Influence of Firm’s Recovery Endeavors upon Privacy Breach on Online Customer Behavior

BEN C.F. CHOI, SUNG S. KIM, AND ZHENHUI (JACK) JIANG

BEN C.F. CHOI (chun.choi@unsw.edu.au; corresponding author) is a lecturer in information systems, technology and management at the UNSW Business School, Australia. He received his Ph.D. in information systems from the National University of Singapore. His research interests focus on information privacy, social media, and mobile applications. His research has been published in Information Systems Research and the proceedings of the International Conference on Information Systems.

SUNG S. KIM is an associate professor of operations and information management in the Wisconsin School of Business at the University of Wisconsin-Madison. He holds a Ph.D. in information technology management from the Georgia Institute of Technology. His research focuses on automaticity in IT use, online consumer behavior, information privacy, and philosophical and methodological issues. His work has appeared in Management Science, Information Systems Research, Journal of Management Information Systems, MIS Quarterly, Journal of the Association for Information Systems, and Decision Sciences.

ZHENHUI (JACK) JIANG is an associate professor in the Department of Information Systems of National University of Singapore (NUS) and a senior investigator at NUS (Suzhou) Research Institute. His research interests include the design and evaluation of social media, electronic commerce, human computer interaction, and information privacy. His work has been published in Information Systems Research, Journal of Management Information Systems, MIS Quarterly, and the proceedings of Human–Computer Interaction conferences. He has served on the editorial board of MIS Quarterly, IEEE Transactions of Engineering Management, and Journal of AIS, among others.

ABSTRACT: The soaring number of privacy breaches has prompted affected firms to learn how to effectively recover damaged customer relationships. In this study we develop and test a model that explains how online customer behavior is influenced by a firm’s recovery endeavors when privacy breaches occur. Drawing on a service recovery perspective, we integrate the notions of justice perceptions and psychological responses into a theoretical framework. The proposed model was tested against data collected from 1,007 online customers based on a hypothetical scenario. Results show that three types of justice perceptions, distributive, procedural, and interactional justice, jointly affect psychological responses—that is, perceived breach and feelings of violation. In addition, psychological responses were shown to be important in shaping postincident outcomes such as post-word of mouth and post-
likelihood of switching. The study gives researchers and practitioners a useful conceptual tool for analyzing the effectiveness of organizational practices in recovering customer relationship after privacy breaches.

**KEY WORDS AND PHRASES**: online customer behavior, privacy, privacy breaches, psychological responses, security, structural equation modeling.

In recent years, privacy breaches—the theft, loss, or other forms of compromise of personally identifiable information such as credit card and Social Security numbers—have soared in the United States. According to the Identity Theft Resource Center [11], approximately 700 breaches are publicly reported annually in the United States. A more sobering piece of news is that the number of publicized breaches is thought to be considerably lower than that of actual breaches [31]. Undoubtedly, this unfortunate trend endangers the information privacy of customers and, at the same time, threatens the profitability and reputations of businesses. Several high-profile privacy breaches clearly illustrate these threats to practitioners. For example, Sony’s PlayStation Network was hacked in 2011, and this incident was believed to affect 77 million user accounts [61]. As a result of a class action lawsuit, the users of PlayStation Network were offered free digital rewards (e.g., games), and the victims of identity theft could claim reimbursement up to $2,500 [74]. The costs associated with the data breach were reported to exceed $171 million [57]. Meanwhile, the computer system at Target Corporation, a major American retailing company, was hacked in 2013, and because of the incident, nearly 70 million customer records were compromised [1, 46]. Target announced that the costs associated with the data breach exceeded $160 million. On the whole, a privacy breach is highly likely to hurt the performance of a firm.

Privacy breaches can occur for a variety of reasons that include not only software attacks such as denial-of-service, backdoors, and cracking passwords, but also human error, forces of nature, and phishing [78, 80]. Although firms may implement various organizational and technical measures to prevent privacy breaches [35, 40], customers’ data may nevertheless leak through unforeseen holes [60]. Thus, managers should be well prepared for such a disaster so that their business can return to normal as quickly as possible. Identifying and addressing technical problems that may prevent a privacy breach can be complex and may require a significant amount of time, money, and effort. Nevertheless, it is an equal challenge to repair the damaged relationships with customers after a breach [4, 60]. Given that reputation is one of the most valuable assets in a networked economy, firms cannot afford to underestimate the potential magnitude of damage that a privacy breach poses to customer referrals in the form of word of mouth [73]. Moreover, firms should take appropriate steps to keep their customers from switching to competitors after a disaster, because in this digital economy, customer loyalty can be easily lost [63]. To mitigate the potentially disastrous consequences of a data breach for customer relationships, firms have recourse to numerous recovery tactics. These include, but
are not limited to, providing financial compensation for the privacy damages, establishing channels of clarification to permit effective customer feedback, and apologizing for the service failure [78]. Yet little is known about the effectiveness of these organizational measures in regulating word of mouth and likelihood of switching, which are the metrics critical to gauging the quality of customer relationships.

Information systems (IS) research has progressed significantly in expanding our understanding of online customers’ predispositions, beliefs, attitudes, and behavior in relation to information privacy [70]. Earlier studies on these topics focused on identifying the nature of concern for information privacy in the context of direct marketing [18]. Subsequently, Malhotra et al. [50] developed a scale of information privacy concerns specific to the Internet context. IS researchers also have tried to identify the impact of privacy concerns on customer behaviors, such as willingness to release personal information, identity misrepresentation, relationship termination, word of mouth, and complaints [22, 60, 70]. In addition to privacy concerns, some researchers have begun to examine various implications of data breaches [50, 68]. For example, Malhotra and Malhotra [48] studied the impact of breach incidents on market value of firms. They found that market value depreciation occurred even long after the event of a breach incident. Meanwhile, Sen and Borle [68] assessed the risk of data breach in terms of several criteria including an organization’s physical location and industry type. Their findings indicate that investment in IT security actually increased the risk of data breach incidents probably because the investment was not spent in an effective manner.

Their findings indicate that the investment in IT security is positively associated with the risk of data breach incidents. This is probably because (1) the investment in IT security is the result of high risk of a data breach incident or (2) the investment was not spent in an effective manner. Recently, Bansal and Zahedi [4] examined how organizational responses to a data breach help repair damaged customer trust. They showed that apology was generally more effective than no response or denial in repairing trust. The study by Bansal and Zahedi [4] is one of the first studies to show the role of organizational responses to a data breach in maintaining customer relationships. Despite a few pioneering efforts, researchers still lack a systematic foundation for understanding the effectiveness of organizational remedies to a breach in managing online customer behavior such as word of mouth and likelihood of switching [60, 70].

The objective of this study is to enrich the IS literature by developing and testing a model that explains online customer behavior after privacy breach recovery, that is, an online firm’s postincident responses to a breach incident in order to mitigate the impact of the breach.1 The overarching theory in this study is drawn from a service recovery perspective, which posits that customers’ specific beliefs with regard to organizational remedies determine overall psychological evaluations, which in turn regulate behavior [32, 52, 69]. In particular, the theory of justice is used as a theoretical basis in identifying consumers’ specific beliefs associated with the key attributes of privacy breach remedies [18, 55]. This justice theory suggests that
people evaluate privacy-related issues in terms of three criteria, namely, distributive justice, procedural justice, and interactional justice [19, 50]. According to the service recovery perspective, these justice factors have constantly been shown to be salient in the context of information privacy [70]. Thus, we argue that these three types of justice perceptions can reasonably indicate the specific criteria that online customers employ in assessing organizational endeavor undertaken to remedy a breach incident.

