework to emerge from participants' combined experiences (Locke, 2007).

The study recruited 41 participants including 24 consumers and 17 experts. The consumers were experiencers with knowledge and experience of the online environment. They had various professions, such as human resource administrator, academic director, entertainment manager, and students. The experts were observers with professions such as CEO, cybersecurity officer, cybersecurity consultant, and consumer researcher (see Appendix C for the participants' profiles). The participants were from Australia, New Zealand, the United Kingdom, the United States, and China.

The data collection process used purposive sampling and we followed protocols from Kvale (1983) to design semi-structured interviews (see Appendix D for the interview guide). Firstly, the interviews were audio-recorded and transcribed verbatim with consent from participants. To ensure communicative validity (Kvale, 1995; Sandberg, 2005), the interviewers explained the research theme to the participants. Secondly, the interviewers ensured that participants were comfortable with the setting and made the interview conversation-like and informal. Thirdly, the interviews were kept open-ended, and the interviewers asked participants to share their lived experiences. The interview duration ranged from approximately half an hour to one and a half hours. Reliability as interpretative awareness was achieved by ensuring that all aspects of participants' experiences were deemed equally important during the data collection and analysis phases (Kvale, 1995; Sandberg, 2005). The data analysis involved using online software (Otter.ai) that helps transcribe recorded speech-to-text transcription. Three researchers share the interview notes, and they capture, organize, and control the complexity of the participants' lived experiences. To ensure participant anonymity, names and identifying features of individuals, companies, products, and other related terms have been changed.

To analyze the data, the study used thematic analysis (Braun and Clarke, 2006). We then followed open coding through which we identified all statements about participants' interpretation of transparency, control, and data privacy practice/policy that makes participants feel less (or more) vulnerable (see Appendix E). To analyze the data from interviews, three researchers coded the key themes independently. To attain analyst triangulation, the data analysis involved first-order, second-order, and third-order codes. The emerging themes were analyzed using a set of guidelines from Groenewald (2004). Later, three researchers assessed the data quality to identify if there were overlaps in the codes. In this step, 26 first-order codes and 9 second-order codes were identified about transparency (see Appendix E). Similarly, 28 first-order codes and 6 second-order codes were identified about control (see Appendix F), and 25 first-order codes and 7 second-order codes were identified about strategies (see Appendix G). Through an iterative process of refinement and reformulation of re-reading interviews and retracing the literature, third-order themes were developed (Hycner, 1985). The final form of triangulation involved bridging the gap between empirical data and theory. By adapting the bricolage approach to conceptual leaping, the researchers engaged in a continual iterative process, moving between empirical data and justice theory, linking how consumers perceive a firm's transparency and control practices as fair or unfair. Aligning with the approach advocated by Lofland and Lofland (1995), the analysis granted a slight preference to the empirical data. As advised by Pratt (2009), in the analysis phase, the researchers remained conscientious about steering clear of two common pitfalls: presenting data without sufficient context and disclosing an excess of data without comprehensive interpretation.

4. Findings

The findings reveal how participants interpret transparency and control that construct a fair and just mechanism of information transmission, which impacts consumer vulnerability in an online environment. The conceptual dimensions of transparency and control are presented in Appendix E and Appendix F respectively. The findings also provide insight into strategically communicating the value of transparency and control to address consumer vulnerability (key codes and themes are summarized in Appendix G). The following sub-sections explain each conceptual dimension of transparency and control and present strategic approaches to communicate their value.

4.1 Transparency

The findings suggest that participants' interpretation of transparency regarding firms' privacy practices is not limited to the information shared with them but also encompasses how firms communicate the information and whether the communication is clear and reliable. Based on the analysis, three conceptual dimensions of transparency are identified, including integrity, understandability, and proactivity.

Integrity. The findings reveal that participants interpret transparency as the way firms maintain the integrity of their information. Their interpretations focus on whether the information provided is valid, reliable, complete, and relevant about how data are collected, stored, and used to profile and target consumers. One participant stated, "The bare minimum would be to give [*consumers*] proper and accurate records for data subject requests" (Participant No. 26). Some other participants suggested that firms do not provide relevant information, which makes them feel vulnerable. Firms could take a more transparent approach to provide users with relevant information regarding their data. Further relevant insights were provided by participants: "Transparency will be like this…They [*firms*] tell us which data is being stored and which is not" (Participant No. 25); "I cannot see in what way they [*firms*] register my behavior online" (Participant No. 24). This dimension of transparency reflects how consumers perceive the quality of the information they receive about the management of their data (Awad and Krishnan, 2006).

Understandability. The findings show that participants interpret transparency as the understandability of how firms communicate with them. This interpretation focuses on open, upfront, and clear interaction between firms and users. Understandable, upfront, and open communication can mitigate an individual's vulnerability (Mazurek and Małagocka, 2019; Hansson *et al.*, 2020). One reason is that consumers develop a positive expectation of fairness through a firm's communication (Seiders and Berry, 1998). For example, a participant said, "You know, they [*firms*] wouldn't be transparent if they weren't upfront about the fact that they are going to use your data" (Participant No. 03). Another participant shared their view on how firms should be clear in their communication with users. For example, if data are shared with third parties, firms should explicitly communicate this practice to users. Users feel vulnerable when they cannot understand the provided information easily. On the same theme, one participant stated, "I don't understand the privacy policies around it!" (Participant No. 21). Another participant explained, "I feel that, in the future, whoever is using my data should tell me that where is the tree [*diagram*] – where this is going [*data flow*]?" (Participant No. 13). Similarly, another participant shared that firms should be open in their communication, "Rather than hiding it [*their data practice*], they need to say it outright" (Participant No. 01). This dimension of transparency reflects the way consumers interpret how firms foster adequate and open communication with them (Bies, 2001), thus making them feel less vulnerable.

Proactivity. The findings also show how participants interpret transparency as proactivity in firms' data management practices. Participants suggested that if firms send timely reminder messages, inform users of policy updates or changes, and actively seek consent, they would perceive that such practices convey transparency. Proactivity in a firm's management can be viewed as a process applied to any set of actions through anticipating, planning, and striving to have an impact (Grant and Ashford, 2008). An individual's judgment of perceived justice can be enhanced through proactive privacy intervention strategies (Zhao *et al.*, 2012). Individuals tend to judge a firm through such proactive privacy practices and evaluate if the firm would safeguard their interests (Larsen and Lawson, 2013). For example, a participant mentioned that if there is a policy change or update, the firm should proactively remind users of any changes. Another participant shared, "Reminding you when it comes up and it says, we're using cookies, you are acknowledging the use of cookies, that sort of reminds you…that's transparency" (Participant No. 21). On the same theme, one participant explained that firms that seek consent proactively rather than hiding their data collection practices would gain consumers' trust and make consumers feel less vulnerable. Another participant stated, "They [*firms*] are not allowing transparency about the data they are capturing through your device… whatever you have in cache. Though I give up my information personally, it [*firm*] is not asking my consent for sharing the information [with third parties]" (Participant No. 17). Firms should actively inform users if their data are being used or sold to third parties. Consumers shared that firms adopting such proactive practices convey that they value and respect users' privacy, thus making users feel less vulnerable.

4.2 Control

The findings suggest that the ways participants interpret control are not restricted to technical and operational control but also include data governance control. Three conceptual dimensions of control are identified, including autonomy, easiness, and agency.

Autonomy. The findings exhibit how participants interpret control as *autonomy* over a firm's data governance, responsibility, data ownership, comprehension of privacy rights, and data management practices, such as data policies, standards, and procedures. The autonomy of data governance reflects how a firm provides consumers the ability to make decisions on their own and act on choices that are free from external influences (Wertenbroch *et al.*, 2020). Participants discussed how individuals should be responsible and in control of their data rights. Participants also shared different expectations of who they consider to be responsible for their data. A few participants stated that users should be held responsible because they input the data: "We're responsible because we choose to give our data up sometimes" (Participant No. 21). A few others asserted that firms should be held responsible and accountable because they collect and store consumer data. Several participants explained the dual responsibility of both users and firms because users input their information and firms store it. The remainder contended that governments or law enforcement agencies should hold private firms responsible and accountable. When describing the experience of using a social media website, one participant explained, "This company is a private company…so it is responsible for its user data…if the user data [*are*] hacked by hackers, then it [*this problem*] is a police matter" (Participant No. 04).

Easiness. Another component through which participants interpret control is related to their interactions with firm-provided platforms, particularly the *easiness* of managing control settings and options. Specifically, participants focus on evaluating whether a firm offers clear and simplified operational controls (e.g., turn off all control options in privacy settings with a single click) when they interact with its platforms. Easiness also includes whether user-friendly default settings and explicit consent provisions are available to consumers. One participant suggested that the easiness of the control settings matters when using social media platforms. Another explained that he sometimes must turn off the privacy settings while browsing online because such settings are turned on by default: "It [*privacy setting*] should be something that you can turn on [*when you need it*] rather than something you need to turn off to protect privacy. It shouldn't be active right now." (Participant No. 01).

Agency. Participants interpret control as having *agency* over technical control. The technical control mechanisms are the data privacy options controlled by firms to manage consumer information, such as data removal and data access under legal requirements (e.g., the California Consumer Privacy Act and European General Data Protection Regulation). The agency on technical control reflects if firms allow consumers to manage their information independently (Kupfer, 1987; Stoneburner *et al.*, 2002). The findings suggest that participants conceptualized data removal and data access as a form of technical control provided by firms. Consistent with the findings from prior research (Smith and Cooper-Martin, 1997; Martin *et al.*, 2017), we show that consumers' vulnerability decreases when they can control or manage the impact of their information transmission.

4.3 Communicating the value of transparency and control

The findings elucidate strategies for firms to communicate the value of transparency and control in addressing consumer vulnerability. Specifically, our findings reveal several types of value: assurance value, delivered through government/regulator enforcement of data privacy and protection laws, firms' compliance with industry-specific data auditing, and firms' adherence to best practices; technical value, provided through hardware and physical security controls and firms' internal control management; social value, conveyed through ethical competence, impact on consumer well-being, and internal and external communication; and functional value, delivered through personalization.

