Please quote as: Diesterhöft, T. O.; Benner, D.; Brauer, B. (2022). Introducing Conversational Explanations as a Novel Response Strategy to Data Breach Incidents in Digital Commerce. pre-ICIS Workshop on Information Security and Privacy (WISP). Copenhagen, Denmark.

Introducing Conversational Explanations as a Novel Response Strategy to Data Breach Incidents in Digital Commerce

Till Ole Diesterhöft[1]
University of Göttingen,
Göttingen, Germany

Dennis Benner
University of Kassel,
Kassel, Germany

Benjamin Brauer
University of Göttingen,
Göttingen, Germany

ABSTRACT

In order to individualize and personalize digital services, an increasing number of e-commerce providers are exploiting abundant amounts of customer information. Alongside these positive effects, an inherent risk of compromise of customer information arises, resulting in data breaches. Compelled by regulations, companies are obliged to notify their customers. Previous literature indicates that different data breach response strategies can mitigate the negative effects of these security incidents. Drawing on data breach and conversational agent (CA) research, we theorize that the manner in which a data breach is communicated is equally relevant. We test our developed hypotheses in an online experiment (n=89). Our results show that explaining a data breach increases customer satisfaction. Simultaneously, we reveal that CAs lend themselves as a tool to positively influence this degree of explanation. Our work provides novel insights into the centrality of explanation in a data breach response and their positive correlation with CAs.

Keywords: conversational agents, data breaches, response strategies.

INTRODUCTION

To facilitate and personalize digital services and digital commerce providers leverage a wealth of sensitive customer information and data (Ho et al. 2011). For instance, in digital

[1] Corresponding author. tillole.diesterhoeft@uni-goettingen.de +49 551 3921704

commerce personalized product recommendations on customer data have become very popular. While this allows for a more tailored experience for customers, it also entails an inherent risk. This risk is manifested by the potential compromise of sensitive information due to security gaps, known as data breaches (Goode et al. 2017). Data breaches can be defined as security incidents "in which individuals gain access to the personal data of […] customers" (Hoehle et al. 2022, p. 300). Only recently, the sportswear manufacturer Adidas disclosed that following a cyberattack on its online store. The company learned "that an unauthorized party claimed to have acquired limited data related to certain adidas customers" (adidas 2018). Such data breaches pose substantial direct and indirect costs to companies (Foerderer and Schuetz 2022; Martin and Murphy 2017). Indeed, the average cost of a data breach jumped from $3.86 million to $4.24 million last year alone (Ponemon Institute 2021). Since preventing data breaches is virtually infeasible (Gwebu et al. 2018), companies need to strategize how to respond to them to mitigate the induced costs (Hoehle et al. 2022). In this regard, recent Information Systems (IS) literature has been able to identify numerous pioneering strategies. Besides the compensation of customers, e.g., by vouchers or identity theft monitoring services (Goode et al. 2017), offering an apology is recognized as a key element to mitigate the incurred damages (Bansal and Zahedi 2015; Masuch, Greve, and Trang 2021). In examining these nascent findings, we note that the current state of data breach research mainly focuses on studying the response strategies apology and compensation.

However, as data breaches and its circumstances are uncertain by nature (Choi et al. 2016), customers' expectations and perceptions towards these events are vital (Goode et al. 2017; Hoehle et al. 2022). Especially in the context of privacy, it is critical that customers develop an understanding of the described issues (Arcand et al. 2007). As a result, the current

standard approach to data breach responses, i.e., apologizing by showing remorse, or compensating customers through, for instance, coupons, may leave customers uninformed and left out because of the lack of emphasis on data breach explanation as well as limited communication channels available. For example, detailed information about the data breach are oftentimes not included in practical responses or vague (D'Arcy and Basoglu 2022). This may leave customer questions unanswered and them wanting a more in-depth interaction for further details as well as a less distant seeming interaction with the digital commerce provider. If these customers' needs are not met, a negative impact on the customers' trust and intention to continue business can be induced (Hoehle et al. 2022; Masuch, Greve, and Trang 2021). Here, conversational agents (CA) may provide an alternative approach to novel response strategies. Because of their conversational nature and high availability CAs can serve as a conversational alternative to conventional data breach response strategies. Moreover, CAs can converse with customers and provide them with additional information or employ additional response strategies in contrast to a simple notification or mail. Thus, we investigate the option of using CAs as a viable approach to enacting data breach response strategies. Here, we focus on explanations where the CA processes relevant information on the data breach for the customer. Therefore, we raise the following research questions (RQ):

