Aug 10th, 12:00 AM

Play Your Cards Right: Utilizing Differential Privacy as a Competitive Advantage

Till Ole Diesterhöft
University of Goettingen, tillole.diesterhoeft@uni-goettingen.de

Aycan Aslan
Georg-August-Universität Goettingen, aycan.aslan@uni-goettingen.de

Marvin Braun
University of Goettingen, marvin.braun@uni-goettingen.de

Play Your Cards Right: Utilizing Differential Privacy as a Competitive Advantage

Completed Research

Till Ole Diesterhöft
University of Goettingen
tillole.diesterhoeft@uni-goettingen.de

Aycan Aslan
University of Goettingen
aycan.aslan@uni-goettingen.de

Marvin Braun
University of Goettingen
marvin.braun@uni-goettingen.de

Abstract

Given the increasing amount of information being leveraged in business models, a growing number of companies have adopted differential privacy (DP) as a means of ensuring privacy. DP enables the adjustment of privacy characteristics of individual information. Nevertheless, measurements taken rarely lead to total prevention of information loss due to external events, i.e., data breaches. Owing to the control nature of DP, we argue that even in the occurrence of a data breach, investments made in this technology can be strategically exploited to positively influence perceived information privacy control. Drawing on prior literature, we propose a relationship between customers' information privacy control and satisfaction. By conducting a between-subjects experiment (n=185), we can confirm these assumptions. Our paper paves the way for the disclosure of privacy measures, in particular DP, to enable a more positive reaction of customers towards data breaches, thus creating competitive advantages.

Keywords

Differential privacy, perceived information control, data breach notifications.

Introduction

With the growing utilization of user data, data breaches have become an everyday phenomenon for companies. They are observable across industries and can cause severe damage. This includes negative effects on the company's reputation, e.g., loss in consumer trust (Culnan and Williams, 2009) and financial impact or a decline in stock market value (Malhotra and Malhotra, 2011). In their report on data breaches, the Ponemon Institute (2021) concluded that the average cost for a data breach amount to USD 4.24 million, the highest average cost in the 17-year history of the report. Due to these wide-ranging implications of data breaches, the sufficient handling of such has become a strategically important task for companies. Accordingly, strategies for preventing and mitigating the negative outcomes of data breaches are an essential pillar in companies' risk management.

The growing body of academic literature on managing and responding to data breaches has highlighted that the strategic conceptualization of data breach responses enhances customers' satisfaction, trust, and repurchase intentions (Goode et al. 2017, Masuch et al. 2021). Providing a customer-centric and tailored response yields decreased harm to customers' behavioral intentions (Hoehle et al., 2022), enabling businesses to gain long-term competitive advantages. In this context, prior studies have shown the positive influence that control, a form of empowering the consumer, over their data can have (Joosten et al., 2017). For example, Tucker (2014) showed that people responded more favorably to ads when they had the possibility of controlling their privacy settings. Further, Martin et al. (2017) demonstrate that granting consumers greater control over the use of their personal information can suppress the negative impacts regarding data breaches. However, when discussing the potential of customer control in reducing the

negative effects of data breaches, it often remains unclear which and how companies can utilize specific technologies to achieve such control.

A possible response for this search for sufficient technologies to ensure more consumer control over personal information is differential privacy (DP). DP is a privacy technology that gained popularity in the last years among companies such as Apple, Microsoft, and Google (Cummings et al., 2021). In essence, DP describes the modification of a dataset to reduce the possibility of identifying information about individuals (Dwork and Roth, 2013). Fitting for the context of data breach responses, the privacy protection provided by DP is not binary. Hence, the protection cannot be divided into private and not private but rather is a continuum that represents the level of information leakage occurring (Dwork and Roth, 2013). The data analyst can adjust this continuum and the respective level of privacy guaranteed by fine-tuning the model parameters in the differentially-private setup. This very characteristic of DP yields the potential for utilizing it in the context of customer control in data breach responses since the parameters of the differentially-private model can be seen as 'knob' with which the level of privacy can be *controlled*. These controllable features of DP pose the question of whether DP can be used as a strategic technological tool to ensure consumers higher levels of control over the information in data breach responses, ultimately leading to a competitive advantage. Against this background, this paper investigates following research question (RQ):

RQ: *Can differential privacy be leveraged in data breach responses to unlock competitive advantages for businesses?*

To answer this question, we conduct a between-subjects study in the form of an online experiment (n=185). We manipulate the security measure considering the digital technology of DP. We demonstrate that publicizing these DP measures positively affects customer satisfaction and behavioral intentions. Furthermore, the privacy concern of customers is alleviated. Thus, we show that DP can be used as an innovative asset in data breach communication to increase customer engagement and satisfaction.