Assurance value. Participants explained how firms should assure consumers that they follow rules and regulations set by the government, regulatory bodies, or industry. Such assurance signals that the overall ecosystem is regulated. Furthermore, the government should intervene to enforce privacy laws and eliminate grey areas. For example, one participant stated that while data privacy laws require adequate security control, firms differ considerably in their interpretation of "adequate". Furthermore, firms should comply with industry-specific data auditing and follow best practices. The expert participants explained that firms should assure consumers that they comply with privacy laws and industry policies. Firms should also provide assurance that they apply industry-leading data privacy practices and security recommendations to protect consumers from privacy risks (Lwin *et al.*, 2016). One participant (CEO) stated, "We assure consumers that we use the best practices and we 100% adhere to regulatory guidelines" (Participant No. 03).

Technical value. The findings show that firms should emphasize technical value, including the strengths of their relevant techniques, systems, and processes of transparency and control. This technical value could be communicated by strengthening firms' hardware and physical security controls and their internal data management system. Such data security infrastructure in firms helps protect consumer privacy and mitigate vulnerability. Physical controls include using encrypted hardware, denying access to laptops, confidentiality agreements, and confidentiality systems. A participant explained that, while logging into a specific website, the website verifies the account based on the device in use. This data security practice makes him feel more secure. He elaborated, "When you're logging in from a particular device, the device recognition [or authentication] feature is very useful. [This] cybersecurity [feature], or any system perhaps, captures your information, logs it properly, and then checks for your device history [to verify you]. It's a good feature to have, and I feel secure whenever I see this feature is enabled" (Participant No. 11).

Social value. The findings also reveal that firms should emphasize social values, including ethics and care about consumers. Participants expressed their concerns that firms may be involved in practices that are legal but not necessarily ethical. They emphasized that firms should adopt ethical practices and demonstrate responsibility regarding consumer well-being. One participant said, "Firms should be mindful about the impact they can create on the mental well-being of people" (Participant No. 09). One participant explained, "If you are not taking your customers along with you, that’s not a good practice at all. At this moment in time, people are very much concerned about their personal information, personal preferences, etc.” (Participant No. 02).

Functional value. Finally, the findings show that firms can communicate the benefits of personalization as functional value. Participants stated that they receive benefits from personalized marketing services that match their preferences. Thus, when firms learn about consumers by collecting and using consumer data, they can more effectively provide services or promotional messages of interest to consumers. One participant suggested a key benefit of collecting personal information: “[*Firms*] personalize it [their products or services] and give you something that you kind of have in your head” (Participant No. 14). To summarize, the findings identify the ways to conceptualize transparency and control and reveal ways in which firms can communicate the value of transparency and control to address and mitigate consumer vulnerability.

5. Discussion

When discussing the findings, the study adapts justice theory as it provides a valuable lens to view the way consumers perceive fair information practices and explain the observed themes (Ashworth and Free, 2006; Bies, 2001). Specifically, as summarized in Table I, justice theory helps to link how consumers perceive a firm’s practices regarding transparency and control as fair or unfair through informational, distributive, procedural, and interactional dimensions (Culnan and Bies, 2003).

Justice theory suggests that three broad psychological processes underlie justice judgments, including distributive justice, procedural justice, and interactional justice (Cohen-Charash and Spector, 2001). Procedural justice concerns firms’ privacy policies regarding the processes and procedures of information transmission and consumers’ interpretation of them. Distributive justice concerns the trade-off consumers make in terms of the benefits they receive as they provide their personal information while risking privacy. Lastly, interactional justice concerns the fairness of interpersonal treatment and communication in online interactions (Martin and Murphy, 2017). The key linkage between gossip theory and justice theory lies in understanding how the spread of information (gossip) intersects with an individual's notions of fairness, equity, and justice in a firm's data privacy practices. Furthermore, when interpreting the findings, we empirically incorporate both experiencer and observer perspectives to help ensure a comprehensive and holistic understanding of both transparency and control to address the complexity of these concepts in the online context. The observers provided an external and analytical stance whereas the experiencer provided an internal and experiential stance.

Regarding *transparency,* the information justice dimension of consumers' interpretation is exhibited in how consumers perceive the integrity of the information they receive about the management of their data (Ellis *et al.*, 2009; Awad and Krishnan, 2006). If consumers judge such information shared by a firm as trustworthy (Lwin et al., 2016), it may contribute to a more equitable distribution of knowledge to understand how decisions on personal data are made, which would lessen their vulnerability (Mills and Krantz, 1979). Previous studies have found that if consumers experience covert information collection even when it is just for personalization, they are likely to feel vulnerable (Aguirre *et al.*, 2015; Taylor *et al.*, 2009). Similarly, understandable communication as a conceptual dimension of transparency aligns with interpersonal justice in which consumers judge the fairness of a firm's practice through the interpersonal communication they receive (Scott *et al.*, 2009; Greenberg, 1993). Such understandable interaction and communication may mitigate consumers' vulnerability (Mazurek and Małagocka, 2019; Hansson *et al.*, 2020) and contribute to building their trust (Colquitt and Rodell, 2011). Furthermore, proactivity as a conceptual dimension of transparency aligns with procedural justice in which the consumers interpret fairness in a firm's privacy processes and procedures (Ellis *et al.*, 2009; Martin and Murphy, 2017). Our findings align with previous research which shows that firms' proactive data management approaches mitigate consumers' privacy concerns and vulnerability (Martin and Murphy, 2017). If firms proactively adopt such practices, it may help reconcile and rebuild consumer trust in situations where data misuse or data breaches have occurred.

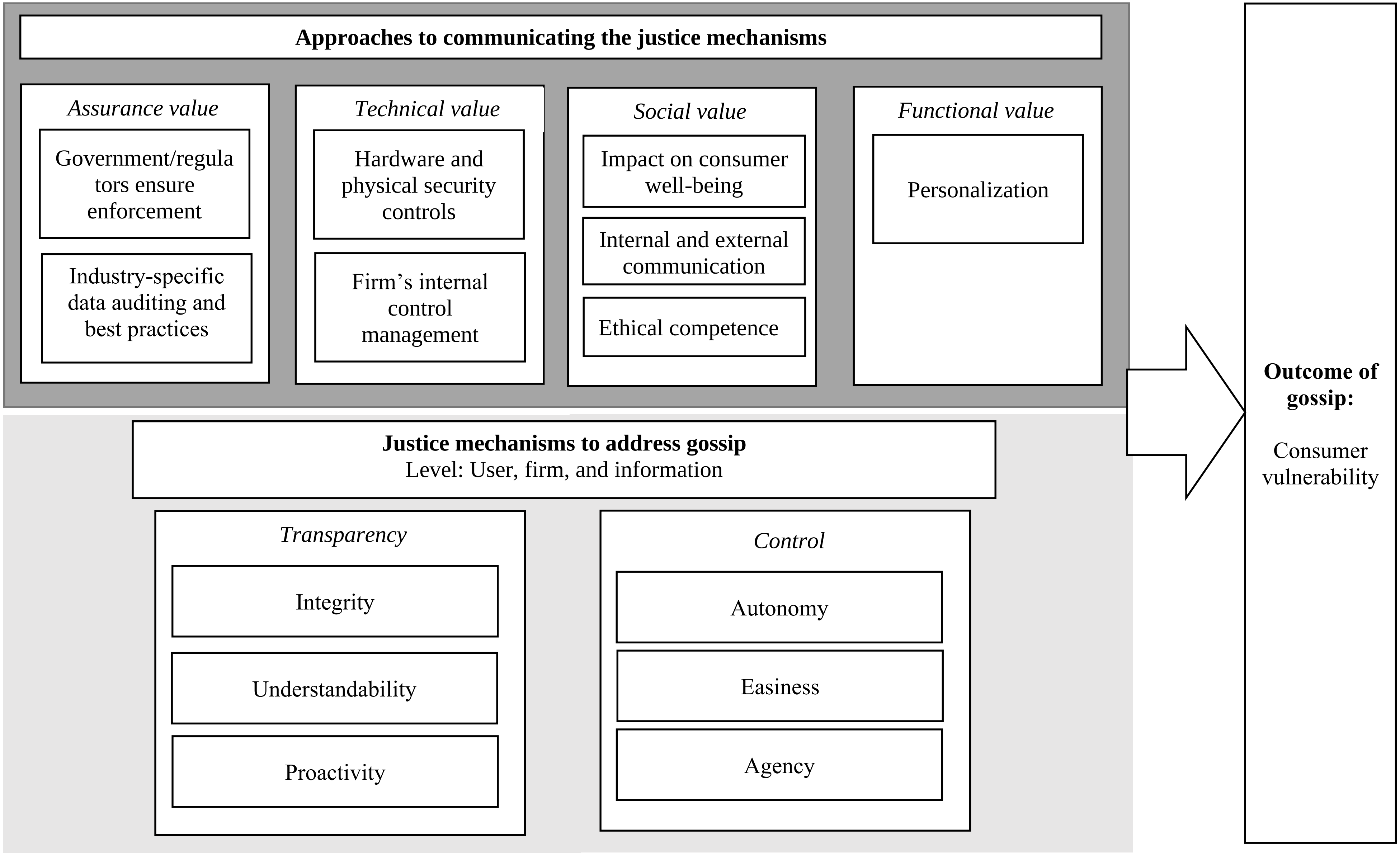
Regarding *control,* the autonomy dimension of control aligns with distributive justice, which concerns individuals' judgments of the distribution of inputs (e.g., information rights, ownership, and responsibility of data) with the firm's outputs (e.g., personalization, free services, and financial compensations) (Heeks and Renken, 2018; Martin and Murphy, 2017; Seiders and Berry, 1998). Our findings note a parallel privacy paradox: even though consumers value these outputs (e.g., personalization) provided by firms (Awad and Krishnan, 2006), they believe that the autonomy to control their data-related rights, ownership, and accountability should belong to consumers. If firms provide consumers autonomy over the governance of their data, it may demonstrate their willingness to safeguard consumer rights. Furthermore, the agency dimension of technical control aligns with the information justice dimension, which involves providing information about technical control measures to consumers and informing them of data collection, access, and removal (Konovsky, 2000; Thibaut and Walker, 1978). Previous studies indicate that when users' requests to manage their information are declined, they tend to develop unfavorable attitudes and behaviors (Ashworth and Free, 2006). Our findings suggest that consumers view information about such policies as representations of firms' information justice (Vail *et al.*, 2008). If firms provide agency over the technical adoption of such practices, they may help protect consumers' interests and thus contribute to firms' reputations. Lastly, easiness as a conceptual dimension of control aligns with interactional justice, which reflects the judgment consumers make regarding the fair treatment they receive during an exchange with a firm (Whitman *et al.*, 2012). The findings suggest that the interactions between firms and consumers are exhibited through the online control options provided to consumers. Prior research has found that consumers respond more favorably when they can control their privacy settings (Tucker, 2014; Bies, 2001). If firms provide easy-to-manage operational controls, it helps empower consumers to make decisions that directly mitigate their vulnerability.