RQ1: *What influence does message delivery by CAs have on data breach explanation?*

RQ2: *What effect does the explanation of a data breach have on customers' behavioral intentions?*

In the following, we first present the background on data breaches and response strategies as well as the role of CAs in our research context. We then continue to raise our hypotheses that

we will test. Followingly, we present our research approach and methodology in detail. Finally, we present the results from our online experiment as well as implications for future research.

RELATED RESEARCH

Data Breaches and Response Strategies

In focusing on the delivery of individualized services and products to customers, e-commerce and online merchant companies leverage vast volumes of customer data (Ho et al. 2011). Thereby, it is of utmost necessity that the security and privacy of these are assured (Anderson et al. 2017). However, despite implementing preventive measures, it is almost impossible to entirely prevent data breaches (Gwebu et al. 2018). For instance, employees cannot be stopped from accidentally committing a data breach or from carrying out a deliberate internal data breach. When these data breaches occur, sensitive customer information is compromised. As a result of this exposure, Social Security Numbers, or Insurance Numbers, among other things, can be leaked, resulting in the risk of identity theft (Choi et al. 2016). If sensitive information is breached, regulations require companies to notify their customers (Foerderer and Schuetz 2022). These outbound communications show various negative effects on the company. Beside the negative impact on the stock market value (Foerderer and Schuetz 2022), data breaches also lead to a deterioration of customer behavioral intentions (Martin et al. 2017). These include decreased trust in the company, less satisfaction with the business, or a decline in the intention to repurchase products and services (Janakiraman et al. 2018; Malhotra and Kubowicz Malhotra 2011). Thus, companies are exposed to both short-term and long-term existential threats. To mitigate these risks, companies can implement so-called communicative data breach response strategies (Hoehle et al. 2022).

A customer-oriented, tailored approach is to be pursued, which is based on the requirements of the respective customers (Masuch, Greve, and Trang 2021). Offering compensation, instantiated by monitoring services, discounted content, or monetary remuneration, is identified as a key strategic response strategy (Goode et al. 2017). Additionally, providing apologies and remorse to customers reduces the negative effects on the behavioral intentions of customers (Bansal and Zahedi 2015). While positive effects can be achieved through these strategic approaches, all efforts highlighted strive for an intention to drive change through outcome-related aspects. However, especially in data breaches, customer perceptions and thus understanding of these incidents is of utmost relevance (Goode et al. 2017; Hoehle et al. 2022). This is due to the uncertain nature of data breaches. Uncertainties, for instance, include possible information misuse, the unknown state of breached information, and the broader security concerns towards the breached company (Choi et al. 2016; Confente et al. 2019). Consequently, to accurately assess and cope with a data breach, customers require to understand all these aspects and uncertainties. Therefore, companies need to make appropriate explanatory efforts to support customers affected by a data breach. Hence, we argue that in addition to the established strategic approaches, the explanation statements could be a substantial addition.

Conversational Agents as a Data Breach Response Strategy

In general, conversational agents can be defined as (semi-)autonomous technological artifacts that make use of natural language which enables them to interact with human users in a human-like and more natural-seeming way (de Keyser et al. 2019). The general idea in this context is a technology-based approach to provide humans with assistance that is available around the clock, at low cost and to offer a more personal communication to provide assistance or support (Diederich et al. 2022). Furthermore, CAs can feature social behavior that enables

them to converse in a more natural and humanistic fashion, thus providing a more pleasant communication channel such as digital commerce providers (Bittner et al. 2019). Here, CAs can use this communication channel to provide specific domain or task support (i.e., handling data breaches) as a self-service offering (Diederich et al. 2022). For instance, CAs can be used to outsource high-intensity, high-cost tasks (i.e., managing and communicating data breach situations to users/customers) to an automated entity and thus turning this task to a self-service offering. To interact in such a human-like way, CAs commonly use text or voice including natural language as well as informal language (Schmitt et al. 2021). Moreover, CAs can include social elements such as social cues that are natural to human-human interaction and reflect natural human behavior (Feine et al. 2019). Overall, these characteristics can make CAs a more pleasant means of communication between customers and digital commerce providers, that can support a specific task (e.g., handling data breaches via CAs) and thus result in a better experience (Van Alstyne et al. 2016).