Meanwhile, we borrow the concept of psychological response evaluation from a psychological contract perspective to represent general thoughts and feelings relevant to the context of information privacy. Specifically, this psychological contract perspective suggests that individuals’ overall psychological evaluations are summarized into cognitive and emotional factors, which are represented by, respectively, (1) perceived breach, which refers to an overall cognitive judgment that an online firm has failed to fulfill obligations related to how to handle personal information and how to respond to a breach incident, and (2) feelings of violation, which are defined as the emotional state of betrayal or distress that a customer feels toward a vendor after privacy breach recovery [58, 59, 65]. Furthermore, considerable research shows that these psychological responses are affected by various types of justice perceptions and their interactions [23, 47]. Thus, we propose not only main effects of justice perceptions but also their interaction effects on perceived breach and feelings of violation. Our model posits that, consistent with the service recovery perspective, online customers’ psychological responses (i.e., general thoughts and feelings) regulate postincident outcomes that include word of mouth and likelihood of switching.

Our theoretical framework is intended to make several contributions to the information privacy literature. First, we attempt to extend justice theories by including psychological responses as mediating variables between justice perceptions and postincident outcomes. Second, our conceptual model includes various interaction effects in addition to the simple linear relationships between justice perceptions and psychological responses. Finally, we differentiate perceived breach, which represents a cognitive response, from feelings of violation, which indicate an emotional response. Overall, our model is expected to contribute significantly to the body of knowledge relating to online customer behavior after privacy breach recovery; moreover, the findings of this study will help managers develop effective organizational practices to retain desirable customer relationships after an incident.

Literature Review

Online Privacy Breach and Organizational Remedies

An online privacy breach refers to an online firm’s failure to protect personal information. It occurs when there is unauthorized access to or collection, use, disclosure, or disposal of personal information. Prior studies have identified several
common types of intentional privacy breaches, including insider disclosure or theft, selling personal data to third parties, or sharing information with third parties [13, 64]. In contrast, our study deals with nonintentional privacy breach, which, for example, includes hacking and virus attacks from outsiders [4]. We thereafter use privacy breach to refer to nonintentional privacy breach. Although online privacy breaches share some features with privacy breaches in traditional retailing, they also exhibit significant differences. For example, the spread of privacy breach damage is much faster and wider in the context of online privacy breach as compared to the traditional context. In addition, the ease of copying personal information implies that the damages of an online privacy breach may unfold over a long window because personal information can be persistent as well as easily reproduced and reused in the online environment [50].

Given that a privacy breach endangers customers’ privacy, online firms are typically expected to uphold their responsibilities in implementing sound technical, structural, and procedural improvements to minimize the possibility of privacy breaches [60]. In order to reduce negative consequences, firms need to react effectively to a privacy breach so as to mitigate and recover from its consequences. However, in most cases, attempts to recover from privacy breach in an online context is rather challenging as the interaction between an online firm and its customers does not involve face-to-face encounters, and is thus less effective in the context of service recovery [53]. Hence, it is necessary to consider the specificity of the online privacy context in examining the effectiveness of organizational remedies after a breach.

The Service Recovery Perspective

The service recovery literature offers a theoretical perspective for understanding customer behavior in response to organizational recovery efforts after an online privacy breach. Specifically, the literature posits that customers’ specific beliefs with regard to organizational remedies determine their overall psychological evaluations of these measures [32, 52, 69]. Central to this argument is the idea that customers’ judgment of a firm arises from their specific assessment of the key attributes of the firm’s service recovery effort [72]. A growing volume of empirical evidence supports this perspective. For instance, in a study on service recovery encounters, Schoefer and Ennew [67] paid special attention to customers’ beliefs associated with financial compensation, waiting time, and service agent interactions. Their results suggested that customers’ overall appraisal of the travel company was the consequence of their specific beliefs.

Furthermore, according to the service recovery perspective, customer behaviors are the salient consequences of their overall psychological evaluations of a firm’s endeavor in remedying a service failure [52]. The main thrust of past research in examining organizational remedies has been to focus on how customers adjust their behavior in accordance with their overall judgments of firms after service recovery
In a study examining service recovery in restaurants and hotels, DeWitt et al. [20] showed that customers’ continued patronage depended on their postrecovery appraisal of the firm. Likewise, Kau and Loh [38] revealed that mobile users’ overall satisfaction after service recovery was an important driver of recommendation behavior.

In essence, the service recovery perspective highlights the importance of customers’ overall psychological evaluations in influencing their behavior after a service failure, that is, data breach in this study; moreover, their overall psychological evaluations are the summary of customers’ specific beliefs with regard to organizational remedies in response to the failure.

The Theory of Justice

A theoretical model for online privacy breach recovery needs to take into account factors that circumscribe the remedies undertaken by online firms. These factors are rooted in specific compensation, redress procedures, and explanations. The service recovery perspective suggests that the justice framework may serve as a useful starting point for looking at customers’ specific beliefs with regard to privacy breach remedies [32, 52, 69]. Justice (also often referred to as fairness) is indicative of how fairly an individual is treated by another individual or by an organization [17, 18, 55]. It is viewed as a key principle in a variety of social exchange relationships [17, 72]. Unsurprisingly, a growing number of researchers have been studying the concept of justice to explain individuals’ behavior in the context of information privacy [2, 4, 60]. A consistent finding of these justice-based privacy studies is that individuals’ perceptions about the fairness of a particular privacy situation affect how these individuals actually react to the situation under investigation. In general, we believe that this justice perspective provides a valuable framework for examining how people react to the recovery tactics undertaken by online firms after a privacy breach.

The justice framework identifies three types of justice, namely, distributive, procedural, and interactional, all of which are particularly relevant in privacy breach recovery [17, 33]. First, distributive justice refers to the perceived fairness of outcomes including allocation of resources that a customer receives from a vendor [51]. Distributive justice is based on the notion of equity, which is the result of a mental comparison of inputs and outputs [26]. Second, procedural justice refers to the perceived fairness of the procedure used in handling a customer’s question or feedback regarding a vendor’s reaction to a breach [75]. Procedural justice differs from distributive justice because procedural justice is concerned with the fairness of the process in handling customer complaints, whereas distributive justice focuses mainly on outcomes [28]. Finally, interactional justice refers to the perceived fairness of the interpersonal treatment with which the procedures are implemented [9]. In particular, procedural justice focuses on formal
procedures, but interactional justice deals with subtleties such as respect, care, and politeness [9].

Prior research has drawn on the justice framework to study recovery tactics after service failure. For instance, Goles et al. [27] examined delivery delay in commercial transactions. They found that when a seller was helpful in resolving the issue, patrons perceived less violation of their expectations and experienced fewer negative emotions compared to when the seller was not helpful. Likewise, in a study on e-service recovery, Collier and Bienstock [16] verified the importance of justice in recovering from damaged shipments and found that by ensuring distributive justice, procedural justice, and interactional justice, customers were more satisfied and happier with their online purchase experience. Overall, past studies show that the justice framework forms a relevant theoretical basis for identifying the key attributes of organizational remedies after a service failure.

Psychological Contract

The service recovery perspective theorizes that customers’ specific beliefs with regard to organizational remedies determine their overall psychological evaluations of firms [32, 52, 69]. Whereas the justice perspective sheds light on the development of specific beliefs associated with the organizational remedies, the notion of psychological responses helps in understanding customers’ overall psychological evaluations of remedy strategies after privacy breach recovery. Specifically, the psychological contract perspective posits that social exchange partners establish a contract, which can be developed explicitly or implicitly, to delineate obligations between partners in the exchange [58, 65].

Violation of a psychological contract occurs when an exchange partner fails to uphold its obligations. To illustrate, in online shopping, customers generally expect an online retailer to deliver a functional product within a stated period. If the firm fails to do so, customers may feel psychologically betrayed by the firm [60]. Similarly, a firm is expected to apologize and to compensate customers accordingly when the firm cannot safeguard customers’ personal information. Consequently, when an online firm fails to properly respond to a privacy breach incident in terms of compensation, procedures, and politeness, customers are likely to think the firm has violated a psychological contract because it not only is incompetent in safeguarding customer information but also is unable to remedy the problem.