Table I. Conceptual dimensions, definitions, and examples of transparency and control in data management practice

Construct	Conceptual Dimensions	Definition	Examples
Transparency	*Integrity* of information (informational)	Individual interpretation of data management practices is based on whether the information is truthful, complete, and reliable.	Information shared with users is valid, reliable, relevant, and complete. It informs users of data management processes such as accurate records of data collected, data resold, recorded history, and cookie usage.
	Understandability in communication (user interaction)	Individual interpretation of whether the communication of data management is open and clear.	Information about privacy laws, terms and conditions, and data sharing/usage is easy for users to understand.
	Proactivity in data management practices (firm)	Individual interpretation of whether the firm takes the initiative to inform users of their data management and relevant changes.	Firms seek permission, send reminder messages of data collection, and inform consumers about changes in policies or procedures.
Control	*Autonomy* of data governance (firm)	Individual interpretation of whether the firm provides them distributive autonomy over data-related rights, responsibility, ownership, and accountability.	Firms provide autonomy to consumers to let them be aware of who owns the rights to control data, who is responsible for handling data, and who is accountable for data-related issues.
	Easiness of operational control (user interaction)	Individual interpretation of whether interaction on a firm's platform provides data privacy options that are easy to manage.	When users interact with a firm's platform, they are provided with flexible control options and authorization options (e.g., control settings such as personalized ads are turned off by default or completely turned off through a single click).
	Agency over technical control (information)	Individual interpretation of whether the firm allows them to manage their information independently.	Consumers are offered information about control options to access, manage, and remove their data.

Our findings show that firms should communicate the *assurance, technical, social,* and *functional* values of transparency and control. The *assurance value* emphasizes communicating that privacy-related rules and regulations set by the government or industry are being followed by firms. Such communication involves a firm's focus on safety and responsibility for avoiding privacy risks, which can help gain consumer confidence and trust (Hui *et al.*, 2007). The *technical value* involves communicating the utilities of technical advances and procedures in transparency and control. Such technical value impacts organizational performance (Melville *et al.*, 2004) and has great potential to mitigate consumer vulnerability (Wünderlich *et al.*, 2020). The *social value* emphasizes the ethics and care demonstrated through transparency and control. The ethical and social values of a firm reflect its motives and characteristics, such as altruism, benevolence, and sincerity, that contribute to earning consumers' trust and mitigating their vulnerability (Fan, 2005). Finally, the *functional value* emphasizes communicating the benefits of using consumers' data to meet their needs and preferences. Such benefits in terms of personalized services can significantly overshadow consumers' perception of privacy risk and feelings of vulnerability (Awad and Krishnan, 2006). The study presents the conceptual framework in Figure 1.

Figure 1. Conceptual framework


Approaches to communicating the justice mechanisms
Assurance value
Government/regulators ensure enforcement
Industry-specific data auditing and best practices
Technical value
Hardware and physical security controls
Firm's internal control management
Social value
Impact on consumer well-being
Internal and external communication
Ethical competence
Functional value
Personalization
Justice mechanisms to address gossip
Level: User, firm, and information
Transparency
Integrity
Understandability
Proactivity
Control
Autonomy
Easiness
Agency
Outcome of gossip:
Consumer vulnerability

5.1. Theoretical contributions

In the data privacy literature, gossip theory suggests that consumer vulnerability in the online environment is mitigated by two key suppressors, including transparency and control (Martin *et al.*, 2017). Built on this theory, our study makes two contributions. First, prior studies on transparency and control have a singular focus on either user, firm, or information perspective based on rationalistic approaches (e.g., Benlian and Hess, 2011; Dinev *et al.*, 2013; Esmaeilzadeh, 2020; Karwatzki *et al.*, 2017; Kim *et al.*, 2019). In gossip theory, gossip is associated with how the information flows from the gossip target to other parties; therefore, exploring the meanings of gossip suppressors, transparency and control, requires integrating perspectives from users, information, and firms rather than looking using a singular perspective. Such integration helps identify the conceptual dimensions to better understand these concepts in data privacy literature as it explores their breadth and facilitates the development of valid measurements for future research. The findings exhibit multidimensional and comprehensive conceptual dimensions. For example, our conceptualization of transparency focuses on informational (integrity of information), user interaction (understandability in communication), and firm (proactivity in data management practices), while our conceptualization of control focuses on user interaction (easiness of operational control), firm (autonomy of data governance), and information (agency over technical control). Additionally, past research on transparency and control is dominated by undertaking the experiencer perspective (e.g., Taylor *et al.*, 2009; Zhang *et al.*, 2017; Hong and Thong, 2013; Dinev *et al.*, 2013; Zhao *et al.*, 2012; Wang, 2019; Punj, 2019; Hajli and Lin, 2016; Ray *et al.*, 2011; Markos *et al.*, 2017; Morimoto, 2021; Song *et al.*, 2016; Suh and Han, 2003; Tucker, 2014; Xu *et al.*, 2012; Benlian and Hess, 2011; Kim *et al.*, 2019; Esmaeilzadeh, 2020; Xu *et al.*, 2011; Karwatzki *et al.*, 2017; Betzing *et al.*, 2020). Our study empirically incorporates insights from both experiencers and observers to offer a more comprehensive understanding of vulnerability. Specifically, our conceptual framework provides an understanding of how transparency and control serve as justice mechanisms to effectively tackle the issue of gossip and subsequently mitigate vulnerability.

Second, though many studies highlight the importance of communicating privacy practices to mitigate consumer vulnerability, very little attention is given to how to communicate the value of transparency and control. This study offers novel theoretical insights into how to strategically communicate the value of transparency and control. Specifically, our findings show that firms should communicate the *assurance*, *technical*, *social*, and *functional* values of transparency and control. The literature acknowledges that communication is an important aspect of gossip theory (Martin *et al.*, 2017). Gossip theorists suggest that communication enables the exchange of information within social networks (Dunbar, 2004). Thus, exploring what consumers value and then conveying such values extends the utility of gossip theory by applying it in the online environment (Norberg and Horne, 2014).

5.2. Managerial implications

Our findings have important implications that help firms mitigate consumer vulnerability through managing transparency and control in their data privacy practices and communicating the value of transparency and control. First, our findings suggest that firms should undertake measures related to transparency and control to mitigate consumers' vulnerability at every stage of their experience (e.g., registration, usage, and offline). For example, Twitter has an automatic pop-up window that allows consumers to easily manage their privacy settings when registering, and Google sends reminders of privacy updates and changes to existing users.

Second, our findings demonstrate that transparency and control are subjective to consumers and depend on their interpretations and experiences. To positively shape consumer interpretation and improve their experience, our study suggests that firms should make control settings easy to manage and make consumers aware of their data-related rights and responsibilities. For example, under the General Data Protection Regulation, firms should provide consumers the “right to be forgotten” (or “right to erasure”) and allow them to request for removal of their personal data. In addition, firms should take responsibility for ensuring that consumers are aware of such rights.

Third, firms should deliver simple, clear, and relevant information about their privacy policies. Many firms have extremely lengthy and complex privacy terms and conditions (Wirth *et al.*, 2022), which undermine consumers’ perceptions of transparency. For example, it is estimated that the combined privacy terms and conditions of the 13 most popular apps take users over 17 hours to read (Kleinman, 2020). Thus, firms should demonstrate transparency by improving the understandability of privacy policies. For example, WhatsApp uses non-technical words and short highlights with illustrations on its data security information pages.

Finally, firms should communicate the benefits of their privacy practices and clarify how consumer data are used to meet consumers’ needs and preferences. Such benefits, in terms of personalized services, can significantly outweigh consumers’ perceived privacy risks and reduce their feelings of vulnerability.

5.3. Limitations and future research directions

First, this research identifies conceptual dimensions of transparency and control so future studies can develop multidimensional measurements of two constructs to precisely evaluate how consumers perceive firms’ data privacy practices. Second, this research does not consider the impacts of cultural norms on personal privacy. Future studies can extend the research context to other countries, considering possible variations in consumer vulnerability based on cultural beliefs around privacy rights and people’s interpretation of data ownership (Brynjolfsson *et al.*, 2021). Third, though our study reveals strategic approaches to communicating the value of transparency and control, it did not test the effectiveness of these approaches. Future studies can fill this gap by empirically investigating the effect of communicative approaches on consumer responses. Fourth, consumers face information overload in the digital world, which creates difficulty in understanding the policies and making efficient decisions (Alemany *et al.*, 2021). As a result, they may experience vulnerability (Muzatko and Bansal, 2023). Considering this issue, future research should further explore how to balance transparency and control and mitigate consumers' mental effort. Finally, the study extends an invitation for future research to employ quantitative methods in examining transparency and control. This entails assessing perspectives from both experiencers and observers (e.g., Hill and Sharma, 2020). Future studies may consider using surveys to measure the potential disparities between these two viewpoints. They could also develop policy-related experimental scenarios based on the observers' viewpoint and then test the scenarios by using experiencers as subjects. Exploring these potential disparities could provide valuable insights. Such insights would aid observers, including policymakers and experts, in refining their comprehension of transparency and control and improving related policies and practices to truly benefit experiencers. From the experiencer's standpoint, the insights contribute to the enhancement of customer privacy that safeguards the digital realm.