In the context of digital commerce and potential data breach incidents, this can translate into a high potential for delivering fast, cost-effective and more in-depths responses to data breaches to customers. Using CAs in such encounters can make a currently very impersonal and distant communication of data breaches more intimate and personal (Sheehan et al. 2020). On the one hand, CAs can provide a more natural, human-like experience, anywhere and anytime, potentially strengthening the relationship between the digital commerce provider and the customer on both interpersonal and business levels (Holz et al. 2009). This could be particularly useful in critical cases like data breaches, where the relationship between commerce providers and customers can be significantly harmed. On the other hand, this cost-effective communication that is available at all times and in all places can enable digital commerce providers to effectively

scale-up their data breach response strategy which is particularly important for larger companies where scaling can become a key success factor (Huang et al. 2017; Lewis et al. 2011). Consequently, CAs have been established across many different service and commerce sectors to interact and support customers. (Qiu and Benbasat 2009). To be able to provide assistance, CAs can identify, localize, connect and compute relevant information on the users' behalf and thus enable a semi-autonomous self-service to the customer (Beverungen et al. 2019; Lim and Maglio 2018). For instance, CAs can identify, localize, connect and compute the relevant information concerning a data breach incident for an affected customer and therefore provide fast, available and cost-effective help. Moreover, the characteristics of CAs allow digital commerce providers to quickly adapt to the customer's needs and changing requirements (Beverungen et al. 2019). Therefore, CAs are in general expected to become even more important including different self-service and digital commerce applications (Nordheim et al. 2019). In the context of our research this is expressed in a novel conversational-based response strategy.

HYPOTHESES DEVELOPMENT AND RESEARCH MODEL

In this section we present our hypotheses based on the issues presented in the introduction and consequently our RQs, as well as the related research, particularly on data breaches and CAs. In this regard we also present our research model below in Figure 1. Because data breaches are usually handled in a very distant and impersonal way (i.e., simple mailings or notifications on the commerce provider website) the interaction can be perceived as similarly inhumane. Such a seemingly uninvolved response of the digital commerce provider can potentially have a negative impact on the customer's attitude.

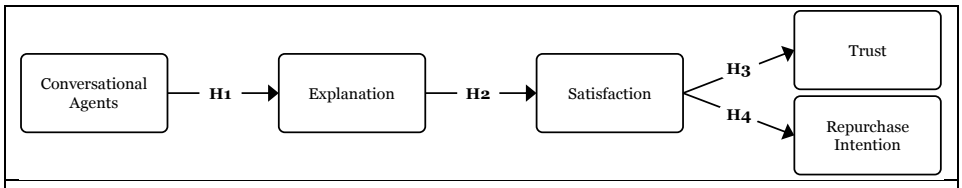

Figure 1. Research Model

Therefore, we suggest using the human-like conversational characteristics of CAs to inform users about data breach incidents and deliver a more personal explanation of the incident via a CA. Following our introduction of CAs and their potential role for handling data breach responses as a novel communication strategy, we present our first hypothesis (H1):

H1: *The use of conversational agents is positively related to customers' perceived explanation.*

Customers are unsettled in the event of data breaches as the risk, e.g., from credit card fraud, may not be precisely defined (Choi et al. 2016). Thus, "when an unintentional and internal data breach does manifest, customers feel a negative sense of uncertainty" (Confente et al. 2019, p. 9). Consequently, customers occupy a position in which the availability of information assumes a decisive function. Especially in the context of customer privacy, it is necessary for customers to build sufficient understanding of privacy issues (Arcand et al. 2007). In turn, an improved understanding enables customers to better cope with privacy-related aspects (Lee et al. 2013). In the context of data breaches, therefore, one way to address the uncertainty of data breaches is through a company's explanation efforts. As a result of this explanation, customers will experience the feeling that they possess increased knowledge about the data breach. In line with this, we argue that the negative effects of uncertainty are diminishing, leading to a higher satisfaction with the data breach response. Against this background, we propose:

H2: *Customers' perceived explanation of the data breach is positively related to customer satisfaction.*

As the breach of data depicts a violation of customer trust, repairing trust in the aftermath of these incidents is pivotal (Bansal and Zahedi 2015). Trust is shaped by previous experiences with a company. Central to this is the level of satisfaction that has been achieved by these experiences (Masuch, Greve, and Trang 2021). If experiences are positive and satisfying, the overall stability of the relationship increases, resulting in a higher level of customer trust (Kau and Wan-Yiun Loh 2006). Thus, in our context, it is implied that satisfaction with a data breach response positively influences trust in a company. This relationship has been demonstrated both in data breach and in related incident literature streams (Goode et al. 2017; Masuch, Greve, and Trang 2021). As a confirmatory part of our study, we therefore hypothesize the following:

H3: *Customer trust is positively related to customer satisfaction.*

Following a data breach, achieving repurchase intention of customers regarding products and services is crucial for online and mobile commerce providers (Goode et al. 2017). Influencing customers' repurchase intentions is integrated as an inherent consequence in the conceptualization of satisfaction (Oliver 1996). This is due to the interference of satisfaction with behavioral intentions (Oliver 1996). Customers vary their attitude towards repurchasing based on their level of satisfaction with a company (Maxham and Netemeyer 2002). Consequently, data breach literature suggests that a satisfactory response to a data breach increases the repurchase intention of customers (Goode et al. 2017). In a confirmatory sense, we hypothesize:

H4: *Customers repurchase intention is positively related to customer satisfaction*

RESEARCH APPROACH

In this section we present our general research approach for our online experiment. To test the derived hypotheses, we conducted a 1x2 vignette-design study (n=89). The questionnaire (see Table 1) was distributed to German participants, especially students in a university

environment. Because of incomplete responses, 21 answers had to be removed. The sample for the experiment has a mean age of 29 years (SD = 11.74). Both men and women were equally represented (50%) in our sample. 36% hold a graduate degree. Participants were first asked to imagine that they are a customer of the fictitious e-commerce company fashionstore24. They were informed that they have already purchased products and services from the company. Participants were then randomly assigned to one of the two treatments. In the first treatment, participants were presented with a typical data breach notification from fashionstore24, which was adapted based on practical applications (Foerderer and Schuetz 2022; Janakiraman et al. 2018). Information about the cause of the data breach, the personal data affected, the company's internal response, and the company's strategy was provided. Based on the literature, we used a compensation as the response strategy (Goode et al. 2017; Hoehle et al. 2022). In the second treatment, participants interacted with a CA (developed using the Google Dialogflow platform for practical reasons). This CA included the identical information as the data breach notification in the first treatment. However, the information was not directly presented in its entirety, but rather at the customer's request. Customers were able to interact with fashionstore24's CA to receive information about the data breach. The CA started the dialog with an initial message stating that a data breach had occurred. The customer was then asked what details he would like to know or if there were any follow-up questions. It is important to note that the context and content of the two notification methods, email notification and CA, is identical, which is crucial to ensure comparability.

PRELIMINARY FINDINGS

Measurement Model Results

To evaluate the proposed research model, we applied the partial least squares structural equation modeling (PLS-SEM) method. Following nascent IS literature, we decided to use PLS-SEM over the covariance-based approach (Trenz et al. 2020). This is due to several reasons. First, PLS-SEM has the capability of concurrently analyzing theoretical links between different constructs (Hair et al. 2021). Second, PLS-SEM allows us to analyze complex models with a relatively small sample size (Fombelle et al. 2016). Third, the focus of our study is to explore relationships rather than to measure their magnitude.