According to the psychological contract perspective, when a contract is not honored, individuals react psychologically with cognitive and emotional responses [58, 65]. A cognitive response occurs as a result of a deliberate calculation of whether the firm’s treatment meets or falls short of the psychological contract. The service recovery literature suggests that a cognitive response is predominately shaped by compensation adequacy and procedural fairness. Although adequate compensation ensures equity in offsetting damages associated with the privacy breach, fair procedures assure a formal process that leads to an equitable outcome.
In contrast, an emotional response transcends a mere cognitive appraisal of an event and relates instead to feelings of distress associated with the firm’s lack of faithfulness and oversight [67]. Past research that examined service recovery suggests that an emotional response can be especially sensitive to reparation and interpersonal treatment. Inadequate reparation not only contributes to customers’ perceptions of a breach of the psychological contract but also triggers feelings of contract violation [29]. Poor interpersonal treatment is experienced when customers undergo bad social interactions, such as personal slights, demeaning offenses, or disrespectful actions, which are known to arouse a sense of violation [5]. In the literature, these cognitive and emotional dimensions are represented, respectively, by perceived breach and feelings of violation [58, 65]. Perceived breach indicates a cognitive judgment concerning the extent of a firm’s deviation from an expected obligation, whereas feelings of violation represent an emotional reaction to such a violation. The two constructs represent essentially distinct properties of psychological responses. Thus, it is important to take into account both factors for a better explanation of individuals’ reactions to a firm’s recovery efforts in addressing a breach incident. In sum, used as the overarching framework in this study, the service recovery literature postulates that customers’ specific justice perceptions with regard to organizational remedies determine overall psychological evaluations, which are summarized into perceived breach and feelings of violation. Furthermore, the literature suggests that customers’ overall psychological evaluations, in turn, regulate their behavior after service recovery.

Research Model and Hypotheses

By drawing on the service recovery perspective, we proposed our conceptual model, which is presented in Figure 1. In the model, preincident outcomes represent online customer behavior before a breach incident, whereas justice perceptions, psychological responses, and postincident outcomes reflect customers’ perceptions and behavior in relation to a firm’s recovery efforts upon a privacy breach. In general, the model shows that customers’ justice perceptions as specific beliefs determine psychological responses as overall evaluations, which in turn, influence postincident outcomes. We first develop research hypotheses concerning the relationships between justice perceptions and psychological responses (H1–H3). Subsequently, we offer theoretical explanations of the impact of the interaction between justice perceptions on psychological responses (H4–H5). Finally, we hypothesize the effects that psychological responses have on postincident outcomes (H6–H7).

Justice Perceptions and Psychological Reactions

Distributive justice is especially important in reducing perceived breach of psychological contract in online privacy breach recovery. In the online environment, to complete commercial transactions, customers are typically required to provide
personal information to online firms with which they often lack a history of interpersonal relations [60]. As a result, customers in general expect that an online firm will attempt, to a greater or lesser extent, to safeguard their information. A privacy breach essentially challenges customers’ cost assessment by exposing them to unforeseen damages such as identity theft and credit card fraud. Although many are dissatisfied by the unexpected privacy loss, customers are likely to react less negatively when the online firm, despite the lack of interpersonal relationships, ensures distributive justice in privacy breach recovery [33]. In the context of information privacy, people have been shown to be willing to reveal their personal information in exchange of economic compensation [70, 81]. These findings imply

Figure 1. Proposed Model
that distributive justice could play a certain role in mitigating the negative consequences of a data breach incident on an online firm.

Distributive justice is often maintained through the provision of financial compensation, such as vouchers, discounts, and free credit monitoring [39, 79]. In online privacy breach recovery, adequate financial compensation is particularly important because it can restore the balance of personal information exchange [44]. Indeed, recent IS studies offer empirical evidence that financial compensation is particularly important in shaping customers’ cognitive response to privacy issues in the online environment. For instance, in a study on location-based services, Xu et al. [81] revealed that distributive justice addressed users’ negative perceptions associated with the exposure of locality information to online companies. In essence, by compensating for the costs inflicted by a privacy breach, distributive justice restores equity in online transactions and hence alleviates customers’ negative perceptions toward the breach of psychological contract. Thus, we hypothesize that perceived breach will decrease (increase) as distributive justice increases (decreases).

**Hypothesis 1a:** Distributive justice will be related negatively to perceived breach.

The appraisal-tendency framework posits that negative emotions arise from individuals’ appraisal of responsibility for negative events [43]. Especially when others are responsible for the negative events, individuals experience negative emotions, such as anger, dejection, and agitation. Similarly, customers often experience strong negative emotions in online privacy breaches. This is because when customers provide personal information in online transactions, they generally expect the online firms to be responsible in properly managing their information [76]. As a result, in recovery from an online privacy breach, customers’ appraisal of a firm’s responsibility for the privacy loss arouses negative emotions.

Distributive justice is especially important in addressing customers’ feelings of violation in online privacy breach recovery. Given the lack of personal relationships in online commercial transactions, customers may be highly anxious about the firm’s commitment to safeguarding their privacy. By ensuring distributive justice, customers could ascertain the online firm’s faithfulness in upholding its responsibility in the recovery and hence reduce their feelings of displeasure or hostility. Furthermore, distributive justice helps ensure adequate reparation, which is a key remedy for customers’ emotional feelings triggered by online privacy breaches. Evidence suggests that distributive justice is of particular importance to customers’ emotional responses about online privacy issues. For instance, Hann et al. [30] found that financial compensations reduced customers’ feelings of insecurity and vulnerability that stemmed from online privacy failures. Thus, we hypothesize that feelings of violation will decrease (increase) as distributive justice increases (decreases).

**Hypothesis 1b:** Distributive justice will be related negatively to feelings of violation.
Although compensation may not satisfy all victims of a privacy breach, these victims often want to ensure that procedural justice is maintained in service recovery—that is, to ensure that the process in which they are compensated is consistent, fair, and reasonable. According to the psychological contract perspective, customers’ cognitive response (i.e., perceived breach) is predominantly determined by the outcome and the procedure that leads to the outcome [58]. In particular, the theory of justice suggests that when customers perceive a high degree of fairness in the outcome allocation procedure, they believe outcome equity is ensued [10]. Because a fair procedure helps ensure equity restoration, procedural justice is likely to have a prominent effect on cognitive response. Indeed, past research suggests that procedural justice in online service recovery is especially important in evoking a cognitive response because service representatives and customers usually do not physically meet each other [33]. Since customers are separated from the actual recovery process in the online environment, they often have limited access to the procedures this process entails. Consequently, customers may be forced to rely entirely on the firm’s website to learn about the recovery policies. Difficulty in obtaining information through the firm’s website leads customers to question the justice of service recovery procedures and intensifies their dissatisfaction with the firm [15].

Research has shown that procedural justice ranks among the most essential practices that online companies can use to placate customers whose privacy is at risk (e.g., [16]). In online privacy breach recovery, procedural justice manifests in terms of organizational mechanisms through which customers can be informed about the recovery process, such as how the privacy breach was identified, what information was leaked, and what safeguards are in place to resolve the privacy failure. A high degree of procedural justice helps overcome the lack of physical interaction by increasing the transparency of privacy breach recovery procedures and assuring customers about the firm’s fair practices in addressing privacy issues [19]. As a result, when customers perceive a high degree of procedural justice in privacy breach recovery, they conclude that the online firm is taking steps to ensure equity in the recovery. Thus, in online privacy recovery, it is reasonable to expect that fair procedures (e.g., thorough descriptions of the decision-making processes) reduce customers’ perceived breach of a psychological contract. Therefore,

**Hypothesis 2: Procedural justice will be related negatively to perceived breach.**

The psychological contract perspective posits that the personal interaction process individuals experience plays a prevailing role in shaping emotional responses [58]. According to this perspective, feelings of violation are particularly sensitive to negative social experience and hence do not require deliberate reflection. Similarly, in the service recovery context, ample evidence suggests that interactional justice plays a key role in shaping customers’ emotional reactions associated with service recovery. For example, Chebat and Slusarczyk [12] surveyed bank customers on their service recovery experience and found that their negative emotions could be reduced when they received respectful and pleasant treatment from bank staffs.
The effects of interactional justice on emotions are particularly evident in recovery endeavor from an online privacy breach. This is because an online privacy breach not only entails explicit damage, such as financial loss and wasted time, but also engenders immense negative emotions, such as anger, hurt, and frustration. Furthermore, given the lack of established interpersonal relationships, customers are especially likely to feel disregarded by the online firm and develop negative feelings [6]. Lack of apologies not only worsens customers’ distress but also makes them doubt the online firm’s sincerity in accepting responsibility [33]. In essence, when an online business does not handle privacy breach recovery with high interactional justice, customers are likely to experience negative emotions. Therefore, we propose that interactional justice is negatively related to feelings of violation.