6. Conclusions

This study explores the conceptual dimensions of transparency and control underlying firms' privacy practices and investigates strategic approaches to communicating the value of transparency and control to address consumer vulnerability. The conceptual framework integrates justice theory and gossip theory, which addresses the gap in understanding how transparency and control are employed as tools to address gossip-related vulnerability and ensure fair, transparent, and ethical interactions between consumers and firms. Our findings provide a comprehensive understanding of the dimensions of transparency and control which complement the communication approaches to mitigate vulnerability. The findings aid the understanding of transparency and control in data privacy literature as they explore their breadth and facilitate the development of valid measurements for future research. Our managerial implications help firms develop ethical data practices and apply strategic approaches for communicating the value of transparency and control to foster consumer trust and address consumer vulnerability.

References

Agozie, D.Q. and Kaya, T. (2021), "Discerning the effect of privacy information transparency on privacy fatigue in e-government", *Government Information Quarterly,* Vol. 38 No. 4, pp. 101601.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K. and Wetzels, M. (2015), "Unraveling the personalization paradox: the effect of information collection and trust-building strategies on online advertisement effectiveness", *Journal of Retailing,* Vol. 91 No. 1, pp. 34-49.

Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V. and Viglia, G. (2020), "Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: the role of perceived warmth", *Journal of Retailing,* Vol. 96 No. 4, pp. 490-506.

Albashrawi, M. and Motiwalla, L. (2019), "Privacy and personalization in continued usage intention of mobile banking: an integrative perspective", *Information Systems Frontiers,* Vol. 21 No. 5, pp. 1031-1043.

Alemany, J., Del Val, E. and García-Fornes, A.M. (2021), "'Who should I grant access to my post?': identifying the most suitable privacy decisions on online social networks", *Internet Research,* Vol. 31 No. 4, pp. 1290-1317.

Ashworth, L. and Free, C. (2006), "Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns", *Journal of Business Ethics,* Vol. 67 No. 2, pp. 107-123.

Awad, N.F. and Krishnan, M.S. (2006), "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization", *MIS Quarterly,* Vol. 30 No. 1, pp. 13-28.

Baker, S.M., Gentry, J.W. and Rittenburg, T.L. (2005), "Building understanding of the domain of consumer vulnerability", *Journal of Macromarketing,* Vol. 25 No. 2, pp. 128-139.

Baker, S.M., Hunt, D.M. and Rittenburg, T.L. (2007), "Consumer vulnerability as a shared experience: tornado recovery process in Wright, Wyoming", *Journal of Public Policy & Marketing,* Vol. 26 No. 1, pp. 6-19.

Batat, W. and Tanner, J.F. (2021), "Unveiling (in)vulnerability in an adolescent's consumption subculture: a framework to understand adolescents' experienced (in)vulnerability and ethical implications", *Journal of Business Ethics,* Vol. 169 No. 4, pp. 713-730.

Benlian, A. and Hess, T. (2011), "The signaling role of IT features in influencing trust and participation in online communities", *International Journal of Electronic Commerce,* Vol. 15 No. 4, pp. 7-56.

Berger, P.L. and Luckmann, T. (1967), *The Social Construction of Reality,* Penguin Books, London, England.

Betzing, J.H., Tietz, M., vom Brocke, J. and Becker, J. (2020), "The impact of transparency on mobile privacy decision making", *Electronic Markets,* Vol. 30 No. 3, pp. 607-625.

Bies, R.J. (2001), "Interactional (in) justice: the sacred and the profane", Greenberg, J. and Cropanzano, R. (Ed.s), *Advances in Organizational Justice,* Stanford University Press, Stanford, CA, pp. 89-118.

Bleier, A. and Eisenbeiss, M. (2015), "The importance of trust for personalized online advertising", *Journal of Retailing,* Vol. 91 No. 3, pp. 390-409.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology,* Vol. 3 No. 2, pp. 77-101.

Brewster, T. (2019), "FaceApp: Is the Russian face-aging app a danger to your privacy?", *Forbes,* available at:

https://www.forbes.com/sites/thomasbrewster/2019/07/17/faceapp-is-the-russian-face-aging-app-a-danger-to-your-privacy/#2846472f2755 (accessed 2 January 2024).

Brynjolfsson, E., Wang, C. and Zhang, X. (2021), “The economics of IT and digitization: eight questions for research”, *MIS Quarterly,* Vol. 45 No. 1, pp. 473-477.

Buglass, S.L., Binder, J.F., Betts, L.R. and Underwood, J.D.M. (2016), “When ‘friends’ collide: social heterogeneity and user vulnerability on social network sites”, *Computers in Human Behavior,* Vol. 54, pp. 62-72.

Chen, Q., Feng, Y., Liu, L. and Tian, X. (2019), “Understanding consumers’ reactance of online personalized advertising: a new scheme of rational choice from a perspective of negative effects”, *International Journal of Information Management,* Vol. 44, pp. 53-64.

Chen, S.J., Tamilmani, K., Tran, K.T., Waseem, D. and Weerakkody, V. (2022), “How privacy practices affect customer commitment in the sharing economy: A study of Airbnb through an institutional perspective”, *Industrial Marketing Management*, Vol. 107, pp.161-175.

Chen, S.J., Tran, K.T., Xia, Z.R., Waseem, D., Zhang, J.A. and Potdar, B. (2023), “The double-edged effects of data privacy practices on customer responses”, *International Journal of Information Management,* Vol. 69, pp. 102600.

Cheng, J., Usman, M., Bai, H. and He, Y. (2022), “Can authentic leaders reduce the spread of negative workplace gossip? The roles of subordinates’ perceived procedural justice and interactional justice”, *Journal of Management & Organization,* Vol. 28 No. 1, pp. 9-32.

Cho, H. (2022), “Privacy helplessness on social media: its constituents, antecedents and consequences”, *Internet Research,* Vol. 32 No. 1, pp. 150-171.

Cohen-Charash, Y. and Spector, P.E. (2001), “The role of justice in organizations: a meta-analysis”, *Organizational Behavior and Human Decision Processes,* Vol. 86 No. 2, pp. 278-321.

Colquitt, J.A. and Rodell, J.B. (2011), “Justice, trust, and trustworthiness: a longitudinal analysis integrating three theoretical perspectives”, *Academy of Management Journal,* Vol. 54 No. 6, pp. 1183-1206.

Creswell, J.W. (2014), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches,* Sage Publications, Thousand Oak, CA.

Culnan, M.J. and Bies, R.J. (2003), “Consumer privacy: balancing economic and justice considerations”, *Journal of Social Issues,* Vol. 59 No. 2, pp. 323-342.

Dinev, T., Xu, H., Smith, J.H. and Hart, P. (2013), “Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts”, *European Journal of Information Systems,* Vol. 22 No. 3, pp. 295-316.

Duan, S.X. and Deng, H. (2022), “Exploring privacy paradox in contact tracing apps adoption”, *Internet Research,* Vol. 32 No. 5, pp. 1725-1750.

Dunbar, R.I. (2004), “Gossip in evolutionary perspective”, *Review of General Psychology,* Vol. 8 No. 2, pp. 100-110.

Dyussembayeva, S., Viglia, G., Nieto-Garcia, M. and Invernizzi, A.C. (2020), “It makes me feel vulnerable! The impact of public self-disclosure on online complaint behavior”, *International Journal of Hospitality Management,* Vol. 88, pp. 102512.

Eggers, F., Beke, F.T., Verhoef, P.C. and Wieringa, J.E. (2023), “The market for privacy: understanding how consumers trade off privacy practices”, *Journal of Interactive Marketing,* Vol. 58 No. 4, pp. 341-360.

Elhai, J.D., Levine, J.C. and Hall, B.J. (2017), “Anxiety about electronic data hacking: predictors and relations with digital privacy protection behavior”, *Internet Research,* Vol. 27 No. 3, pp. 631-649.

Ellis, K.M., Reus, T.H. and Lamont, B.T. (2009), “The effects of procedural and informational justice in the integration of related acquisitions”, *Strategic Management Journal,* Vol. 30 No. 2, pp. 137-161.

Emler, N. (1994), “Gossip, reputation, and social adaptation", Goodman, R.F. and Ben-Ze’ev, A. (Ed.s) *Good Gossip,* University Press of Kansas, Lawrence, KS, pp. 117-138.

Esmaeilzadeh, P. (2020), “The impacts of the privacy policy on individual trust in health information exchanges (HIEs)”, *Internet Research,* Vol. 30 No. 3, pp. 811-843.

Fan, Y. (2005), “Ethical branding and corporate reputation”, *Corporate Communications: An International Journal,* Vol. 10 No. 4, pp. 341-350.

Fang, X., Yang, Z., Zhang, Y. and Guo, C. (2023), “Adverse effects of data breach on public companies: a study based on interpersonal gossip theory”, *Emerging Markets Finance and Trade,* Vol. 59 No. 9, pp. 1-14.

Fox, A.K. and Hoy, M.G. (2019), “Smart devices, smart decisions? Implications of parents’ sharenting for children’s online privacy: an investigation of mothers”, *Journal of Public Policy & Marketing,* Vol. 38 No. 4, pp. 414-432.

Fox, G. and James, T.L. (2021), “Toward an understanding of the antecedents to health information privacy concern: a mixed methods study”, *Information Systems Frontiers,* Vol. 23 No. 6, pp. 1537-1562.