Research Background

Data Breach Notifications

In addition to numerous positive effects, the increasing use of customer information also leads to the risk of data breaches. Data breaches occur when customer information is compromised by internal employees or external attackers, resulting in the information being leaked to the public (Confente et al., 2019). Theft of customer information can include sensitive information such as social security numbers or private health information (Sen and Borle, 2015), both of which can lead to identity theft and thus indirect costs for customers. Due to this, new regulations in the USA and Europe have been introduced, forcing businesses to inform their customers about the occurrence of a data breach involving sensitive customer information (Culnan and Williams, 2009). As a result, businesses must disclose data breach notifications, which, in contrast to traditional security incidents, establish a novel information interface to the customer (Janakiraman et al., 2018). Drawing on this peculiarity, research has revealed that notifying customers about a data breach has numerous negative effects, such as losing customer trust or decreasing a company's financial performance (Malhotra and Malhotra, 2011). Likewise, negative word-of-mouth and an impaired repurchase intention can be triggered (Wang and Huff, 2007). Consumer privacy concerns in particular play a pivotal role in privacy breaches. Data breaches have been shown to increase the privacy concerns of customers (Culnan and Williams, 2009; Chen and Jai, 2021), which in turn can be seen as a long-term risk for affecting a company's business (Wirtz and Lwin, 2009).

While Martin et al. (2017) also show that negative damages can arise, they further indicate how this damage can be reduced. In a study of the effects of data breach notifications on customers, they suggest that customer control can inhibit the negative effects of a data breach notification. They describe this control as the amount of empowerment a customer has to dictate how the company manages customer information (Martin et al., 2017). In addition to reducing the adverse effects, a potential integration of control into the data breach response process may show multifaceted benefits, such as the possible increase in satisfaction (Diesterhöft et al., 2022). Research further suggests that increasing customers' perceived control can reduce customers' privacy concerns (Martin and Murphy, 2017).

We highlight that prior literature emphasizes that perceived control of the processed information can be a central moderator on the adverse effects of a data breach notification. However, no research has yet

addressed the central role of privacy control and how it can be harnessed by novel digital technologies. Therefore, the question arises as to how this specific control can be induced and how it can be steered by businesses to reduce further the negative effect of data breach notifications.

(Differential) Privacy and its Strategic Use by Companies

DP is a formal definition proposed by Dwork and Roth (2013) that has gained popularity in the last years. In essence, DP is the modification of a dataset to reduce information about single individuals while retaining the capability of statistical reasoning about the dataset (Dwork and Roth, 2013). The dataset modification is usually achieved by a noise-adding mechanism (Dwork and Roth, 2013). The added noise and consequent perturbation of the dataset make it hard for an adversary to tell which aspects of the given analysis came from randomness and which from individuals present in the dataset (Dwork and Roth, 2013). For companies, the elegance of DP lies in its adaptability. Compared to traditional techniques, DP does not provide binary privacy protection (e.g., private or not-private) but instead denotes the level of information leakage possible (Dwork and Roth, 2013). The privacy budget is quantified, among others, by the parameter ε. Hence, ε can be seen as a 'knob' to fine-tune the privacy provided by the algorithm and can be adjusted by the respective data analyst. Here, low levels of ε lead to higher levels of privacy, while high values of ε provide lower privacy, yielding companies the control to fine-tune the level of privacy.

DP has several unique benefits that distinguish it from traditional privacy methods (Dwork and Roth, 2013). However, the most important being the mathematical quantification and rigor regarding the level of privacy ensured. Compared to traditional techniques (e.g., data masking), DP provides provable mathematical guarantees. Due to this uniqueness, DP has become a leading technique to meet the growing consumer demand for data privacy in the digital age. Consequently, several companies have started deploying DP in the last few years. For instance, Apple uses DP to collect aggregated, thus noised-up, statistics on the Emoji usage of their consumers (Cummings et al., 2021). Based on these statistics and learnings Apple can generate, emojis are being ordered based on the consumers' preferences, improving the consumer experience. Further, Google uses DP to generate statistics of Google Chrome crash reports confidentially (Cummings et al., 2021). Following these early adopters, new startups emerge that focus on DP, while also additional existing companies have announced to experiment and ultimately implement DP.

With the growing number of negative examples of consumer privacy violations, e.g., in the form of data breaches (Malhotra and Malhotra, 2011), companies recognized the demand of consumers for sufficient and credible data privacy. In this context, Buck and Burster (2017) indicate that consumers consider privacy as a factor in their preference structure when downloading an app. Further, Jakobi et al. (2021) show that well-designed data protection processes can enhance the customer experience and be a key element in managing the future customer experience.