Hypothesis 3: Interactional justice will be related negatively to feelings of violation.

Interactions Between Justice Perceptions

Referent cognitions theory (RCT) offers an explanation for the joint effect of distributive justice and procedural justice on subsequent cognitive reactions [23]. Specifically, this theory states that individuals tend to evaluate outcomes (i.e., distributive justice) based on whether fair procedures are followed (i.e., procedural justice). When people have a high opinion of the fairness of the procedures followed, they would be less sensitive to outcome equity in service recovery. However, if they perceive the procedures as unfair, they are more likely to focus on attaining an equitable outcome. Thus, according to RCT, the question of whether fair procedures were faithfully followed moderates the way people cognitively evaluate outcome equity. In particular, RCT predicts that when procedural justice is ranked higher, the effect of distributive justice on cognitive response becomes weaker; in contrast, when procedural justice is ranked lower, its effect becomes stronger.

RCT is considered as an informative perspective in explaining individual behavior in recovery from an online privacy breach. Whereas relationships in traditional business settings are predominantly built through personal interaction, they are typically maintained online with little person-to-person contact. Indeed, customers often interact with an online firm through self-service technology. Thus, in the absence of direct contact, procedural justice is considered the actual reflection of the online firm’s compliance with principles of fair information practice (FIP) [19]. When procedural justice is high, customers can be assured that the online firm has followed the industry guidelines and privacy laws in providing equitable compensation, thereby reducing their sensitivity toward distributive justice. However, when procedural justice is amiss, equitable compensation for the firm’s negligence cannot be guaranteed; hence, customers’ sensitivity toward distributive justice is likely heightened. Taken together, in the domain of online privacy breach recovery, customers who are satisfied with organizational procedures tend to perceive the
monetary reward as acceptable; therefore, procedural justice could complement distributive justice in affecting perceived breach. Thus,

**Hypothesis 4:** The relationship between distributive justice and perceived breach will decrease (increase) as procedural justice increases (decreases).

The cognitive appraisal model of emotion holds that the effect of outcome appraisal on emotions is moderated by the judgment of the outcome allocation experience \[54\]. According to the model, an individual’s emotional response begins with an appraisal of an outcome as either harmful or beneficial \[77\]. Essentially, when the outcome is undesirable, negative emotions emanate. This outcome appraisal is coupled with an experience appraisal, which involves an evaluation of the way individuals are treated in the course of receiving the outcome \[77\]. In online privacy breach recovery, when interactional justice is high, customers would find the service representative sincere and helpful in addressing the privacy failure incident. As the service representative represents the online firm in privacy recovery, customers would be assured that the firm is accepting its responsibility, and hence their emotional response will be less aroused by distributive justice. By contrast, when interactional justice is low, customers would find the service representative disrespectful and lacking empathy. Consequently, they might become especially angry that the online firm is not accepting its responsibility. In such a case, they are more likely to consider the firm irresponsible and thus increase the impact of distributive justice in arousing feelings of violation. Thus,

**Hypothesis 5:** The relationship between distributive justice and feelings of violation will decrease (increase) as interactional justice increases (decreases).

We proposed earlier that procedural justice and interactional justice reflect different aspects of justice perceptions, and thus their effects on psychological responses would be systematically different (i.e., H2 and H3). Similarly, we argued that because of the difference between procedural justice and interactional justice, their moderating effects would be clearly distinct (i.e., H4 and H5). It would be interesting to examine whether procedural justice and interactional justice really have differential effects on perceived justice and feelings of violation.

**Determinants of Postincident Outcomes**

Customer behavior takes on a myriad of forms such as repurchases, payment of a premium, and interest in alternatives \[8, 21\]. Nevertheless, two behavioral outcomes, namely, word of mouth and likelihood of switching, have been the focus of attention among researchers and practitioners \[83\].

Word of mouth refers to the extent to which an individual intends to recommend, or say positive things about, a service to others \[71\]. Serving as a reference is risky because it involves the potential of tarnishing the social image or credibility of the person making the reference. Thus, a referral represents the ultimate form of a
customer’s dedication to a firm. In this regard, research shows that word of mouth—which represents a customer’s willingness to recommend a firm’s product or service to others—is a more powerful predictor of a firm’s revenue growth than customer loyalty, customer satisfaction, or intent to repurchase [62]. Moreover, the significance of word of mouth is being amplified in the Internet age because opinions spread freely with few barriers of time, space, or socioeconomic status. A number of IS studies have been conducted to explain individuals’ willingness to recommend within the context of online business (e.g., [70]). Furthermore, word of mouth has been the focus of much information privacy research designed to gauge the effect of privacy perceptions on customer behavior. In particular, Culnan and Williams [60] argued that service providers were essentially in “the reputation business,” and thus it was important for them to cultivate “a culture of privacy” (p. 683). Therefore, it is important to examine the determinants of word of mouth for a better understanding of online customers’ reactions to privacy breach recovery.

Likelihood of switching is defined as the extent to which a customer intends to leave his or her current vendor [56]. Acquiring a new customer is expensive because of “one-time” activities such as advertising, promotions, account setup, and so on [63]. A firm loses the opportunity to maximize the return from the initial investment if the new customer defects without subsequent transactions. Customer retention is said to be one of the most critical factors affecting the bottom line of a business. Thus, it is important for an online firm to understand the mechanism that keeps a customer from switching to an alternative vendor.

As shown in Figure 1, two types of postincident outcomes are examined in this study, namely, post-word of mouth and post-likelihood of switching. In this study, post-word of mouth refers to the level of word-of-mouth activity after a firm’s service recovery attempt. Similarly, post-likelihood of switching refers to the likelihood of switching after a firm’s service recovery endeavors. Although preincident outcomes drive postincident outcomes, customer behavior may not remain the same after personal information is compromised [52]. Specifically, our model posits that in the context of online privacy, customers’ overall psychological evaluations of a firm’s recovery practices (i.e., perceived breach and feelings of violation) affect behavioral outcomes (i.e., post-word of mouth and post-likelihood of switching). The service recovery literature suggests that in online service failures and recovery settings, customer behaviors are mainly a function of customers’ overall psychological evaluations of recovery practices [32, 52]. This is because in the online context, customers rarely have human contact with an online firm, and the lack of personal interaction makes it difficult for them to build a close relational bond. As a result, customers tend to base their behavioral decisions on their overall psychological evaluations—that is, perceived breach and feelings of violation—instead of on other long-term relational considerations.

Based on this rationale, we expect perceived breach to affect both post-word of mouth and post-likelihood of switching after privacy breach recovery. Past research has clearly demonstrated the impact of perceived breach on customer behavior. For
instance, in the context of online privacy, Poddar et al. [60] found that because online exchanges lack physical contact, online customer behavior in the presence of a privacy threat is influenced more by what people think about the situation than by their prior relationship with the online vendor. Thus, we hypothesize that in a situation in which an online firm attempts to recover from a breach incident, perceived breach will affect customer behaviors such as post-word of mouth and post-likelihood of switching.

Hypothesis 6a: Perceived breach will be negatively related to post-word of mouth.