Grant, A.M. and Ashford, S.J. (2008), “The dynamics of proactivity at work”, *Research in Organizational Behavior,* Vol. 28, pp. 3-34.

Greenberg, J. (1993), “The social side of fairness: interpersonal and informational classes of organizational justice”, *Justice in the Workplace: Approaching Fairness in Human Resource Management,* Cropanzano, R. (Ed.), Lawrence Erlbaum Associates, Hillsdale, NJ, pp. 79-103.

Groenewald, T. (2004), “A phenomenological research design illustrated”, *International Journal of Qualitative Methods,* Vol. 3 No. 1, pp. 42-55.

Guo, Y., Wang, X. and Wang, C. (2022), “Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern”, *Journal of Enterprise Information Management,* Vol. 35 No. 3, pp. 774-795.

Hajli, N. and Lin, X. (2016), “Exploring the security of information sharing on social networking sites: the role of perceived control of information”, *Journal of Business Ethics,* Vol. 133 No. 1, pp. 111-123.

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F. and Morsut, C. (2020), “Communication-related vulnerability to disasters: a heuristic framework”, *International Journal of Disaster Risk Reduction,* Vol. 51, pp. 1-9, 101931.

Heeks, R. and Renken, J. (2018), “Data justice for development: what would it mean?”, *Information Development,* Vol. 34 No. 1, pp. 90-102.

Hill, R. and Sharma, E. (2020), “Consumer vulnerability”, *Journal of Consumer Psychology,* Vol. 30 No. 3, pp. 551-570.

Hong, W. and Thong, J.Y. (2013), “Internet privacy concerns: an integrated conceptualization and four empirical studies”, *MIS Quarterly,* Vol. 37 No. 1, pp. 275-298.

Hugl, U. (2011), “Reviewing person’s value of privacy of online social networking”, *Internet Research,* Vol. 21 No. 4, pp. 384-407.

Hui, K.-L., Teo, H.H. and Lee, S.-Y.T. (2007), “The value of privacy assurance: an exploratory field experiment”, *MIS Quarterly,* Vol. 31 No. 1, pp. 19-33.

Hycner, R.H. (1985), “Some guidelines for the phenomenological analysis of interview data”, *Human Studies,* Vol. 8 No. 3, pp. 279-303.

James, T.L., Nottingham, Q., Collignon, S.E., Warkentin, M. and Ziegelmayer, J.L. (2016), “The interpersonal privacy identity (IPI): development of a privacy as control model”, *Information Technology and Management,* Vol. 17 No. 4, pp. 341-360.

Janakiraman, R., Lim, J.H. and Rishika, R. (2018), "The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer", *Journal of Marketing,* Vol. 82 No. 2, pp. 85-105.

Kang, H., Shin, W. and Huang, J. (2022), "Teens' privacy management on video-sharing social media: the roles of perceived privacy risk and parental mediation", *Internet Research,* Vol. 32 No. 1, pp. 312-334.

Karwatzki, S., Dytynko, O., Trenz, M. and Veit, D. (2017), "Beyond the personalization–privacy paradox: privacy valuation, transparency features, and service personalization", *Journal of Management Information Systems,* Vol. 34 No. 2, pp. 369-400.

Kennedy, A.-M., Jones, K. and Williams, J. (2019), "Children as vulnerable consumers in online environments", *Journal of Consumer Affairs,* Vol. 53 No. 4, pp. 1478-1506.

Kim, T., Barasz, K. and John, L.K. (2019), "Why am I seeing this ad? The effect of ad transparency on ad effectiveness", *Journal of Consumer Research,* Vol. 45 No. 5, pp. 906-932.

Kleinman, Z. (2020), "Popular app T&Cs 'longer than Harry Potter'", *BBC News*, available at: https://www.bbc.com/news/technology-54838978 (accessed 2 January 2024).

Konovsky, M.A. (2000), "Understanding procedural justice and its impact on business organizations", *Journal of Management,* Vol. 26 No. 3, pp. 489-511.

Kumar, V., Zhang, X. and Luo, A. (2014), "Modeling customer opt-in and opt-out in a permission-based marketing context", *Journal of Marketing Research,* Vol. 51 No. 4, pp. 403-419.

Kupfer, J. (1987), "Privacy, autonomy, and self-concept", *American Philosophical Quarterly,* Vol. 24 No. 1, pp. 81-89.

Kvale, S. (1983), "The qualitative research interview: A phenomenological and a hermeneutical mode of understanding", *Journal of Phenomenological Psychology,* Vol. 14 No. 2, pp. 171.

Kvale, S. (1995), "The social construction of validity", *Qualitative Inquiry,* Vol. 1 No. 1, pp. 19-40.

Larsen, G. and Lawson, R. (2013), "Consumer rights: an assessment of justice", *Journal of Business Ethics,* Vol. 112 No. 3, pp. 515-528.

Leary, M.R. and Leder, S. (2009), "The nature of hurt feelings: emotional experience and cognitive appraisals", Vangelisti, A.L. (Ed.), *Feeling Hurt in Close Relationships,* Cambridge University Press, New York, NY, pp. 15-33.

Liang, C., Peng, J., Hong, Y. and Gu, B. (2023), "The hidden costs and benefits of monitoring in the gig economy", *Information Systems Research,* Vol. 34 No. 1, pp. 297-318.

Libaque-Sáenz, C.F., Wong, S.F., Chang, Y. and Bravo, E.R. (2021), "The effect of fair information practices and data collection methods on privacy-related behaviors: a study of mobile apps", *Information & Management,* Vol. 58 No. 1, pp. 103284.

Liyanaarachchi, G., Deshpande, S. and Weaven, S. (2020), "Market-oriented corporate digital responsibility to manage data vulnerability in online banking", *International Journal of Bank Marketing,* Vol. 39 No. 4, pp. 571-591.

Locke, E.A. (2007), "The case for inductive theory building", *Journal of Management,* Vol. 33 No. 6, pp. 867-890.

Lofland, J. and Lofland, L. (1995), *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis,* Wadsworth, Boston, MA.

Lwin, M.O., Wirtz, J. and Stanaland, A.J. (2016), "The privacy dyad: antecedents of promotion-and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern", *Internet Research,* Vol. 26 No. 4, pp. 919-941.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), “Internet users’ information privacy concerns (IUIPC): the construct, the scale, and a causal model”, *Information Systems Research,* Vol. 15 No. 4, pp. 336-355.

Markos, E., Milne, G.R. and Peltier, J.W. (2017), “Information sensitivity and willingness to provide continua: a comparative privacy study of the united states and brazil”, *Journal of Public Policy & Marketing,* Vol. 36 No. 1, pp. 79-96.

Martin, K., Borah, A. and Palmatier, R. (2017), “Data privacy: effects on customer and firm performance”, *Journal of Marketing,* Vol. 81 No. 1, pp. 36-58.

Martin, K.D., Kim, J.J., Palmatier, R.W., Steinhoff, L., Stewart, D.W., Walker, B.A., Wang, Y. and Weaven, S.K. (2020), “Data privacy in retail”, *Journal of Retailing,* Vol. 96 No. 4, pp. 474-489.

Martin, K and Murphy, P. (2017), “The role of data privacy in marketing”, *Journal of the Academy of Marketing Science,* Vol. 45 No. 2, pp. 135-155.

Mazurek, G. and Małagocka, K. (2019), “What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think”, *Business Horizons,* Vol. 62 No. 6, pp. 751-759.

Melville, N., Kraemer, K. and Gurbaxani, V. (2004), “Information technology and organizational performance: an integrative model of IT business value”, *MIS Quarterly,* Vol. 28 No. 2, pp. 283-322.

Mills, R.T. and Krantz, D.S. (1979), “Information, choice, and reactions to stress: a field experiment in a blood bank with laboratory analogue”, *Journal of Personality and Social Psychology,* Vol. 37 No. 4, pp. 608-620.

Morimoto, M. (2021), “Privacy concerns about personalized advertising across multiple social media platforms in Japan: the relationship with information control and persuasion knowledge”, *International Journal of Advertising,* Vol. 40 No. 3, pp. 431-451.

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E. and Wang, S. (2012), “Disclosure antecedents in an online service context: the role of sensitivity of information”, *Journal of Service Research,* Vol. 15 No. 1, pp. 76-98.

Mpinganjira, M. and Maduku, D.K. (2019), “Ethics of mobile behavioral advertising: antecedents and outcomes of perceived ethical value of advertised brands”, *Journal of Business Research,* Vol. 95, pp. 464-478.

Muzatko, S. and Bansal, G. (2023), “It pays to be forthcoming: timing of data breach announcement, trust violation, and trust restoration”, *Internet Research,* Vol. ahead-of-print No. ahead-of-print, https://doi.org/10.1108/INTR-12-2021-0939.

Norberg, P.A. and Horne, D.R. (2014), “Coping with information requests in marketing exchanges: an examination of pre-post affective control and behavioral coping”, *Journal of the Academy of Marketing Science,* Vol. 42 No. 4, pp. 415-429.

O’Sullivan, S.R. (2015), “The market maven crowd: collaborative risk-aversion and enhanced consumption context control in an illicit market”, *Psychology & Marketing,* Vol. 32 No. 3, pp. 285-302.

Oldeweme, A., Märtins, J., Westmattelmann, D. and Schewe, G. (2021), “The role of transparency, trust, and social influence on uncertainty reduction in times of pandemics: empirical study on the adoption of COVID-19 tracing apps”, *Journal of Medical Internet Research,* Vol. 23 No. 2, pp. 25-93.

Parkinson, J., Schuster, L., Mulcahy, R. and Taiminen, H.M. (2017), “Online support for vulnerable consumers: a safe place?”, *Journal of Services Marketing,* Vol. 31 No. 4/5, pp. 412-422.

Pollach, I. (2005), “A typology of communicative strategies in online privacy policies: ethics, power and informed consent”, *Journal of Business Ethics,* Vol. 62 No. 3, pp. 221-235.