Constructs and Items	Loadings
Explanation (Kau and Wan-Yiun Loh 2006)	
They told me why the data breach had happened in the first place.	0.842
The company seemed very interested in explaining the data breach to me.	0.804
I was given a reasonable explanation as to why the data breach occurred.	0.831
They did not tell me the cause of the data breach. *	0.706
Satisfaction (Maxham and Netemeyer 2002)	
In my opinion, fashionstore24 provided a satisfactory resolution to the data breach on this particular occasion.	0.917
	0.917
I am not satisfied with fashionstore24's handling of this particular data breach. *	0.928
Regarding this particular data breach, I am satisfied with fashionstore24.	
Repurchase Intention (Goode et al. 2017)	
I intend to continue purchasing products from fashionstore24.	0.960
All things considered; I will purchase products from fashionstore24 over the next 12 months.	0.956
Chances are high that I will continue purchasing products from fashionstore24.	0.972
I don't intend to repurchase products from fashionstore24 in future. *	0.952
Trust (Kau and Wan-Yiun Loh 2006)	
I believe fashionstore24 can be relied on to keep its promises.	0.822
I believe that fashionstore24 is trustworthy.	0.880
I feel pretty negative about fashionstore24. *	0.796
All constructs have been carefully translated into German. The constructs were measured with a 7-Likert scale (1=strongly disagree, 7=strongly agree). *=reverse coded scale	

Table 1. Measurement of Constructs

This characteristic supports the use of the PLS-SEM approach (Goodhue et al. 2012). Chatbot manipulation was included as a dummy variable in the measurement model. All other constructs were adapted to the context based on the literature (see Table 1). We then assessed the

validity and reliability of our model. The indicator reliability is given if all loadings are above 0.705 (Hair et al. 2019). This implies that each item explains more variance than the measurement error. Hair et al. (2021) further argue that loadings below 0.705 can be retained if they do not impact the overall validity and reliability of the model. Next, we examined the internal consistency reliability. Here we evaluated the Cronbach's alpha (α) and the composite reliability (CR). Internal consistency reliability is achieved when both parameters are above 0.7 (Hair et al. 2021; Nunnally and Bernstein 1994). Moreover, the average variance extracted (AVE) needs to be evaluated for convergent validity. Each construct should explain at least half of its variance (threshold corresponding to 0.5) (Henseler et al. 2009). To examine the discriminant validity, we employed the Fornell Larcker criterion. Discriminant validity is given if a constructs' square root AVE is greater than the correlation with all other constructs (Fornell and Larcker 1981). Table 2 indicate that the reliability and validity of our model is met.

	AVE	α	CR	Explanation	Satisfaction	Trust	Repurchase Intention
Explanation	0.561	0.796	0.862	**0.749**			
Satisfaction	0.848	0.910	0.944	0.658	**0.921**		
Trust	0.845	0.907	0.942	0.616	0.822	**0.919**	
Repurchase Intention	0.922	0.972	0.979	0.528	0.704	0.822	**0.960**
bold: squared AVE (FL criterion)							

Table 2. Discriminant and Convergent Validity

Structural Model Results and Post Hoc Analysis

We performed the PLS-SEM using the bootstrapping method with 10000 samples. The results are shown in Figure 2. We find evidence that the use of a conversational agent is more effective in explaining a data breach than a traditional data breach notification via mail.