Hypotheses Development

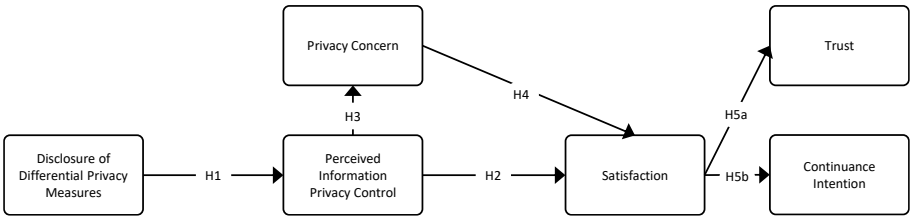

Figure 1: Theoretical Research Model of Differential Privacy in Data Breach Responses

As mentioned earlier, the deployment of DP, by its very nature, allows for a high level of control of the level of privacy guaranteed (Dwork and Roth, 2013). Accordingly, in the academic literature, the parameter ε has been coined the "privacy control parameter" (Zhang et al., 2011), which can be flexibly adjusted for the given context (Friedman and Schuster, 2010). As stated previously, the privacy level provided can be adjusted by the employing company, which opens the possibility to adjust the level of privacy guaranteed for the given context or customer. In this context, we argue that when communicated respectively, consumers will recognize these controllable characteristics of DP, which will impact the perceived level to which the privacy measure deployed can be influenced. Therefore, we hypothesize that:

H1: *The disclosure of the deployment of differential privacy measures positively impacts customers' perceived information privacy control.*

Recent literature has revealed that establishing customer control in the context of a data breach notification leads to a suppression of negative effects on customers (Martin et al., 2017). We expand on the service failure context related to the data breach domain (Goode et al., 2017), which demonstrates an inversion of these effects, i.e., establishing control to reduce negative effects and enable positive outcomes (Joosten et al., 2017). Creating different types of control, i.e., process, decisional, and information control, has been shown to induce a more positive perception of customers towards service failure (Guo et al., 2016). Information control describes the wealth of information that may be supplied about an event, enabling a customer to form an understanding of the situation (Thompson, 1981). As differential privacy enables the controllability of privacy characteristics (Dwork and Roth, 2013), disclosing the use of privacy-preserving measures represents an information provision regarding privacy control. Accordingly, considering a novel use of the innovative technology of differential privacy in data breach notifications, we argue that revealing the arising control through this technology has a positive impact on customers. Thus, we hypothesize:

H2: *Perceived information privacy control positively impacts satisfaction with the data breach response.*

We note a rich body of academic literature discussing the factors that affect the level of privacy concerns of consumers (Martin and Murphy, 2017). Prior research shows that consumer concern is linked to the level of control over that information (Goodwin, 1991). Specifically, literature in the context of control theory demonstrates that consumer perceived control is a key factor affecting privacy concerns (Xu et al., 2012; Norberg and Horne, 2014). Against this background, we argue that the level of consumer control influences the level of privacy concern in the context of data breaches. We, therefore, hypothesize that:

H3: *Perceived information privacy control negatively impacts privacy concerns.*

In the context of data breaches, satisfaction reflects the feelings of consumers about how the data breach incident has been handled (Masuch et al., 2021). Data breach research has identified this satisfaction as a pivotal element in evaluating the effectiveness of data breach responses (Masuch et al., 2021). Prior studies have shown that privacy attributes can function as antecedents of satisfaction (Ribbink et al., 2004; Chang and Chen, 2009). Hence, users having higher levels of privacy concern may negatively impact their satisfaction. Thus, we hypothesize:

H4: P*rivacy concern negatively impact satisfaction with the data breach response.*

While customer satisfaction is a central pillar for evaluating customer-centric communication strategies (Churchill and Surprenant, 1982), influenced behavioral intentions are of necessary consideration, especially for assessing actual post-data breach impact on customers (Hoehle et al., 2022). Since previous data breach and service failure research has pointed out the positive relationships between satisfaction and trust (Kau and Wan-Yiun Loh, 2006; Masuch et al., 2021) as well as satisfaction and continuance intentions (Wirtz and Mattila, 2004), we include these relationships in our study. Therefore, we hypothesize:

H5: *Satisfaction with the data breach response positively impacts customers' (a) trust and (b) continuance intention.*

Research Design and Experimental Setting

Following the developed research model, we designed a 2x1 between-subjects study. The study was conducted in the context of a scenario-based online experiment. To achieve a high degree of acceptance of the scenario, we opted for a data breach in the healthcare context. Data breaches in this domain are characterized by highly sensitive information (Seh et al., 2020), resulting in high financial expenses for the company (Ponemon Institute, 2021) as well as far-reaching consequences for customers through information misuse (Czeschik, 2018). We argue that this type of experimental scenario increases relatedness to the setting, thereby increasing the realism of a data breach scenario. Both scenarios were framed in this healthcare context, differing only in the type of privacy measures applied (traditional privacy measures and DP). Participants were acquired by distributing the survey in a university context; therefore, participants were primarily students at a German university. Due to incomplete questionnaires, 29 data sets had to be removed. The final sample comprises 185 participants, with an average age of 25 years (SD=3.08). A total of 69 women (37.3%) and 112 men (60.5%) participated, while 4 participants (2.2%) did

not specify a gender. 90% of the participants support digitization in healthcare, 30% have already shared health information via digital means, and 42% have experienced an actual data breach.