Pratt, M.G. (2009), "From the editors: for the lack of a boilerplate: tips on writing up (and reviewing) qualitative research", *Academy of Management Journal,* Vol. 52 No. 5, pp. 856-862.

Privacy Rights Clearinghouse (2019), "*Chronology of data breaches*", available at: https://privacyrights.org/data-breaches (accessed 2 January 2024).

Punj, G.N. (2019), "Understanding individuals' intentions to limit online personal information disclosures to protect their privacy: implications for organizations and public policy", *Information Technology and Management,* Vol. 20 No. 3, pp. 139-151.

Ray, S., Ow, T. and Kim, S.S. (2011), "Security assurance: how online service providers can influence security control perceptions and gain trust", *Decision Sciences,* Vol. 42 No. 2, pp. 391-412.

Rosenberg, M., Confessore, N. and Cadwalladr, C. (2018), "How Trump consultants exploited the Facebook data of millions", *New York Times,* available at: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (accessed 2 January 2024).

Sandberg, J. (2005), "How do we justify knowledge produced within interpretive approaches?", *Organizational Research Methods,* Vol. 8 No. 1, pp. 41-68.

Satariano, A. (2023), "Meta fined $1.3 billion for violating E.U. data privacy rule", *New York Times,* available at: https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html (accessed 2 January 2024).

Schlackl, F., Link, N. and Hoehle, H. (2022), "Antecedents and consequences of data breaches: a systematic review", *Information & Management,* Vol. 59 No. 4, pp. 1-15, 103638.

Scott, B.A., Colquitt, J.A. and Paddock, E.L. (2009), "An actor-focused model of justice rule adherence and violation: the role of managerial motives and discretion", *Journal of Applied Psychology,* Vol. 94 No. 3, pp. 756-769.

Seiders, K. and Berry, L.L. (1998), "Service fairness: What it is and why it matters", *Academy of Management Perspectives,* Vol. 12 No. 2, pp. 8-20.

Smith, N.C. and Cooper-Martin, E. (1997), "Ethics and target marketing: the role of product harm and consumer vulnerability", *Journal of Marketing,* Vol. 61 No. 3, pp. 1-20.

Song, J.H., Kim, H.Y., Kim, S., Lee, S.W. and Lee, J.-H. (2016), "Effects of personalized e-mail messages on privacy risk: moderating roles of control and intimacy", *Marketing Letters,* Vol. 27 No. 1, pp. 89-101.

Steinhoff, L. and Martin, K.D. (2023), "Putting data privacy regulation into action: the differential capabilities of service frontline interfaces", *Journal of Service Research,* Vol. 26 No. 3, pp. 330-350.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), *Risk Management Guide for Information Technology Systems,* National Institute of Standards and Technology, Gaithersburg, MD.

Suh, B. and Han, I. (2003), "The impact of customer trust and perception of security control on the acceptance of electronic commerce", *International Journal of Electronic Commerce,* Vol. 7 No. 3, pp. 135-161.

Taylor, D.G., Davis, D.F. and Jillapalli, R. (2009), "Privacy concern and online personalization: the moderating effects of information control and compensation", *Electronic Commerce Research,* Vol. 9 No. 3, pp. 203-223.

Thibaut, J. and Walker, L. (1978), "A theory of procedure", *California Law Review,* Vol. 66, pp. 541-566.

Tucker, C.E. (2014), "Social networks, personalized advertising, and privacy controls", *Journal of Marketing Research,* Vol. 51 No. 5, pp. 546-562.

Vail, M.W., Earp, J.B. and AntÓn, A.I. (2008), “An empirical study of consumer perceptions and comprehension of web site privacy policies”, *IEEE Transactions on Engineering Management*, Vol. 55 No. 3, pp. 442-454.

Wang, E.S.-T. (2019), “Effects of brand awareness and social norms on user-perceived cyber privacy risk”, *International Journal of Electronic Commerce,* Vol. 23 No. 2, pp. 272-293.

Wax, A., Rodriguez, W.A. and Asencio, R. (2022), “Spilling tea at the water cooler: a meta-analysis of the literature on workplace gossip“, *Organizational Psychology Review,* Vol. 12 No. 4, pp. 453-506.

Wertenbroch, K., Schrift, R.Y., Alba, J.W., Barasch, A., Bhattacharjee, A., Giesler, M., Knobe, J., Lehmann, D.R., Matz, S. and Nave, G. (2020), “Autonomy in consumer choice”, *Marketing Letters,* Vol. 31 No. 4, pp. 429-439.

Weydert, V., Desmet, P. and Lancelot-Miltgen, C. (2020), “Convincing consumers to share personal data: double-edged effect of offering money”, *Journal of Consumer Marketing,* Vol. 37 No. 1, pp. 1-9.

Whitman, D.S., Caleo, S., Carpenter, N.C., Horner, M.T. and Bernerth, J.B. (2012), “Fairness at the collective level: a meta-analytic examination of the consequences and boundary conditions of organizational justice climate”, *Journal of Applied Psychology,* Vol. 97 No. 4, pp. 776-791.

Wirth, J., Maier, C., Laumer, S. and Weitzel, T. (2022), “Laziness as an explanation for the privacy paradox: a longitudinal empirical investigation”, *Internet Research,* Vol. 32 No. 1, pp. 24-54.

Wünderlich, N.V., Hogreve, J., Chowdhury, I.N., Fleischer, H., Mousavi, S., Rötzmeier-Keuper, J. and Sousa, R. (2020), “Overcoming vulnerability: channel design strategies to alleviate vulnerability perceptions in customer journeys”, *Journal of Business Research,* Vol. 116, pp. 377-386.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011), “Information privacy concerns: linking individual perceptions with institutional privacy assurances”, *Journal of the Association for Information Systems,* Vol. 12 No. 12, pp. 798-824.

Xu, H., Teo, H.-H., Tan, B.C. and Agarwal, R. (2012), “Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services”, *Information Systems Research,* Vol. 23 No. 4, pp. 1342-1363.

Zhang, F., Pan, Z. and Lu, Y. (2023a), “AIoT-enabled smart surveillance for personal data digitalization: contextual personalization-privacy paradox in smart home”, *Information & Management,* Vol. 60 No. 2, pp. 103736.

Zhang, F., Zhang, H. and Gupta, S. (2023b), “Investor participation in reward-based crowdfunding: impacts of entrepreneur efforts, platform characteristics, and perceived value”, *Information Technology and Management,* Vol. 24 No. 1, pp. 19-36.

Zhang, J., Li, H., Luo, X. and Warkentin, M. (2017), “Exploring the effects of the privacy-handling management styles of social networking sites on user satisfaction: a conflict management perspective”, *Decision Sciences,* Vol. 48 No. 5, pp. 956-989.

Zhao, L., Lu, Y. and Gupta, S. (2012), “Disclosure intention of location-related information in location-based social network services”, *International Journal of Electronic Commerce,* Vol. 16 No. 4, pp. 53-90.

APPENDICES. Appendix A. Review of literature on consumer vulnerability in the online environment

Study	Method	Context	Definition
Aguirre *et al.* (2015)	Quantitative: Experiments	Online personalized advertising	"*Vulnerability arises when consumers lack a sense of control over the situation and experience a state of powerlessness, brought about by marketplace imbalances"* (p. 37).
Bleier and Eisenbeiss (2015)	Quantitative: Experiments	Online personalized advertising	"*A loss of control due to a privacy intrusion reflects a consumer's vulnerability to the data-collecting and advertising firm and prompts privacy concerns*" (p. 395).
O'Sullivan (2015)	Qualitative: Netnography	Online	Consumer vulnerability is "*a state of powerlessness that arises from an imbalance in the marketplace: it occurs when control is not in the consumer's hands, creating a dependence on external factors to establish fairness*" (p. 286).
Buglass *et al.* (2016)	Quantitative: Digitally derived data and surveys	Social network sites	Consumers' online vulnerability is "*the capacity to experience detriments to psychological, reputational or physical wellbeing…due to risks encountered whilst engaging in online activities*" (p. 62).
Martin *et al.* (2017)	Quantitative: Experiments, event study, and field study	General business contexts	Consumer vulnerability refers to "a c*ustomer's perception of his or her susceptibility to being harmed as a result of various uses of his or her personal data*" (p. 37).
Parkinson *et al.* (2017)	Qualitative: Netnography	Online support group	Consumer vulnerability is "*generally accepted as a state of powerlessness that hinders consumption goals and may create circumstances which negatively affect perceptions of self*" (p. 413).
Chen *et al.* (2019)	Quantitative: Survey	Online personalized advertising	Vulnerability is the lack of a sense of control over the service or the perception of a threat to one's self-concept; consumers may experience vulnerability. It is a negative emotional state.
Fox and Hoy (2019)	Qualitative: Interviews and observations	Online sharenting by parents	Consumer vulnerability "*focuses on a dynamic, situational, and temporary condition…and includes a sense of reduced ability to act in one's best interest*" (p. 415).
Kennedy *et al.* (2019)	Conceptual	Online context	Consumer vulnerability focuses on the themes of powerlessness, hindrance of consumption goals, and effect on Self.

Study	**Method**	**Context**	**Definition**
Dyussembayeva *et al.* (2020)	Mixed methods	Online complaint behavior	Vulnerability "*is the state of being exposed to the possibility of being attacked or harmed, either physically or emotionally*" (p. 2).
Hill and Sharma (2020)	Conceptual	General	Consumer vulnerability is "*a state in which consumers are subject to harm because their access to and control over resources is restricted in ways that significantly inhibit their abilities to function in the marketplace"* (p. 551).
Liyanaarachchi *et al.* (2020)	Conceptual	Online banking	Consumer vulnerability is "*a state of powerlessness that arises from an imbalance in marketplace interactions or the consumption of marketing messages and products*" (p. 573).
Martin *et al.* (2020)	Mixed methods: Interviews, survey, and case studies	Retail	"*Customer personalization through tools such as location tracking, facial recognition, emotion tracking, and voice encoding and interpretation, all of which might aggravate consumers' sense of vulnerability*" (p. 474).
Batat and Tanner (2021)	Qualitative: Quasi-Ethnographic study	Various vulnerabilities of adolescent consumers	Consumer vulnerability is "*is shaped by the norms and codes of the cultural setting in which it is embedded, and is perceived in a reflexive and subjective way by the individual as a feeling related to powerlessness and fear of a potential loss due to risk*" (p. 714).