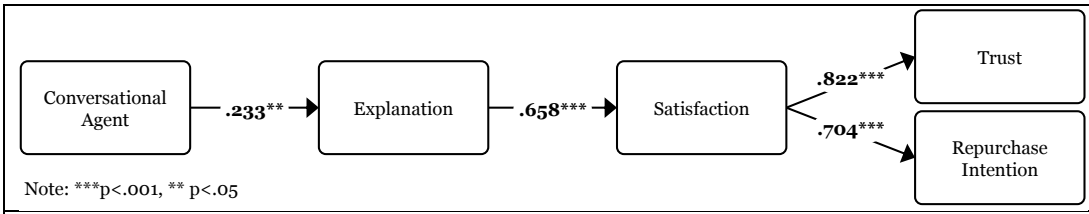

Figure 2. Structural Model

Our results indicate that conversational agents significantly positively lead to an improved explanation of the data breach (β=.233, p=.021). Thus, supporting H1. Furthermore, the results indicate that the explanation of a data breach has a significant positive effect on satisfaction (β=.658, p<.001). Hence, the better a data breach and its circumstances are explained to the customer, the higher is his or her satisfaction. Accordingly, our hypothesized relationship is substantiated (H2). As a confirmatory part of this study, we show that satisfaction has a positive influence on both trust of the customer in the company (β=.822, p<.001) and the intention to repurchase products or services (β=.704, p<.001). Consequently, we find empirical evidence for H3 and H4. To disentangle the effects of conversational agents and explanations in the research model, we conducted a post hoc indirect effect analysis. Paramount interest for our study was to determine the extent to which both conversational agents and explanations may influence customers' behavioral intentions. Accordingly, we examined the indirect effects of both constructs. Table 3 highlights the results of our post hoc analysis.

Indirect Effects	**β value**	**p value**
CA → Explanation → Satisfaction	.147	.027**
CA → Explanation → Satisfaction → Trust	.121	.030**
CA → Explanation → Satisfaction → Repurchase Intention	.104	.033**
Explanation → Satisfaction → Repurchase Intention	.459	<.001***
Explanation → Satisfaction → Trust	.535	<.001***
**p<0.05, ***p<0.001		

Table 3. Post Hoc Analysis of Indirect Effects

Our analysis indicates that CA mediated by explanation has a significant positive effect on satisfaction. Furthermore, we find that CA mediated by explanation and satisfaction has a significant positive effect on trust as well as on repurchase intention. Likewise, we note that explanation mediated by satisfaction has a significant positive effect on trust and repurchase intention.

DISCUSSION

Our intention was to investigate CAs in combination with the data breach explanation as a novel response strategy for data breaches in digital commerce. To answer our RQs, we conducted an online experiment (n=89) in a fictional digital commerce setting. Our preliminary results suggest a positive influence of CA as a communication channel for data breaches. Furthermore, our results indicate the importance of explanations in the context of data breaches. Thus, based on our first findings, we summarize that a data breach explanation positively impacts customers' satisfaction (H2), trust (H3) and repurchase intentions (H4) that relate to RQ2. Regarding CAs, we argue that a more in-depths investigation is necessary to present a conclusive finding (RQ1). We find that H1 is technically statistically significant with a slight positive impact, however because our synthetic experimental setting with limited sample size this may vary in the field. In this regard, we also must consider potential limitations of our study. For instance, we focus on a general approach to response strategies that may not reflect local requirements (i.e., laws) and should therefore be tested and adapted in such specific conditions. Further, while our results are statistically significant, we have to emphasize that the degree varies. For example, the loadings of the CA influence (i.e., H1) are not as strong as expected. Moreover, our experiment was conducted in a synthetic setting of an online experiment that may

or may not be fully transferable to a real-world setting. The novelty of CAs in the context of data breaches constitutes another limitation. Participants could be influenced by this novelty alone, so responses may be biased. Therefore, in addition to measuring the manipulation, the perceived realism of the implemented scenario should be explicitly introduced as a control variable in later studies. Furthermore, our sample may not reflect the general population due to their demographic characteristics (e.g., age of 29). Additionally, we have to acknowledge that we have only conducted an online experiment and further investigation under real-world boundaries is necessary.

CONCLUSION

All in all, we have shown that CAs can play a significant role in delivering data breach response notifications to customers and that this novel method of conversational explanation delivery in data breach cases can have positive influences on the customer. Moreover, from a practical point of view explanation of incidents combined with CAs has the potential to significantly reduce the cost of communication as well as provide a better experience without the user having to rely on customer support. Furthermore, detangling the theoretical grounding even further towards a generalized theory for conversational explanation responses in data critical scenarios would be another potentially valuable step forward. Nevertheless, we are also aware of our limitations that are rooted in our online experiment setting that does not provide a real-world evaluation. Thus, we will investigate real-world usage in the future and hope other researchers will too. We wish to encourage fellow researchers to take up our first steps and follow our approach in future research. Here, we also argue that potential research opportunities may emerge from employing more or different strategies as well as designs, for instance using digital nudges or a persuasive CA approach (Schöbel et al. 2020). In addition to data breach

explanations, helpful information and feedback for potential countermeasures (e.g., password security) could be useful to prevent future incidents. Here, CAs could be used to instruct the user and guide or teach the user such countermeasures or how to respond in data breach situations.