Regarding our experimental setting, all participants received the same information initially. Participants were advised to put themselves in the situation where the doctor informs them about a non-profit initiative in which patients can share their medical records to advance medical research during their next primary care doctor visit. Participants were informed that their personal health information is recorded by the MedData-app, designed by the initiative. Next, participants are confronted with the information that a data breach occurred concerning the MedData-app in an e-mail. Following this general disclosure of the data breach, participants were divided into two scenarios. In this first scenario, our baseline scenario, participants were informed about standard privacy measures deployed: "*While we can't fully assess the damage caused, we can ensure you that the MedData-app employed the most widespread and accepted data protection measures."* However, in the second scenario, our DP scenario, participants were confronted with the information that the MedData-app deployed DP: "*While we can't fully assess the damage caused, we can ensure you that the MedData-app employed differential privacy, a novel, mathematical technique to preserve privacy where the privacy measures can be fine-tuned for the given context*." This description was aligned with recent literature to represent the unique DP characteristics (Cummings et al., 2021).

Data Analysis and Results

We employed the partial least squares structural equation modeling (PLS-SEM) approach to test our hypotheses (Hair et al., 2011). PLS-SEM has gained increasing popularity in IS research (Ringle et al., 2012; Guo et al., 2021). Given the novel investigation of the effects of DP, our study pertains to an exploratory investigation. Accordingly, PLS-SEM is suitable since only the effects between latent variables, but not their effect size, are relevant to our research (Goodhue et al., 2012). Furthermore, PLS-SEM is useful for smaller samples (Fombelle et al., 2016), making it suitable for our study. We used SmartPLS3 (Ringle et al., 2015).

Construct Measures

Construct (adapted from)	Items	Loadings
Perceived Information Privacy Control (Chau and Hu, 2002)	I would have the ability to change the characteristics of the privacy measures employed.	0.901
	The characteristics of the privacy measures employed would be entirely within my control.	0.917
	I would have the resources to make use of the characteristics of the privacy measures employed	0.833
	I would not have the knowledge to make changes to the characteristics of the privacy measures employed.	N/A
Privacy Concern (Li, 2014)	*How concerned are you that your personal health information may be used for purposes other than the reason you provided the information for?*	*0.573*
	How concerned are you about your personal privacy on the MedData-app?	0.778
	How concerned are you about the fact that the MedData-app might know/track you?	0.792
	How concerned are you about the MedData-app sharing your personal health information with other parties?	0.795
	It does not bother me when the MedData-app is collecting too much information about me.	0.737
	I have no doubts about how well my privacy is protected on the MedData-app.	0.758
Satisfaction (Goodwin and Ross, 1992; Kantsperger and Kunz, 2010; Park and Park, 2016)	I was satisfied with the way that the initiative has handled the problem.	0.920
	Overall, I am satisfied with the initiative's reaction to the security incident.	0.945
	I had a good experience with the initiative's reaction.	0.927
	I was pleased with the way the initiative reacted to the problem.	0.950
Continuance Intention (Kuo and Wu, 2012; Goode et al., 2017)	I intend to continue using the MedData-app of the initiative in the future.	0.960
	I plan to continue participating in the data collection of the initiative.	0.975
	The chances are high that I will keep sharing my data with the initiative.	0.967
Trust (Choi and Ji, 2015)	I think the MedData-app is safe.	0.916
	I find the MedData-app trustworthy.	0.933
	All in all, I trust the MedData-app.	0.955
	I find the MedData-app reliable.	0.888

Table 1: Constructs and Items

For the measurements of the constructs, all items were adapted based on the literature and adjusted to our context. All items were measured with a 7-Likert scale. In addition to the constructs, demographic

questions, manipulation checks, and a construct designed to measure common method variance were retrieved. We controlled for age, gender, and prior data breach experience. The disclosure of privacy measures was dummy coded with a binary latent variable. All constructs, items, and corresponding loadings are shown in Table 1.

Model Validation and Assessment

Before the structural model was assessed, we first evaluated the reliability and validity of our measurement model. Reliability is achieved by ensuring indicator and internal consistency reliability. Indicator reliability can generally be assumed when the loading is above 0.708, indicating that at least 50% (as $0.708^2 \approx 0.5$) of the variance of an item can be explained by the associated latent variable. Indicators that lie in the range of 0.4-0.708 can be retained in the measurement model if the validity and reliability criteria at the construct level are met (Hair et al., 2021). Internal consistency reliability is established by measures of Cronbach's alpha ($\alpha > 0.7$) and composite reliability ($\rho C > 0.7$) (Nunnally and Bernstein, 1994).