[Note: We used Web of Science to search for articles using combinations of keywords "online", "consumer", "privacy", "vulnerability", etc. For quality control, we searched for articles (ranked as either A/A* by the Australian Business Deans Council or 3 and above by the Chartered Association of Business Schools) in the areas of information management, hospitality, tourism, and marketing published from 2015 onwards]

Appendix B. Review of the literature on transparency and control in various online contexts

Study	Method	Context	Definition of control or transparency (if covered)	Perspectives		Suppressors	
				Observer	Experiencer	Transparency	Control
Suh and Han (2003)	Quantitative: Survey	Internet banking in South Korea	Five categories of *security control* are authentication, nonrepudiation, confidentiality, privacy protection, and data integrity.	X	✓	X	Firm ability (security)
Malhotra *et al.* (2004)	Quantitative: Survey	Online privacy in the US	Control is one dimension of information privacy concerns. The *control* factor represents the freedom to voice an opinion (i.e., approval, modification) or exit (i.e., opt-out).	X	✓	X	Firm ability (factors)
Awad and Krishnan (2006)	Quantitative: Survey	Personalized service and personalized advertising in the US	*Information transparency features* mean "features that give consumers access to the information a firm has collected about them, and how that information is going to be used" (p. 14).	X	✓	Firm ability	X
Taylor *et al.* (2009)	Quantitative: Experiment	Online personalization (travel site) in the US	*Information control* refers to "the power of consumers to decide what is learned about them" (p. 208).	X	✓	X	User ability
Benlian and Hess (2011)	Quantitative: Survey and content analysis	Online communities in the US and Germany	"*Transparency* in online environments can be understood as the selective exchange of sensitive information between two entities involved in the exchange relationship in order to reduce ex ante risk and uncertainty" (p.16).	X	✓	Information exchange	X
Ray *et al.* (2011)	Quantitative: Survey	Online services (retail) in the US	*Security control* was defined by five subfactors: authentication control, nonrepudiation control, privacy control, confidentiality control, and data-integrity control.	X	✓	X	Firm abilities (factors)
Mothersbaugh *et al.* (2012)	Quantitative: Experiment	Online service (TV program guide) in the US	Firm-specific *information control* is defined as "the extent to which a consumer believes that she or he can influence if and how the firm uses their personal information for marketing purposes" (p. 77).	X	✓	X	User belief
Xu *et al.* (2012)	Quantitative: Experiment	Location-based services in Singapore	*Perceived control over personal information* is defined as "an individual's belief about the presence of factors that may increase or decrease the amount of control over the release and dissemination of personal information" (p. 1346).	X	✓	X	User belief
Zhao *et al.* (2012)	Quantitative: Survey	Location-based social network services in mobile	*Privacy control* relates to the functions/features provided by service providers to enhance users' perception of their social control and information control.	X	✓	X	Firm ability (functions /features)

Study	Method	Context	Definition of control or transparency (if covered)	Perspectives		Suppressors	
				Observer	Experiencer	Transparency	Control
		environments in China					
Dinev *et al.* (2013)	Quantitative: Survey	Web 2.0 such as blogging sites, tagging sites, user-driven rating sites, and social networking sites in the US	*Information control* is conceptualized as a perception and defined as an “individual’s beliefs in one’s ability to determine to what extent information about the self will be released onto the Web 2.0-related sites” (p. 299-300). *Importance of information transparency* is defined as the “consumer-rated importance of notifying the consumers what types of information a firm has collected about them, and how that information is going to be used” (p. 303)	X	X	Information exchange	User belief
Hong and Thong (2013)	Quantitative: Multiple studies	Internet users in Hong Kong	*Control* is “the degree to which a person is concerned that he/she does not have adequate control over his/her personal information held by websites” (p. 278).	X	✓	X	User concern
Tucker (2014)	Quantitative: Experiment	Social networking sites (Facebook) in the US	*Privacy control* is the introduction of improved privacy control policies (improved privacy interface through which users control their privacy settings).	X	✓		Firm ability
Hajli and Lin (2016)	Quantitative: Survey	Social networking sites in the US	*Perceived control of information* “is considered to be a cognitive construct and is defined as the extent to which an individual feels that SNS allows that individual to control the use of information through privacy settings” (p. 113).	X	✓	X	User perception
James *et al.* (2016)	Quantitative: Survey	General and online behaviors in multiple countries	*Information control belief* is a person’s belief in his or her right to control his or her information. Information management relates to the self-disclosure or non-disclosure of personal information.	X	✓	X	User belief
Song *et al.* (2016)	Quantitative: Experiment	Personalized services (e-mail messages) in South Korea	*Control over personal information* refers to the features that grant consumers access to their personal information and authority to determine how such information can be used for personalized services.	X	✓	X	Firm abilities
Karwatzki *et al.* (2017)	Quantitative: Experiment	A data-intense digital service (website) in Germany	*Information-use transparency* is “the extent to which an online firm provides features that allow consumers to access the data collected about them and informs them about how and for what purposes the acquired information is used” (p. 372).	X	✓	Firm ability	X

Study	Method	Context	Definition of control or transparency (if covered)	Perspectives		Suppressors	
				Observer	Experiencer	Transparency	Control
Markos *et al.* (2017)	Quantitative: Experiment	General context in the US and Brazil	*Perceived privacy control* is linked with the concept of privacy. It relates to the type of personal information and potential harm associated with that information being seen, used, or accessed by others.	X	✓	X	User perception
Zhang *et al.* (2017)	Quantitative: Survey	Social networking sites (Facebook) in the US	*Perceived risk control* is defined as "users' perception of their power to avoid or reduce privacy risk" (p. 962).	X	✓	X	User perception
Kim *et al.* (2019)	Quantitative: Multiple studies	Online targeted advertising (websites) in the US	*Ad transparency* is the disclosure of how consumers' personal information was used to generate ads and/or how firms collect and use consumer personal data to generate behaviorally targeted ads.	X	✓	Firm ability	X
Punj (2019)	Quantitative: Survey	Online context in the US	*Need for control* over personal information is viewed as essential to the conceptualization of privacy. It denotes the degree of control the individual seeks over their personal information online.	X	✓	X	User conceptualization
Wang (2019)	Quantitative: Survey	Websites in Taiwan	*Perceived control* over information disclosure concerns a person's judgment of the efficacy with which he or she can execute specific actions to manage personal information disclosure.	X	✓	X	User judgement
Betzing *et al.* (2020)	Quantitative: Experiment	Mobile apps in the European Union	*Transparency* is "an essential requirement for making informed consent decisions and might fundamentally influence users' behavior regarding (mobile) privacy decision making in the long run" (p. 620).	X	✓	Firm ability	X
Esmaeilzadeh (2020)	Quantitative: Survey	Health information exchange (HIE) in the US	*Perceived transparency of the privacy policy* is "the extent to which people believe that the HIE provides clear information related to notice, choice, access, security measures, retention, and enforcement in the privacy policy" (p. 822). It comprises six dimensions: notice, choice, access, security, retention, and enforcement.	X	✓	User belief	X
Weydert *et al.* (2020)	Quantitative: Experiment	Data brokers in France	*Active control* over data usage is "the ability to control to whom the data broker sells the data and what will be done with it" (p. 3).	X	✓	X	Firm ability

Study	Method	Context	Definition of control or transparency (if covered)	Perspectives		Suppressors	
				Observer	Experiencer	Transparency	Control
Agozie and Kaya (2021)	Quantitative: Survey	e-Government website in Cyprus	*Privacy information transparency* focuses on "privacy information aspects provided to users to ensure an understanding required to evaluate online privacy assurance and performance" or "the extent of accessibility of privacy information available to users to assess reliability and privacy assurance processes on e-government sites" (p. 3).	X	✓	Firm ability	X
Libaque-Sáenz *et al.* (2021)	Quantitative: Experiment	Mobile apps in the US	*Perceived data control* is "consumers' perception of their ability to manage the collection and use of their personal information" (p. 5).	X	✓	X	User perception
Morimoto (2021)	Quantitative: Survey	Personalized advertising in Japan	*Information control* in online privacy, particularly unpermitted personal information disclosure, is associated with perceived intrusiveness.	X	✓	X	User perception (intrusiveness)
Guo *et al.* (2022)	Quantitative: Experiment	Online shopping in China	*Transparency "*clearly discloses enterprises' information policy on data use, such as what information they collect and how it will be used and telling users whether to share with third parties" (p. 776). *Control* is "the extent to which customers have control over the use of their personal information, such as allowing customers to query, modify or delete personal data, and choose the type of personal data that enterprises can collect" (p. 776).	X	✓	Firm ability	User ability
Kang *et al.* (2022)	Quantitative: Survey	Video-sharing social media in China	*Privacy boundary control* is "the extent to which users apply various strategies to withdraw information they had already shared or to actively avoid sharing personal information on the platform by deleting posts, un-tagging themselves or others, or setting their profiles to private" (p. 315).	X	✓	X	User ability
Liang *et al.* (2023)	Quantitative: Experiment	Gig economy platforms (Amazon Mechanical Turk and Prolific)	*Transparency* refers to "the disclosure of what information is collected and how it is collected" (p. 4). *Control* means whether people can modify or remove sensitive information.	X	✓	Firm ability	User ability
Zhang *et al.* (2023a)	Quantitative: Survey	Smart home in China	*Perceived personalized smart object control* is "the degree to which smart homes provide a personalized manner for	X	✓	Firm ability	Firm ability