REFERENCES

adidas. 2018. *Adidas Alerts Certain Consumers of Potential Data Security Incident*. (https://www.adidas-group.com/en/media/news-archive/press-releases/2018/adidas-alerts-certain-consumers-potential-data-security-incident/).

Van Alstyne, M. W., Parker, G. G., and Paul Choudary, S. 2016. "Pipelines, Platforms, and the New Rules of Strategy," *Harvard Business Review* (2016:April).

Anderson, C., Baskerville, R. L., and Kaul, M. 2017. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information," *Journal of Management Information Systems* (34:4), Routledge, pp. 1082–1112.

Arcand, M., Nantel, J., Arles-Dufour, M., and Vincent, A. 2007. "The Impact of Reading a Web Site's Privacy Statement on Perceived Control over Privacy and Perceived Trust," *Online Information Review* (31:5), pp. 661–681.

Bansal, G., and Zahedi, F. M. 2015. "Trust Violation and Repair: The Information Privacy Perspective," *Decision Support Systems* (71), pp. 62–77.

Beverungen, D., Müller, O., Matzner, M., Mendling, J., and Vom Brocke, J. 2019. "Conceptualizing Smart Service Systems," *Electronic Markets* (29:1), pp. 7–18.

Bittner, E., Oeste-Reiß, S., and Leimeister, J. M. 2019. "Where Is the Bot in Our Team? Toward a Taxonomy of Design Option Combinations for Conversational Agents in Collaborative Work," in *HICSS*.

Choi, B. C. F., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904–933.

Confente, I., Siciliano, G. G., Gaudenzi, B., and Eickhoff, M. 2019. "Effects of Data Breaches from User-Generated Content: A Corporate Reputation Analysis," *European Management Journal* (37:4), pp. 492–504.

D'Arcy, J., and Basoglu, K. A. 2022. "Cybersecurity Disclosures The Influences of Public and Institutional Pressure on Firms ' Cybersecurity Disclosures," *Journal of the Association for Information Systems*, pp. 1–29.

Diederich, S., Brendel, A. B., Morana, S., and Kolbe, L. 2022. "On the Design of and Interaction with Conversational Agents: An Organizing and Assessing Review of Human-Computer Interaction Research," *Journal of the Association for Information Systems* (23:1), pp. 96–138.

Feine, J., Gnewuch, U., Morana, S., and Maedche, A. 2019. "A Taxonomy of Social Cues for Conversational Agents," *International Journal of Human-Computer Studies* (132), pp. 138–161.

Foerderer, J., and Schuetz, S. W. 2022. "Data Breach Announcements and Stock Market Reactions: A Matter of Timing?," *Management Science* (February).

Fombelle, P. W., Bone, S. A., and Lemon, K. N. 2016. "Responding to the 98%: Face-Enhancing

Strategies for Dealing with Rejected Customer Ideas," *Journal of the Academy of Marketing Science* (44:6), pp. 685–706.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), p. 39.

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

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

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

Hair, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2021. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, (3rd ed.), SAGE.

Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. "When to Use and How to Report the Results of PLS-SEM," *European Business Review* (31:1), pp. 2–24.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. 2009. "The Use of Partial Least Squares Path Modeling in International Marketing," *Advances in International Marketing* (20), pp. 277–319.

Ho, S. Y., Bodoff, D., and Tam, K. Y. 2011. "Timing of Adaptive Web Personalization and Its Effects on Online Consumer Behavior," *Information Systems Research* (22:3), pp. 660–679.

Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., and Kude, T. 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), pp. 299–340.

Holz, T., Dragone, M., and O'Hare, G. M. P. 2009. "Where Robots and Virtual Agents Meet," *International Journal of Social Robotics* (1:1), pp. 83–93.

Huang, J., Henfridsson, O., Liu, M. J., and Newell, S. 2017. "Growing on Steroids: Rapidly Scaling the User Base of Digital Ventures Through Digital Innovation," *MIS Quarterly* (41:1), pp. 301–314.