Hypothesis 6b: Perceived breach will be positively related to post-likelihood of switching.

Empirical evidence suggests the important role of feelings of violation on online customer behavior in the context of information privacy. For example, Son and Kim [70] showed that individuals’ feelings toward information privacy drive information privacy-protective actions (e.g., refusal, negative word of mouth, complaints). Along the same line, Youn [82] found that affective components affect privacy protection behaviors (e.g., confrontation and avoidance). Thus, it is reasonable to argue that emotional responses to privacy breach recovery affect whether online customers say positive things to others and whether they eventually switch to an alternative vendor.

Hypothesis 7a: Feelings of violation will be negatively related to post-word of mouth.

Hypothesis 7b: Feelings of violation will be positively related to post-likelihood of switching.

Research Methodology

Research Setting

This research employed a scenario-based experiment that integrates the characteristics of field surveys and lab experiments [49]. Specifically, we used a survey questionnaire to measure customers’ perceptions about an actual store while manipulating their treatment through hypothetical scenarios. In this study, subjects were given a web-based survey questionnaire. In the questionnaire, the subjects were first asked to indicate the name of an online vendor they had used in the past year. If a subject had not used an online vendor in the past year, that person was excluded from further consideration. The questionnaire then asked the remaining subjects to express their perceptions about the online vendor. In particular, we measured control variables such as perceived usefulness, perceived ease of use, trusting beliefs, risk beliefs, loyalty, switching costs, pre-word of mouth and pre-likelihood of switching.
After measuring the subjects’ perceptions of the online vendor, we randomly presented one of the eight scenarios to each of the subjects. The scenarios asked the subjects to imagine that they had just received an e-mail from the online vendor that they had named earlier. The message of the e-mail was that hackers had stolen their credit card information. The e-mail message contained a description of the specific remedial steps taken by the online vendor. These steps addressed three categories of justice: distributive, procedural, and interactional. For each category of justice, we developed high and low conditions. Thus, the experimental design is a 2 x 2 x 2 fully crossed between-subjects arrangement. Once a scenario was presented, the subjects were instructed to answer the subsequent questions based on the given scenario. The research variables specific to the scenario were distributive justice, procedural justice, interactional justice, perceived breach, feelings of violation, post-word of mouth, and post-likelihood of switching.

Data Collection

We developed eight different survey questionnaires containing experimental conditions that varied across the three categories of justice (i.e., a 2 x 2 x 2 factorial design). We used a market research firm to collect the data necessary for the main test. A nationwide sample frame of panel members between the ages of thirty and fifty-nine was drawn up. An e-mail invitation—including a link to a web-based survey questionnaire with one of the eight case scenarios—was sent to 6,539 U.S.-based members who had been randomly selected from the panel pool. Subjects were notified that participation was voluntary and that only aggregate data that contained no personally identifiable information would be used. The Web-based survey ran for two weeks, and we collected 1,036 responses, representing a complete response rate of 15.8 percent. However, 29 responses were not usable because they did not meet the age criterion. As a result, a total of 1,007 usable responses were considered for data analysis, which yielded an effective response rate of 15.4 percent. The average age of subjects was forty-eight, and 55 percent were female. No significant differences existed between the eight groups in terms of age and gender (ps > 0.05). We compared the profiles of both respondents and nonrespondents in terms of age and gender and found no statistically significant differences between the two groups (ps > 0.05).

Measures and Scenarios

To measure the research variables, we adapted existing scales for which psychometric properties are established in the literature (see online Appendix A for measurement items and scenarios). These measures were grouped into three parts in the survey questionnaire—Parts A, B, and C. Part A measures individuals’ perceptions about an online vendor. These measures were not specific to any scenarios. In Part B, one of the eight scenarios was presented, and then the
subsequent measures were designed to be specific to the particular scenario. Finally, Part C included measures such as demographic characteristics and other general items that are not specific to a scenario (see online Appendix B for questionnaire development).

Data Analysis and Results

Measurement Model

We used six different fit indices to evaluate model fit: the comparative fit index (CFI), the nonnormed fit index (NNFI), the root mean square error of approximation (RMSEA), and the standardized root mean square residual (SRMR), the goodness-of-fit index (GFI), and the adjusted goodness of fit (AGFI). According to the literature, the fit indices criteria for an acceptable model are: CFI $\geq 0.95$, NNFI $\geq 0.95$, RMSEA $\leq 0.06$, SRMR $\leq 0.08$; GFI $\geq 0.90$, and AGFI $\geq 0.80$ [7, 25, 34]. Our measurement model included 15 multi-item factors with 47 corresponding indicators. In addition to the multi-item factors, the model included four one-item variables such as age, gender, experience, and website usage. The results of CFA showed that the measurement model was a highly satisfactory fit for the data: $\chi^2 (1,057) = 2,059.67$, $p < 0.001$, CFI = 0.99, NNFI = 0.99, RMSEA = 0.031, SRMR = 0.021, GFI = 0.93, AGFI = 0.91. Table 2 shows the means, standard deviations, composite reliability (CR), average variance extracted (AVE), and correlations of the measures based on the measurement model.

Besides model fit, we checked the convergent validity of the scales. Convergent validity is considered satisfactory if the factor loading of an indicator is 0.60 or higher [14]. We inspected the output of LISREL 8 and found that among the indicators examined, the lowest loading was 0.68. This result indicated an acceptable convergent validity for the measures. Subsequently, we examined the discriminant validity of the scales. Specifically, as a way to check whether two scales were empirically differentiable, we performed a chi-square difference test for each pair of factors [3]. The results of the chi-square difference tests indicated that none of the pairs was considered statistically the same, which supported discriminant validity. In addition to convergent and discriminant validity, we also evaluated the reliability of the scales. The reliability of the scales was examined through two criteria, namely, CR and AVE. Reliability is said to be acceptable when CR $\geq 0.70$ and AVE $\geq 0.50$ [3, 24]. As Table 2 shows, the minimum CR and AVE values, respectively, are 0.86 and 0.67, indicating acceptable reliability of the scales.4

Test of Proposed and Alternative Models

To test the proposed model, we used a structural equation modeling (SEM) tool, LISREL 8. In the structural model, justice perceptions and control variables (i.e., age, gender, website experience, website usage, perceived usefulness, perceived ease
Table 2. Properties of Measurement Scales