The validity of the measurement model was assessed by testing convergence and discriminant validity. Convergence validity is reached when the explained variance of a construct among its indicators (average variance extracted (AVE)) is greater than the measurement error, i.e., above 50% (AVE > 0.5) (Henseler et al., 2009). Discriminant validity describes how constructs are different from other constructs, implying that they represent a certain notion that is not reflected in any other construct (Hair et al., 2010). This can be ensured by the Fornell-Larcker (FL) criterion and the heterotrait-monotrait ratio (HTMT). The FL criterion requires that the square root of a construct's AVE must be greater than the correlation with the other constructs. This guarantees that no other construct explains more variance of the indicators than the originating construct (Hair et al., 2021). The HTMT describes the similarity among constructs; here, a value of less than 0.85 is desirable (Henseler et al., 2015). Table 2 shows that our measurement model's convergence and discriminant validity, and internal consistency reliability are met. Furthermore, table 1 reveals that the indicator reliability is given for all but two indicators (marked in italics). One indicator had to be removed (<0.4), while one indicator (<0.708) could be retained due to the given validity and reliability on the construct level. Thus, our measurement model meets the criteria of both validity and reliability. To ensure that no common method bias (CMB) exists, i.e., that there no effects are induced by the measurement method (Kock, 2015), we followed Chin et al.'s (2013) measured latent marker variable approach. To this end, we adopted the construct of the color blue (Simmering et al., 2015). Our results show no significant effects on our latent variables, suggesting that no CMB persists.

	AVE	α	ρC	DP	PIC	PC	Sat	Trust	CI
DP	1.000	1.000	1.000	**1.000**	*0.173*	*0.108*	*0.059*	*0.043*	*0.024*
PIC	0.782	0.861	0.915	0.164	**0.885**	*0.185*	*0.216*	*0.284*	*0.243*
PC	0.552	0.839	0.880	-0.101	-0.153	**0.743**	*0.442*	*0.576*	*0.503*
Sat	0.876	0.953	0.966	0.058	0.199	-0.410	**0.936**	*0.592*	*0.624*
Trust	0.852	0.942	0.958	0.041	0.255	-0.538	0.564	**0.923**	*0.801*
CI	0.936	0.966	0.978	-0.020	-0.227	0.464	-0.600	-0.765	**0.968**
FL criterion in bold, HTMT ratio in italics									

Table 2: Convergent and Discriminant Validity

To assess the significance of our hypothesized paths, we ran the bootstrap method with 10,000 samples (Hair et al., 2021) (see Figure 2). We can confirm all our hypotheses and show that all hypotheses but H3 are significant for at least p<.05. The results of the structural model indicate that the disclosure of DP measures has a direct positive influence on perceived information privacy control (β=.164, p=.022), thus supporting H1. As this control in turn has a positive influence on customer satisfaction (β=.140, p=.042) and a negative influence on privacy concern (β=-.153, p=.073), H2 and H3 are supported. This privacy concern, in turn, adversely affects customer satisfaction (β=-.389, p<.001) in support of H4. As a confirmatory part of our research, H5a and H5b are supported as we demonstrate the positive relationship between customer satisfaction and both trust (β=.564., p<.001) and continuance intention (β=.600., p<.001). We tested all dependent variables for our controlled variables and identified that, except for continuance intention (β=-.139, p=.012), age has no effect on our model. Moreover, prior data breach experience only influences privacy concern (β=.208, p=.007) and satisfaction (β=.136, p=.043), while gender has no effect at all.