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

Kau, A.-K., and Wan-Yiun Loh, E. 2006. "The Effects of Service Recovery on Consumer Satisfaction: A Comparison between Complainants and Non-complainants," *Journal of Services Marketing* (20:2), pp. 101–111.

de Keyser, A., Köcher, S., Alkire, L., Verbeeck, C., and Kandampully, J. 2019. "Frontline Service Technology Infusion: Conceptual Archetypes and Future Research Directions," *Journal of Service Management* (30:1), pp. 156–183.

Lee, H. A., Au, N., and Law, R. 2013. "Presentation Formats of Policy Statements on Hotel Websites and Privacy Concerns: A Multimedia Learning Theory Perspective," *Journal of Hospitality and Tourism Research* (37:4), pp. 470–489.

Lewis, M. O., Mathiassen, L., and Rai, A. 2011. "Scalable Growth in IT-Enabled Service Provisioning: A Sensemaking Perspective," *European Journal of Information Systems* (20:3), pp. 285–302.

Lim, C., and Maglio, P. P. 2018. "Data-Driven Understanding of Smart Service Systems

Through Text Mining," *Service Science* (10:2), pp. 154–180.

Malhotra, A., and Kubowicz Malhotra, C. 2011. "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach," *Journal of Service Research* (14:1), pp. 44–59.

Martin, K. D., Borah, A., and Palmatier, R. W. 2017. "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* (81:1), pp. 36–58.

Martin, K. D., and Murphy, P. E. 2017. "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science* (45:2), Journal of the Academy of Marketing Science, pp. 135–155.

Masuch, K., Greve, M., and Trang, S. 2021. "What to Do after a Data Breach? Examining Apology and Compensation as Response Strategies for Health Service Providers," *Electronic Markets* (31), pp. 829–848.

Masuch, K., Greve, M., Trang, S., and Kolbe, L. M. 2021. "Apologize or Justify? Examining the Impact of Data Breach Response Actions on Stock Value of Affected Companies," *Computers & Security*, pp. 1–18.

Maxham, J. G., and Netemeyer, R. G. 2002. "Modeling Customer Perceptions of Complaint Handling over Time: The Effects of Perceived Justice on Satisfaction and Intent," *Journal of Retailing* (78:4), pp. 239–252.

Nordheim, C. B., Følstad, A., and Bjørkli, C. A. 2019. "An Initial Model of Trust in Chatbots for Customer Service—Findings from a Questionnaire Study," *Interacting with Computers* (31:3), pp. 317–335.

Nunnally, J. C., and Bernstein, I. H. 1994. "The Assessment of Reliability," in *Psychometric Theory* (3rd ed.), New York, NY: McGraw-Hill, pp. 248–292.

Oliver, R. W. 1996. *Satisfaction: A Behavioral Perspective on the Consumer*, Boston, MA: Irwin/McGraw-Hill.

Ponemon Institute. 2021. "Cost of a Data Breach Report 2021," *IBM Security*. (https://www.ibm.com/security/data-breach).

Qiu, L., and Benbasat, I. 2009. "Evaluating Anthropomorphic Product Recommendation Agents: A Social Relationship Perspective to Designing Information Systems," *Journal of Management Information Systems* (25:4), pp. 145–182.

Schmitt, A., Zierau, N., Janson, A., and Leimeister, J. M. 2021. "Voice as a Contemporary Frontier of Interaction Design," *ECIS*.

Schöbel, S., Barev, T. J., Janson, A., Hupfeld, F., and Leimeister, J. M. 2020. "Understanding User Preferences of Digital Privacy Nudges - A Best-Worst Scaling Approach," *HICSS*, pp. 3918–3927.

Sheehan, B., Jin, H. S., and Gottlieb, U. 2020. "Customer Service Chatbots: Anthropomorphism and Adoption," *Journal of Business Research* (115), pp. 14–24.

Trenz, M., Veit, D. J., and Tan, C. W. 2020. "Disentangling the Impact of Omnichannel Integration on Consumer Behavior in Integrated Sales Channels," *MIS Quarterly* (44:3), pp. 1207–1258.