|      | ME  | SD  | CR  | AVE | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   | 10  | 11  | 12  | 13  | 14  | 15  | 16  | 17  | 18  | 19  |
|------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1. AGE | 48.41 | 6.90 | na  | na  | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 2. GEN | 1.55 | 0.50 | na  | na  | NA  | -0.07 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 3. EXP | 5.63 | 3.71 | na  | na  | NA  | -0.02 | -0.07 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 4. WU | 5.16 | 1.68 | na  | na  | NA  | -0.02 | -0.03 | -0.30 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 5. PU | 5.01 | 1.43 | 0.94 | 0.84 | NA  | 0.00  | 0.03  | 0.04  | 0.35  | 0.37 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 6. PE | 5.98 | 1.03 | 0.96 | 0.67 | NA  | -0.03 | -0.30 | -0.33 | -0.37 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 7. TRUST | 5.89 | 1.06 | 0.93 | 0.78 | NA  | -0.07 | -0.02 | -0.02 | -0.32 | -0.39 | -0.62 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 8. RISK | 2.47 | 1.45 | 0.94 | 0.84 | NA  | -0.16 | -0.01 | -0.07 | -0.12 | -0.03 | -0.29 | -0.40 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 9. LOY | 4.87 | 1.57 | 0.95 | 0.86 | NA  | -0.01 | -0.04 | -0.12 | -0.53 | -0.46 | -0.58 | -0.18 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |     |
| 10. SC | 2.96 | 1.62 | 0.92 | 0.79 | NA  | -0.10 | -0.02 | -0.04 | -0.17 | -0.22 | -0.03 | -0.30 | -0.31 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |     |
| 11. WOM | 5.98 | 1.16 | 0.96 | 0.88 | NA  | -0.01 | -0.06 | -0.08 | -0.41 | -0.37 | -0.60 | -0.79 | -0.34 | -0.59 | -0.09 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |
| 12. LOS | 2.85 | 1.47 | 0.92 | 0.79 | NA  | -0.17 | -0.10 | -0.03 | -0.19 | -0.05 | -0.24 | -0.44 | -0.51 | -0.35 | -0.02 | -0.45 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |
| 13. DJ | 2.93 | 1.76 | 0.95 | 0.86 | NA  | -0.04 | -0.06 | -0.02 | -0.13 | -0.15 | -0.02 | -0.11 | -0.09 | -0.17 | -0.14 | -0.06 | -0.09 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |
| 14. PJ | 4.44 | 1.82 | 0.93 | 0.82 | NA  | -0.01 | -0.07 | -0.00 | -0.12 | -0.16 | -0.22 | -0.26 | -0.06 | -0.24 | -0.11 | -0.22 | -0.08 | -0.41 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |
| 15. IJ | 4.73 | 1.72 | 0.97 | 0.90 | NA  | -0.02 | -0.03 | -0.14 | -0.20 | -0.22 | -0.29 | -0.08 | -0.22 | -0.11 | -0.24 | -0.10 | -0.57 | -0.66 | 1.00 |     |     |     |     |     |     |     |     |     |     |     |
| 16. PB | 4.68 | 1.86 | 0.96 | 0.88 | NA  | -0.02 | -0.01 | -0.00 | -0.07 | -0.06 | -0.01 | -0.09 | -0.14 | -0.10 | -0.04 | -0.08 | -0.13 | -0.47 | -0.29 | -0.35 | 1.00 |     |     |     |     |     |     |     |     |     |     |
| 17. PVWOM | 4.70 | 1.78 | 0.94 | 0.84 | NA  | -0.04 | -0.02 | -0.03 | -0.05 | -0.09 | -0.25 | -0.02 | -0.06 | -0.08 | -0.17 | -0.40 | -0.29 | -0.49 | -0.51 | 1.00 |     |     |     |     |     |     |     |     |     |     |
| 18. PLOS | 3.68 | 1.89 | 0.99 | 0.96 | NA  | -0.02 | -0.05 | -0.04 | -0.21 | -0.15 | -0.13 | -0.20 | -0.02 | -0.29 | -0.19 | -0.25 | -0.06 | -0.65 | -0.56 | -0.62 | -0.54 | -0.47 | 1.00 |     |     |     |     |     |     |     |     |
| 19. PWOM | 4.67 | 1.80 | 0.97 | 0.91 | NA  | -0.10 | -0.04 | -0.12 | -0.04 | -0.03 | -0.12 | -0.12 | -0.19 | -0.12 | -0.13 | -0.30 | -0.46 | -0.40 | -0.45 | -0.61 | -0.54 | -0.69 | 1.00 |     |     |     |     |     |     |     |

Notes: n = 1,007; ME = mean; SD = standard deviation; CR = composite reliability; AVE = average variance extracted. AGE = age; GEN = gender; EXP = experience; WU = website usage; PU = perceived usefulness; PEOU = perceived ease of use; TRUST = trusting beliefs; RISK = risk beliefs; LOY = loyalty; SC = switching costs; WOM = pre-word of mouth; LOS = pre-likelihood of switching; DJ = distributive justice; PJ = procedural justice; IJ = interactional justice; PB = perceived breach; FV = feelings of violation; PWOM = post-word of mouth; PLOS = post-likelihood of switching.
of use, trusting beliefs, risk beliefs, loyalty, switching costs, pre-word of mouth, and pre-likelihood of switching) were treated as exogenous variables, whereas psychological reactions and postincident outcomes were specified as endogenous variables. We estimated interaction effects using the means of latent variable scores (MLVS) technique [37] with the residual centering method [41]. It should be noted that the structural errors of the factors that belong to the same category were allowed to correlate [36]. Thus, the errors of perceived breach and feelings of violation were specified to correlate. The same procedure was applied to the pairing of post-word of mouth and post-likelihood of switching. In addition to the proposed model, two alternative models were tested. The first alternative model was the same as the proposed model except that the effects of justice perceptions on psychological responses and postincident outcomes were excluded. The second alternative model also mirrored the proposed model except that it excluded the effects of psychological responses on postincident outcomes. These alternative models were examined as a way to evaluate the relative importance of justice perceptions and psychological responses in determining postincident outcomes.

Table 3 presents the results of the alternative and proposed models. The results of SEM showed that the proposed model was a reasonable representation of the phenomenon. In particular, the fit indexes were well within the acceptable ranges $\chi^2 (1,157) = 2,211.14$, $p < 0.001$, CFI = 0.99, NNFI = 0.99, RMSEA = 0.030, SRMR =0.022, GFI = 0.93, AGFI = 0.90. In addition, we found that the proposed model explained a significant amount of the variation in the endogenous variables. Specifically, the model accounted on average for about half of the variance because squared multiple correlations (SMCs) range from 29 percent to 65 percent (see Table 3). Meanwhile, the first alternative model without the effects of justice perceptions fit the data poorly according to SRMR $\chi^2 (1,181) = 2,798.85$, $p < 0.001$, CFI = 0.99, NNFI = 0.98, RMSEA = 0.037, SRMR =0.111, GFI = 0.91, AGFI = 0.88. Moreover, it accounted for less than 7 percent of the variance in perceived breach (4.0 percent) and feelings of violation (6.8 percent); this implies the importance of justice perceptions in understanding psychological responses. Meanwhile, this model explained about 50 percent of the variation on average in behavioral outcomes. A chi-square test showed that the proposed model represents the data better than the first alternative model $\Delta \chi^2 (24) = 587.71$, $p < 0.001$. The second alternative model without the effects of psychological responses generally fit the data better than the first alternative model $\chi^2 (1,161) = 2,463.25$, $p <0.001$, CFI = 0.99, NNFI = 0.99, RMSEA = 0.033, SRMR =0.111, GFI = 0.91, AGFI = 0.88. Nevertheless, it did not perform better than the proposed model in terms of fit $\Delta \chi^2 (4) = 252.11$, $p < 0.001$. As shown in Table 3, the proposed model accounts for 60 percent of the variance in behavioral outcomes on average, but the second alternative model explains only 51 percent of the variation in behavioral outcomes. These results imply that psychological responses play a significant role in regulating postincident outcomes. As a whole, our results suggest that the proposed model was superior to the partial models in terms of both fit and explained variance.
Table 3. Results of Structural Equation Modeling Analysis