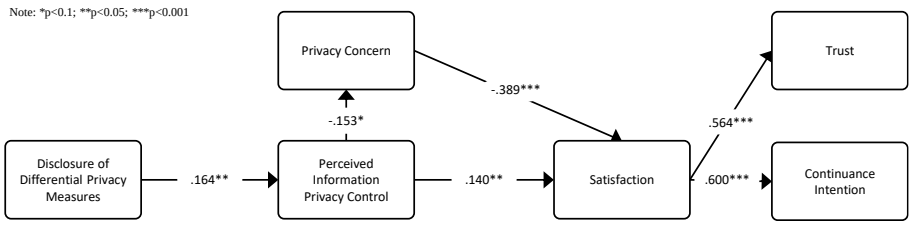

Figure 2: Structural Model Estimates

Discussion

Contributions to Literature

The findings of our study contribute to current literature and theory in three ways: First, we contribute the literature on DP by demonstrating that specific characteristics of DP can be communicated to consumers, opening a new perspective on DP. So far, literature on DP has mainly focused on techniques to implement and optimize DP algorithms, whereby the user perspective on DP was notably absent (Cummings et al., 2021). However, the findings of our work show that specific characteristics of DP can be used to communicate such characteristics to consumers. In this context, we focused on the fact that the privacy guarantees are controllable, which can be communicated to consumers. Our findings show that consumers appreciate the controllable nature of DP by influencing the perceived information privacy control, which positively influences satisfaction, trust, and continuance intention. Second, our study suggests that the implementation of DP as a digital technology can be leveraged as a resource to influence customer satisfaction and their behavioral intentions positively. We provide preliminary insights that a company's privacy and security resources, with DP in our instance, can yield beneficial outcomes when portrayed in communication with customers. This advances extant literature that has focused on the influences of business resources as determinants in the aftermath of a data breach, such as reputation (Gwebu et al., 2018), company size, and age (Rasoulian et al., 2021). Thus, we pave the way for businesses to realize a positive post-breach competitive advantage through pre-data breach privacy and security investments, enabling resources previously untapped in customer communications to be publicized. Third, our study contributes to the literature on customer control. Prior research has shown that control improves customer outcomes in data breach and data breach-like situations (Guo et al., 2016; Martin et al., 2017; Diesterhöft et al., 2022). In particular, control was regarded as the degree of influence on the management of personal information (e.g., user settings controlling how information is used) (Martin et al., 2017). By transferring this notion into the context of DP, we illustrate that control over information privacy further drives customer satisfaction. Thus, our study reveals a radical shift in control and suggests that in communicating data breaches, control is more multifaceted than in other domains, e.g., service failure (Joosten et al., 2017).

Managerial Implications

Besides the contribution to literature, we derive several managerial implications from our findings: First, we show that managers can see and utilize DP as a strategic technology to gain a competitive advantage. As illustrated, companies can strategically use DP in the context of data breaches to minimize the potential harm caused. Hence, when communicated effectively, DP can serve businesses as a multidimensional tool to positively influence factors such as satisfaction with the companies or trust and continuance intention, which can serve as a competitive advantage in an age where privacy issues become increasingly relevant to the decision-making of consumers. Second, we note that practical data breach response strategies mostly focus on compensation or apologizing to the consumer (Goode et al., 2017). Even though these strategies induce beneficial outcomes for the customers (Hoehle et al., 2022), establishing control remains an aspect that is only marginally addressed. We support current literature and reveal that in addition to control over information (Martin et al., 2017), a customer-centered data breach response strategy should also encompass control over information privacy. By increasing customer satisfaction with the response, customer relationships can be improved, and customer churn reduced. Thus, rendering it a fruitful avenue for achieving advantages over competing companies. Especially when conceptualizing response strategies, practitioners should, therefore, also consider the effects that arise from the disclosure of privacy measures.

Limitations and Opportunities for Future Research

We further note four areas in which future research could strengthen our results: First, we recognize that we only used one description of DP. This poses a limitation since, as mentioned earlier, there is no standard description of DP. As demonstrated in other studies (Cummings et al., 2021), different forms and themes to communicate DP and its characteristics exist. Hence, future research should analyze how other forms of describing DP can influence factors such as perceived information privacy control or satisfaction. Second, our study investigates DP as a control source over information only in an experimental setting. Thus, we have no insight into how customers might respond to authentic control distribution. Yet, since DP offers exactly this possibility, future research should examine the impact of DP's unique characteristics through adapted experiments and field studies. Third, our sample primarily consists of younger individuals with a university background. Therefore, a higher technological understanding and a correspondingly improved self-identification with privacy measures provided by companies can be assumed. Future research should study whether perceptions of disclosed privacy measures are influenced by education, age, and culture. Fourth, given the nature of our study, future research should specifically examine what impact the pre-breach disclosure of DP measures has on post-breach customer perceptions. Possible negative effects could arise from the disconfirmation of expectations, potentially negating the effects of DP measures in our study. In this context, the long-term success of DP disclosure measures should be evaluated to determine the effect of a sustained competitive advantage.

Conclusion

In conclusion, our work provides valuable insights into how the novel technology of DP can be strategically utilized by companies to achieve competitive advantages. In conducting a between-subject online experiment (n=185), we indicate that the controllable characteristics of DP can be successfully communicated with customer experiencing a data breach, yielding higher levels of satisfaction, trust, and continuance intentions. We show that companies can proactively communicate these characteristics, i.e., such of DP, creating a superior customer experience. This, in turn, can function as a competitive advantage, where consumers increasingly incorporate privacy-related issues in their decision making.

REFERENCES

Buck, C. and S. Burster. (2017). "App information privacy concerns." *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation 2017-Augus*.

Chang, H. H. and S. W. Chen. (2009). "Consumer perception of interface quality, security, and loyalty in electronic commerce." *Information and Management 46* (7), 411–417.

Chau, P. Y. K. and P. J. Hu. (2002). "Examining a model of information technology acceptance by individual professionals: An exploratory study." *Journal of Management Information Systems 18* (4), 191–229.

Chen, H. S. and T. M. Jai. (2021). "Trust fall: data breach perceptions from loyalty and non-loyalty customers." *Service Industries Journal 41* (13–14), 1–17.