Study	Method	Context	Definition of control or transparency (if covered)	Perspectives		Suppressors	
				Observer	Experiencer	Transparency	Control
			users to control smart devices or smart objects" (p. 4). *Data use transparency is* "the extent to which smart home service suppliers provide features to enable users to access collected data and inform them about how and for what purposes the acquired information is used" (p. 4).				
Zhang *et al.* (2023b)	Quantitative: Survey	Crowdfunding platform in China	*Information transparency* refers to "the level of availability and accessibility of project-relevant information on the crowdfunding platform" (p. 25).	X	✓	Firm ability	X

[Note: We used the Web of Science database to systematically search for articles in reputable journals based on a combination of different keywords— "control" or "transparency", "privacy" or "vulnerability", "online" or "internet", and "information" or "data"—within the business, management, information science, behavioral sciences, and information science categories. X = None]

APPENDIX C. Participant profiles

Number	Role	Gender	Country	Industry	Profession
01	Expert	Male	New Zealand	Services	Cybersecurity analyst
02	Expert	Male	China	Public sector	Cybersecurity officer
03	Expert	Female	New Zealand	Education	Researcher in artificial intelligence
04	Expert	Male	United Kingdom	Education	Researcher in data analytics
05	Expert	Male	New Zealand	IT	Data steward
06	Expert	Female	United States	Aviation	Data consultant
07	Expert	Male	New Zealand	Education	Consumer researcher
08	Expert	Male	New Zealand	Services	Cybersecurity consultant
09	Expert	Male	New Zealand	IT	Software developer
10	Expert	Male	China	Services	E-commerce administrator
11	Expert	Male	China	Healthcare	CEO
12	Expert	Male	China	TV shopping	CEO
13	Expert	Male	Australia	Services	Service delivery specialist
14	Expert	Male	United Kingdom	Education	Researcher in information management
15	Expert	Female	Australia	Banking	Test analyst
16	Expert	Male	Australia	Banking	Senior analyst
17	Expert	Male	United Kingdom	Aviation	Data analyst
18	Consumer	Female	United Kingdom	Entertainment	Marketing executive
19	Consumer	Male	United Kingdom	Education	Postgraduate student
20	Consumer	Female	United Kingdom	Education	Postgraduate student
21	Consumer	Female	United Kingdom	Education	Academic director
22	Consumer	Male	United Kingdom	Education	Postgraduate student
23	Consumer	Male	United Kingdom	Retail	Service manager
24	Consumer	Female	United Kingdom	Education	Postgraduate student
25	Consumer	Female	United Kingdom	Education	Postgraduate student
26	Consumer	Male	United Kingdom	Education	Professor
27	Consumer	Male	United Kingdom	Consulting	Marketing consultant
28	Consumer	Male	United Kingdom	NGO	Community manager
29	Consumer	Female	New Zealand	Education	Postgraduate student
30	Consumer	Male	New Zealand	Education	Student
31	Consumer	Female	New Zealand	Education	Student
32	Consumer	Male	United States	Consulting	Human resource administrator
33	Consumer	Male	United States	Marketing	Digital promotion broker
34	Consumer	Male	Australia	Entertainment	Entertainment manager
35	Consumer	Female	New Zealand	Education	Postgraduate student
36	Consumer	Female	New Zealand	Education	Postgraduate student
37	Consumer	Male	New Zealand	Education	Postgraduate student
38	Consumer	Female	New Zealand	Education	Postgraduate student
39	Consumer	Female	New Zealand	Education	Postgraduate student
40	Consumer	Female	New Zealand	Government	Human resource assistant
41	Consumer	Female	New Zealand	Education	Postgraduate student

Criteria:
Experts should have relevant knowledge, skills and/or professional experience in data privacy policies, procedures, and/or compliance frameworks.

Consumers should have a basic level of browsing online experience such as the ability to browse websites and understand common privacy issues. This was chosen to identify characteristics of participants that represent usual internet users.

APPENDIX D. Interview Guide

1. Please share some bad (or good) experiences in which you felt that the privacy of your data is very insecure (and/or secure). Have your family members, friends, colleagues, or industry partners described any bad (or good) experiences regarding data privacy?
2. What do you think companies, governments, or other organizations should do to make you or customers feel better and have more security? Why?
3. How would you describe good privacy practices and bad privacy practices? Please share some examples or experiences of good (or bad) data privacy practices.
4. Considering a company's online data privacy practices, what does transparency mean to you?
   - Please provide some examples of a company's data privacy practices that convey transparency (or non-transparency) to you or to customers. What do you think of those practices? If you think those practices are right (or wrong), please explain why.
   - What do you think of companies that have transparent (or non-transparent) data privacy practices?
5. Considering a company's data privacy practices, what does control mean to you?
   - Who has control over customer data online? Who do you think owns such data?
   - Please provide some examples of a company's data privacy practices that involve appropriate (or inappropriate) control over customer data. What do you think of those practices? If you think those practices are right (or wrong), please explain why.
   - What do you think of companies that have appropriate (or inappropriate) control over customer data?
6. What would be an appropriate data privacy practice and/or policy in an online environment to make customers feel safe and less vulnerable?
7. What should organizations be doing to exceed consumer privacy expectations?

APPENDIX E. Conceptual characteristics of transparency

First-order code	**Second-order code**	**Themes**
Firms give me confidence that their data collection is only for this specific service or their stated purpose	Valid and reliable record of how data are collected, used, or stored	Integrity
Provide accurate records of data if users request them		
It is unethical to not be transparent about the usage of user data		
Full information regarding the entire flow of user data	Complete information about the data-collection process	
Comprehensive information regarding the process from input of data to remarketing and reselling the data		
Provide relevant information about users with regards to recording history and use of cookies	Relevant information	
Sometimes there is irrelevant information from firms		
Information regarding the data stored	Complete information regarding data storage	
Information regarding all the data stored		
Firms should give users the right to know where their data are stored		
Explain which data are stored and which data are not stored		
Explain how long the data will be stored and end up		
Information regarding all online behaviors of a user is stored		
Communicate the information in a very upfront manner	Open communication	Understand ability
Openly communicate with users if their data are used by third parties		
Explicitly communicate the information about data collected from users		
Easy to find information about data privacy		
Communicate complete information about data usage and storage	Clear communication	
Easy to understand privacy policies		
Easy-to-use terms and conditions when a user signs up		
Clear communication in the form of a diagram to explain the process of data sharing/usage		
Communicate what data are collected and how they are used		
Seeking consent for the data usage/storage/sharing	Seek permission	Proactivity
Send reminder messages if data are used	Reminder messages	
Send reminder messages if data are collected		
Inform users what data are stored, and which are not	Proactively inform users	

APPENDIX F. Conceptual characteristics of control

First-order code	Second-order code	Themes
Consumers should control their data	Data ownership	Autonomy
The firm should not control users' personal data		
Users have full control of their information because they proactively provide it		
Users are responsible for what information they share with firms	Comprehension of data responsibility	
User's responsibility is to determine what they should publish or what they should not publish on the online platforms		
Consumers cannot do anything as they do not have control (over the data)		
Firms can view user data and do what they want to do		
Firms are responsible for using data ethically		
It is the firm's responsibility to protect data		
Two-way control (i.e., information firms provide and the information that users provide)		
The government should hold private firms responsible and accountable		
Control options are unclear	Flexible control options	Easiness
Individual users have the freedom to choose different options		
Default settings should be turned off to collect data		
Consumers give up all their information because they want to access services quickly and completing the process of setting controls is complex		
Firms should obtain permission or consent if improvements or changes in their privacy management are enforced (i.e., consent provisions)	Explicit consent options	
No one should have the right to collect information without user consent		
Seeking explicit consent from anyone who signs up		
By using the service, the users have consented		
Inform users about the advertisements used to target them		
Firms should only use the information if the individual authorized it		
Information withdrawal should always be transparent and available	Data-removal options	Agency
The choice to delete any information relevant to users should be freely available		
The ability to remove information (e.g., wiping user data from the servers)		
Providing options in the settings to delete data		
The user should have access to manage the setting of what data to share	Data-access options	
The user should have access to manage with whom data can be shared		
Firms access to user data means they can do whatever they want with the data		

Appendix G. Strategic approaches to communicating the value of transparency and control

First order code	**Second order code**	**Themes**
The government strengthens the overall ecosystem by enforcing data privacy laws	Government/regulator enforcement of data privacy and protection laws	Assurance value
Governments should assure consumers that firms are transparent about their agreements and contracts		
Regulators should ensure that there are no grey areas in privacy laws		
Firms should be held answerable for reselling data	Compliance with industry-specific best practices	
Firms should comply with industry-specific policies		
Firms should ensure that they comply with regulatory guidelines		
Firms should ensure that they use the best industry privacy practices		
Firms should ensure that they follow security recommendations to mitigate risk		
The uniqueness of a user's device can help firms protect against security vulnerability	Hardware and physical security measures	Technical value
Firms can manufacture hardware that protects consumer privacy		
Firms should ensure that physical measures are deployed (e.g., using encrypted hardware, denying access to laptops)		
Firms should save data only in their own computers and servers (not in clouds, shared servers, or rented servers)		
Firms should ensure effective assessments of data management	Firms' internal data management system	
Firms should strengthen internal management by reducing the number of employees with access to user data		
Firms should have stringent controls on their internal network		
Firms ensure the reporting process for data management is short, and closed-loop management is in place		
Firms need to have a complete technological infrastructure including proactive and reactive controls		
Firms are expected to be both legally and ethically correct	Ethical competence	Social value
Firms need to be ethical while collecting data		
Firms should be mindful of their potential impact on people's mental well-being	Impact on consumer well-being	
Firms should not use data to influence users' views and decision-making		
Firms should collect data to provide a better user experience	Personalization	Functional value
Firms should learn about consumers' preferences to provide more personalized services		
Firms should adjust marketing interactions with users according to users' needs		
Firms' personalized services save users a lot of time		