<table>
<thead>
<tr>
<th>Antecedents</th>
<th>Alternative Model 1</th>
<th>Alternative Model 2</th>
<th>Proposed Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PR</td>
<td>PI</td>
<td>PR</td>
</tr>
<tr>
<td>Control variables</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGE</td>
<td>-0.00</td>
<td>-0.01</td>
<td>-0.02</td>
</tr>
<tr>
<td>GEN</td>
<td>-0.01</td>
<td>-0.04</td>
<td>-0.05</td>
</tr>
<tr>
<td>EXP</td>
<td>-0.03</td>
<td>-0.01</td>
<td>-0.02</td>
</tr>
<tr>
<td>WU</td>
<td>-0.05</td>
<td>-0.01</td>
<td>-0.05</td>
</tr>
<tr>
<td>PU</td>
<td>-0.04</td>
<td>-0.04</td>
<td>-0.04</td>
</tr>
<tr>
<td>PEOU</td>
<td>-0.15**</td>
<td>-0.02</td>
<td>-0.00</td>
</tr>
<tr>
<td>TRUST</td>
<td>-0.06</td>
<td>-0.03</td>
<td>-0.05</td>
</tr>
<tr>
<td>RISK</td>
<td>-0.14***</td>
<td>-0.26***</td>
<td>-0.17***</td>
</tr>
<tr>
<td>LOY</td>
<td>-0.08</td>
<td>-0.02</td>
<td>-0.17***</td>
</tr>
<tr>
<td>SC</td>
<td>-0.01</td>
<td>-0.03</td>
<td>-0.09**</td>
</tr>
<tr>
<td>Preincident Outcomes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WOM</td>
<td>-0.16***</td>
<td>-0.02</td>
<td>-0.22***</td>
</tr>
<tr>
<td>LOS</td>
<td>-0.11***</td>
<td>-0.24***</td>
<td>-0.01</td>
</tr>
<tr>
<td>Justice perceptions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DJ</td>
<td>-0.41***</td>
<td>-0.29***</td>
<td>-0.42***</td>
</tr>
<tr>
<td>PJ</td>
<td>-0.11**</td>
<td>-0.00</td>
<td>-0.23***</td>
</tr>
<tr>
<td>IJ</td>
<td>-0.05</td>
<td>-0.30***</td>
<td>-0.22***</td>
</tr>
<tr>
<td>Interactions between justice perceptions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DJ x PJ</td>
<td>-0.10*</td>
<td>-0.04*</td>
<td>-0.01</td>
</tr>
<tr>
<td>DJ x IJ</td>
<td>-0.01</td>
<td>-0.10**</td>
<td>-0.04</td>
</tr>
<tr>
<td>PJ x IJ</td>
<td>-0.09**</td>
<td>-0.01*</td>
<td>-0.04</td>
</tr>
<tr>
<td>Psychological responses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PB</td>
<td>-0.38***</td>
<td>-0.43***</td>
<td>-0.22***</td>
</tr>
<tr>
<td>FV</td>
<td>-0.32***</td>
<td>-0.32***</td>
<td>-0.13***</td>
</tr>
</tbody>
</table>

SMC (R^2)  
-0.04 | -0.07 | -0.48 | -0.51 | -0.30 | -0.35 | -0.60 | -0.42 | -0.29 | -0.34 | -0.65 | -0.55

* p<0.05, ** p<0.01, *** p<0.001 (two-tailed).
Notes: n = 1,007; DJ = distributive justice; PJ = procedural justice; IJ = interactional justice; PB = perceived breach; FV = feelings of violation; PWOM = post-word of mouth; PLOS = post-likelihood of switching; AGE = age; GEN = gender; EXP = experience; WU = website usage; PU = perceived usefulness; PEOU = perceived ease of use; TRUST = trusting beliefs; RISK = risk beliefs; LOY = loyalty; SC = switching costs; WOM = pre-word of mouth; LOS = pre-likelihood of switching. Hypotheses were tested at the level of 0.01 because of the large sample size.
Test of Research Hypotheses

We took a conservative approach when testing research hypotheses because of a relatively large sample size ($n = 1,007$). Large samples tend to be sensitive to the statistical significance of even a small effect. Instead of using a standard 0.05 significance level, therefore, we adopted a more stringent level of significance of 0.01 (one-tailed) \[42\]. Despite such conservative testing, we found that the data fully supported all the hypotheses proposed in this study.

Effects of Justice Perceptions. We proposed earlier that three types of justice perceptions would influence perceived breach and feelings of violation (H1, H2, and H3). Consistent with our expectation, distributive justice has significant effects on both perceived breach and feelings of violation (H1 supported). In addition, as expected, procedural justice exhibited a significant impact on perceived breach (H2 supported). Finally, consistent with our hypothesis, interactional justice was a significant antecedent of feelings of violation (H3 supported).

Interactions Between Justice Perceptions. We predicted earlier that the effect of distributive justice on perceived breach would decrease with an increase in procedural justice. As expected, we found that procedural justice moderated the relationship between distributive justice and perceived breach (H4 supported). Moreover, in line with our expectations, we found that interactional justice indeed moderated the relationship between distributive justice and feelings of violation (H5 supported).

Our findings also show that the effect of procedural justice on perceived breach would increase with an increase in interactional justice (parameter estimate = $-0.09$, $p < 0.05$). It is important to note that the interaction between procedural justice and interactional justice was rarely observed in traditional settings in which relationships were based on face-to-face contacts. A plausible explanation is that interactional justice is treated as a cue for the authenticity of procedural justice, especially in the context of online privacy breach recovery in which customers are separated from the actual recovery process. In particular, as service representatives represent the online firm in privacy recovery, customers’ understanding of the complex recovery process can be supplemented by their interactions with the representatives. Whereas high quality interactions provide a glimpse of the firm’s policies to ensure fairness in the recovery, poor interaction experience may raise doubts about whether or not fair procedures are followed, and hence reduce customers’ sensitivity to procedural justice.

Effects of Psychological Responses. We proposed that post-word of mouth and post-likelihood of switching would be affected by perceived breach (H6) and feelings of violation (H7). As hypothesized, perceived breach influenced both post-word of mouth and post-likelihood of switching (H6 supported). Likewise, we found that feelings of violation had significant effects on post-incident outcomes (H7 supported).

Controlled Effects. We found that pre-word of mouth had a significant effect on post-word of mouth (0.20, $p < 0.001$, two-tailed) whereas pre-likelihood of switching exerted a significant effect on post-likelihood of switching (0.28, $p < 0.001$, two-
tailed). Each of the justice perceptions had significant effects on both post-word of mouth and post-likelihood of switching. However, none of the interactions between justice perceptions had any significant impact on postincident outcomes, which implies the important role of psychological responses in a theoretical framework.

As indicated in Table 3, individual characteristics—that is, age, gender, experience, and website usage—generally have little impact on psychological responses and postincident outcomes. Only one of 16 paths proved significant, and this exception occurred between age and post-likelihood of switching (estimate = -0.07, p < 0.01, two-tailed). These results imply that older people are less likely to switch to alternatives at the postincident stage, but, except for the age effect, individual characteristics generally do not have impact on online customer behavior. Unlike individual characteristics, however, customers’ perceptions at the preincident stage such as perceived usefulness, perceived ease of use, trusting beliefs, risk beliefs, loyalty, and switching costs were significantly related to at least one of the endogenous variables. These results suggest that preincident perceptions largely mediate the impact of individual characteristics on online customer behavior.

Discussion and Conclusion

The main purpose of this study was to develop and empirically test a model that explains the role of an online firm’s postincident recovery endeavor in mitigating the impact of a privacy breach on customer relationships. Drawing on the service recovery literature, we integrated the notions of justice perceptions and psychological responses into a theoretical framework describing how individuals react to an online firm’s postincident actions. The proposed model was tested on data collected from 1,007 users of online vendors. The results of SEM analysis generally supported our model. As expected, three types of justice perceptions were sharply distinct from each other in their main and interaction effects on psychological responses. In addition, consistent with our hypotheses, psychological responses were shown to play an important role in shaping postincident outcomes in the online context. Overall, our findings suggest that justice perceptions and psychological responses are the keys to a better understanding of online customer behavior after privacy breach recovery. This study provides researchers and practitioners with a conceptual tool for analyzing the effectiveness of organizational practices in mitigating the damaging effect of a privacy breach on customer relationships.

Theoretical Implications

Three Types of Justice Perceptions

The notion of justice and its related perceptions, that is, distributive, procedural, and interactional justice, have been shown to be useful in explaining customers’ privacy-related predispositions and behavioral consequences [50, 70]. Our study contributes
significantly to the information privacy literature by showing how justice perceptions differ from each other in the context of online privacy breach recovery. Specifically, this study demonstrates that distributive justice has positive effects on both cognitive and emotional evaluations. However, we found that procedural justice affects cognitive evaluations (i.e., perceived breach), whereas interactional justice determines emotional evaluations (i.e., feelings of violation). Our findings bolster a common notion that compensation exerts profound effects on individuals’ overall evaluations of a situation in question. More interesting, this study reveals a relatively unknown fact of justice perceptions that once compensation is taken into account, fair procedures affect only the cognitive side but not the emotional side, whereas respectful treatments affect the emotional side but not the cognitive side. We suspect that the emergence of this discernible pattern from this particular study results, at least partly, from its lean online context in which individuals’ judgments about fairness are rarely intermixed with rich human relationships. In any case, more research is needed to explore the distinct nature of justice perceptions that may vary with respect to different privacy contexts. Overall, this study adds to the justice literature by showing theoretically as well as empirically the clearly discernible patterns behind justice perceptions, especially when these patterns are examined within the context of online privacy breach recovery.