Chin, W. W., J. B. Thatcher, R. T. Wright and D. Steel. (2013). "Controlling for Common Method Variance in PLS Analysis: The Measured Latent Marker Variable Approach." In: A. Krishnan, N. Kriegeskorte, & H. Abdi (Eds.), *New Perspectives in Partial Least Squares and Related Methods*, Vol. 56, pp. 231–239.

Choi, J. K. and Y. G. Ji. (2015). "Investigating the Importance of Trust on Adopting an Autonomous Vehicle." *International Journal of Human-Computer Interaction 31* (10), 692–702.

Churchill, G. A. and C. Surprenant. (1982). "An Investigation into the Determinants of Customer Satisfaction." *Journal of Marketing Research 19* (4), 491–504.

Confente, I., G. G. Siciliano, B. Gaudenzi and M. Eickhoff. (2019). "Effects of data breaches from user-generated content: A corporate reputation analysis." *European Management Journal 37* (4), 492–504.

Culnan and Williams. (2009). "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches." *MIS Quarterly 33* (4), 673–687.

Cummings, R., G. Kaptchuk and E. M. Redmiles. (2021). *"I need a better description": An Investigation into User Expectations for Differential Privacy*. *Proceedings of the ACM Conference on Computer and Communications Security*, Vol. 1. Association for Computing Machinery.

Czeschik, C. (2018). "Black Market Value of Patient Data." In: C. Linnhoff-Popien, R. Schneider, & M. Zaddach (Eds.), *Digital Marketplaces Unleashed*, pp. 883–893. Berlin, Heidelberg: Springer Berlin Heidelberg.

Diesterhöft, T. O., M. Greve, A. Aslan and L. M. Kolbe. (2022). "Together We Are Stronger - Paving the Way for Value Co-Creation in Data Breach Responses." In: *International Conference on Wirtschaftsinformatik*, pp. 1–18.

Dwork, C. and A. Roth. (2013). "The algorithmic foundations of differential privacy." *Foundations and Trends in Theoretical Computer Science 9* (3–4), 211–487.

Fombelle, P. W., S. A. Bone and K. N. Lemon. (2016). "Responding to the 98%: face-enhancing strategies for dealing with rejected customer ideas." *Journal of the Academy of Marketing Science 44* (6), 685–706.

Friedman, A. and A. Schuster. (2010). "Data mining with differential privacy." *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* 493–502.

Goode, S., H. Hoehle, V. Venkatesh and S. A. Brown. (2017). "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach." *MIS Quarterly 41* (3), 703–727.

Goodhue, D. L., W. Lewis and R. Thompson. (2012). "Does PLS Have Advantages for Small Sample Size or Non-Normal Data?" *MIS Quarterly 36* (3), 981–1001.

Goodwin, C. (1991). "Privacy: Recognition of a Consumer Right." *Journal of Public Policy & Marketing 10* (1), 149–166.

Goodwin, C. and I. Ross. (1992). "Consumer responses to service failures: Influence of procedural and interactional fairness perceptions." *Journal of Business Research 25* (2), 149–163.

Guo, L., S. L. Lotz, C. Tang and T. W. Gruen. (2016). "The Role of Perceived Control in Customer Value Cocreation and Service Recovery Evaluation." *Journal of Service Research 19* (1), 39–56.

Guo, W., D. Straub, P. Zhang and Z. Cai. (2021). "How trust leads to commitment on microsourcing platforms: Unraveling the effects of governance and third-party mechanisms on triadic microsourcing relationships." *MIS Quarterly 45* (3), 1309–1348.

Gwebu, K. L., J. Wang and L. Wang. (2018). "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management." *Journal of Management Information Systems 35* (2), 683–714.

Hair, J. F., W. C. Black, B. J.Babin and R. E. Anderson. (2010). *Multivariate data analysis*, 7th Edition. Englewood Cliffs: Prentice Hall.

Hair, J. F., G. T. M. Hult, C. Ringle and M. Sarstedt. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)*, 3rd Edition. SAGE.

Hair, J. F., C. M. Ringle and M. Sarstedt. (2011). "PLS-SEM: Indeed a silver bullet." *Journal of Marketing Theory and Practice 19* (2), 139–152.

Henseler, J., C. M. Ringle and M. Sarstedt. (2015). "A new criterion for assessing discriminant validity in variance-based structural equation modeling." *Journal of the Academy of Marketing Science 43* (1), 115–135.

Henseler, J., C. M. Ringle and R. R. Sinkovics. (2009). "The use of partial least squares path modeling in international marketing." *Advances in International Marketing 20*, 277–319.

Hoehle, H., V. Venkatesh, S. A. Brown, B. J. Tepper and T. Kude. (2022). "Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach." *MIS Quarterly 46* (1), 299–340.

Janakiraman, R., J. H. Lim and R. Rishika. (2018). "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer." *Journal of Marketing 82* (2), 85–105.