Interactions Between Justice Perceptions on Psychological Responses

Another contribution of this study to the information privacy literature is the interactions between justice perceptions that are unique to our context of an online firm’s reactions to a privacy breach. As hypothesized, procedural justice somewhat complements distributive justice. Customers with an opportunity to be involved in the recovery process tend more than excluded customers to be less sensitive to monetary reward. Thus, a high level of procedural justice compensates, to some extent, for a low level of distributive justice. Similarly, interactional justice complements distributive justice. High interactional justice implies that an online firm is committed to taking responsibility for a privacy incident. In such a situation, customers are less likely to doubt the fairness of compensation than they are otherwise. Procedural justice and interactional justice are distinct in their interaction effects because procedural justice moderates the effect of distributive justice on perceived breach, but interactional justice moderates the effect of distributive justice on feelings of violation. As proposed by the psychological contract perspective, the cognitive-emotion taxonomy that differentiates procedural justice and interactional justice seems to hold well, even for explaining their interactions with distributive justice on psychological responses.

Although not hypothesized in this study, the interaction between procedural justice and interactional justice is shown to exist on perceived breach. In fact, this interaction between procedural justice and interactional justice was rarely observed in traditional settings in which relationships are based on face-to-face contact. We
reason that interactional justice is similar to procedural justice in that both are more concerned with means than with ends. For this reason, people often consider each of the “relationship-oriented” justice perceptions as a cue for the authenticity of the other dimension. Especially in a domain in which relational bonds are unstable, people are known to evaluate the two types of justice perceptions together instead of independently [47]. Therefore, when interactional justice is lower, online customers are less likely to be sensitive to the question of whether or not fair procedures are followed. This is because in the case of low interactional justice, their reactions are likely to be generally unenthusiastic regardless of the level of procedural justice. Meanwhile, when interactional justice is higher, online customers will be more sensitive to the level of procedural justice. Thus, in the online privacy domain, the effects of procedural justice on perceived breach will be stronger when interactional justice is higher. Consistent with this reasoning, procedural justice is shown to be largely synergistic with interactional justice; that is, the impact of procedural justice is not maximized when interactional justice is low. Our findings will add to the growing literature on justice perceptions and their complex effects on individuals’ overall evaluations.

Perceived Breach and Feelings of Violation

To the best of our knowledge, this is the first study to formally examine psychological contract violation in an online privacy breach. A psychological contract is established between customers and an online firm regarding the security of customer data. A data breach constitutes a violation of a psychological contract in online commercial transactions. Drawing on the taxonomy proposed by Morrison and Robinson [58], we explicitly differentiated between perceived breach, which represents a cognitive response, and feelings of violation, which indicate an emotional response. Our findings show that feelings of violation are indeed distinct from perceived breach ($r = 0.51$). Moreover, the emotional factor (i.e., feelings of violation) is found to affect post-word-of-mouth (parameter estimate = $-0.13$, $p < 0.001$) as well as post-likelihood of switching (parameter estimate = $0.23$, $p < 0.001$) after controlling for its cognitive counterpart (i.e., perceived breach). We should note that Pavlou and Gefen [59] earlier introduced the notion of a psychological response in their effort to examine the buyer–seller relationship in the context of online auctions. Their study, however, focused mainly on the cognitive aspects of a breach and paid less attention to its emotional factors. Our results indicate that the current theory needs to be expanded to include both cognitive and emotional responses. We believe that our dual approach to psychological responses is effective not only in examining privacy problems but also in understanding other social exchange relationships.

Managerial Implications

Our findings provide practitioners with valuable insights into how to salvage customer relationships damaged by privacy-related incidents. In particular, we
advocate that privacy breach recovery should be carefully reengineered. Specifically, managers could consider creating privacy breach remedies that allow for recovery efforts directed at improving the psychological responses experienced by customers. They should have an array of tools and resources available to address the specific needs of customers. Recall that, in our study, perceived breach and feelings of violation were greatly affected by compensation. However, perceived breach became less sensitive to compensation when a fair procedure was in place, and feelings of violation were less affected by compensation when respectful interpersonal treatment was experienced. This result is an important reminder that redressing privacy breaches means more than enacting all three aspects of privacy breach recovery. Thus, online firms must carefully consider the specific psychological responses to improve customers’ privacy situations.

Limitations and Further Research

This study employed hypothetical scenarios to simulate privacy incidents; such simulation is unavoidable to some degree, but nevertheless impairs the study’s realism. Thus, the model and hypotheses need to be further validated by real data. Another limitation relates to the cross-sectional nature of the data. Because of the inherent limitation of the cross-sectional design of this experiment, the time lapse before and after a privacy breach could not actually be allowed, but only marked by a hypothetical scenario. Thus, more conclusive inferences from our findings require evaluation against a future longitudinal study.

This study opens up exciting avenues for further research. In particular, this study shows the significance of emotion in privacy-related behavior. In the present study, one’s emotion is represented by a single factor called “feelings of violation.” Yet customers’ emotional responses are likely to manifest more subtle and complex patterns than what is captured by a one-dimensional variable. In fact, research shows that some emotional responses (e.g., anger and fear) are related to perceived fairness [66], and we believe that those variables would be relevant in the context of information privacy. For example, people could be angry at an online firm if the firm mishandled their personal data. And, they may fear potential misuse or exploitation of their personal information by hackers. We encourage researchers to identify emotional factors that may be important to privacy research and examine how such emotions differentially affect behavioral outcomes.

Conclusions

Despite increased security measures taken by firms, privacy breaches continue to be a serious issue in the modern digital economy. Given the vulnerable nature of the business environment, firms should be prepared to recover effectively and efficiently from privacy-related incidents. To that end, we offer a theory-driven approach to evaluating the effectiveness of alternative organizational practices in helping firms to
maintain their relationships with customers even after a privacy breach. We believe that the model proposed in this study can serve as a solid foundation for further investigation of privacy-related issues. It is hoped that this study will stimulate more research in this important area and that the proposed model will aid this future work.

Supplemental file
Supplemental data for this article can be accessed on the publisher’s website at http://dx.doi.org/10.1080/07421222.2015.1138375

NOTES
1. Our model is specifically designed for a situation in which a customer has been notified of a privacy breach and is now reacting to an online firm’s postincident actions in mitigating the impact of the breach on customer relationships.
2. The concept of perceived breach does not represent one’s perception of the extent of a privacy breach alone. Rather it indicates a deliberate judgment of the degree to which an online firm has failed to fulfill obligations related to how to handle personal information and how to respond to a breach incident. Bansal and Zahedi [4] differentiated repaired trust from violated trust in a study of organizational reactions to a data breach. Perceived breach corresponds more to repaired trust than to violated trust because repaired trust reflects psychological responses after organizational actions, whereas violated trust indicates psychological responses before organizational actions [4].
3. In IS literature, individuals’ privacy-protective responses are classified into three categories: (1) information provision (e.g., refusal, misrepresentation), (2) private action (e.g., negative word of mouth, removal of personal information), and (3) public action (e.g., complaining) [9]. The postincident outcomes examined in this study correspond to the second category—private action.
4. We examined common method variance (CMV) and found that CMV was not substantial in this particular study. The results are shown in online Appendix C. We also checked whether our experimental manipulation of justice items worked. The results are shown in online Appendix D, and they indicate that all three manipulations worked as anticipated.

REFERENCES


Copyright of Journal of Management Information Systems is the property of Taylor & Francis Ltd and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.