Joosten, H., J. Bloemer and B. Hillebrand. (2017). "Consumer control in service recovery: beyond decisional control." *Journal of Service Management 28* (3), 499–519.

Kantsperger, R. and W. H. Kunz. (2010). "Consumer trust in service companies: a multiple mediating analysis." *Managing Service Quality: An International Journal 20* (1), 4–25.

Kau, A.-K. and E. Wan-Yiun Loh. (2006). "The effects of service recovery on consumer satisfaction: a comparison between complainants and non-complainants." *Journal of Services Marketing 20* (2), 101–111.

Kock, N. (2015). "Common method bias in PLS-SEM: A full collinearity assessment approach." *International Journal of E-Collaboration 11* (4), 1–10.

Kuo, Y. F. and C. M. Wu. (2012). "Satisfaction and post-purchase intentions with service recovery of online shopping websites: Perspectives on perceived justice and emotions." *International Journal of Information Management 32* (2), 127–138.

Li, Y. (2014). "The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns." *Decision Support Systems 57* (1), 343–354.
Malhotra, A. and C. Malhotra. (2011). "Evaluating customer information breaches as service failures: An event study approach." *Journal of Service Research 14* (1), 44–59.
Martin, K. D., A. Borah and R. W. Palmatier. (2017). "Data privacy: Effects on customer and firm performance." *Journal of Marketing 81* (1), 36–58.
Martin, K. D. and P. E. Murphy. (2017). "The role of data privacy in marketing." *Journal of the Academy of Marketing Science 45* (2), 135–155.
Masuch, K., M. Greve and S. Trang. (2021). "What to do after a data breach? Examining apology and compensation as response strategies for health service providers." *Electronic Markets 31*, 829–848.
Norberg, P. A. and D. R. Horne. (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 42* (4), 415–429.
Nunnally, J. C. and I. H. Bernstein. (1994). "The Assessment of Reliability." In: *Psychometric Theory*, 3rd Edition, pp. 248–292. New York, NY: McGraw-Hill.
Park, J. J. and J. W. Park. (2016). "Investigating the effects of service recovery quality elements on passengers' behavioral intention." *Journal of Air Transport Management 53*, 235–241.
Ponemon Institute. (2021). *Cost of a Data Breach Report 2021*. *IBM Security*.
Rasoulian, S., Y. Grégoire, R. Legoux and S. Sénécal. (2021). "The Effects of Service Crises and Recovery Resources on Market Reactions: An Event Study Analysis on Data Breach Announcements." *Journal of Service Research* 1–20.
Ribbink, D., S. Streukens, A. C. R. Van Riel and V. Liljander. (2004). "Comfort your online customer: Quality, trust and loyalty on the internet." *Managing Service Quality: An International Journal 14* (6), 446–456.
Ringle, C. M., M. Sarstedt and D. W. Straub. (2012). "A critical look at the use of PLS-SEM in MIS quarterly." *MIS Quarterly: Management Information Systems 36* (1).
Ringle, C. M., S. Wende and J.-M. Becker. (2015). *SmartPLS3*. Bönningstedt: SmartPLS.
Seh, A. H., M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar and R. A. Khan. (2020). "Healthcare data breaches: Insights and implications." *Healthcare 8* (2), 1–18.
Sen, R. and S. Borle. (2015). "Estimating the Contextual Risk of Data Breach: An Empirical Approach." *Journal of Management Information Systems 32* (2), 314–341.
Simmering, M. J., C. M. Fuller, H. A. Richardson, Y. Ocal and G. M. Atinc. (2015). "Marker Variable Choice, Reporting, and Interpretation in the Detection of Common Method Variance: A Review and Demonstration." *Organizational Research Methods 18* (3), 473–511.
Thompson, S. C. (1981). "Will it hurt less if I can control it? A complex answer to a simple question." *Psychological Bulletin 90* (1), 89–101.
Tucker, C. E. (2014). "Social networks, personalized advertising, and privacy controls." *Journal of Marketing Research 51* (5), 546–562.
Wang, S. and L. C. Huff. (2007). "Explaining buyers' responses to sellers' violation of trust." *European Journal of Marketing 41* (9/10), 1033–1052.
Wirtz, J. and M. O. Lwin. (2009). "Regulatory focus theory, trust, and privacy concern." *Journal of Service Research 12* (2), 190–207.
Wirtz, J. and A. S. Mattila. (2004). "Consumer responses to compensation, speed of recovery and apology after a service failure." *International Journal of Service Industry Management 15* (2), 150–166.
Xu, H., H. H. Teo, B. C. Y. Tan and R. Agarwal. (2012). "Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services." *Information Systems Research 23* (4), 1342–1363.
Zhang, N., M. Li and W. Lou. (2011). "Distributed data mining with differential privacy." *IEEE International Conference on Communications*.