Fitness First or Safety First? Examining Adverse Consequences of Privacy Seals in the Event of a Data Breach.

Kristin Masuch
University of Goettingen
kristin.masuch@uni-goettingen.de

Maike Greve
University of Goettingen
maike.greve@uni-goettingen.de

Simon Trang
University of Goettingen
strang@uni-goettingen.de

Abstract

Data breaches are increasing, and fitness trackers have proven to be an ideal target, as they collect highly sensitive personal health data and are not governed by strict security guidelines. Nevertheless, companies encourage their customers to share data with the fitness tracker using privacy seals, gaining their trust without ensuring security. Since companies cannot guarantee security, the question arises on how privacy seals work after not keeping the security promise. This study examines the possibilities to mitigate the consequences of data breaches in advance to maintain the continuance intention. Expectation-confirmation theory (ECT) and privacy assurance statements as a shaping of privacy seals are used to influence customer expectations regarding the data security of fitness trackers in the run-up to a data breach. Results show that the use of privacy assurance statements leads to high-security expectations, and failure to meet these has a negative impact on satisfaction and thus continuance intention.

1. Introduction

The use of mobile devices to track personal activity levels is nowadays a must-have for everyone, not only for professional athletes [1-2]. The technologies enable intermodal connectivity and pocket-sized functionalities that previously required multiple devices. Today, it is standard practice to track, analyze, and exchange personal activity information using such devices [3]. This trend is reflected in the popularity and market size of technologies, such as fitness trackers and smartwatches [1]. The intelligent wearables are mainly used to achieve a kind of personal self-optimization, such as an improvement in physical performance and positive habit formation [3]. This can only be achieved by tracking personal data such as the number of steps, geolocation, or heart rate [1].

In order to enjoy the many uses and benefits of intelligent technology, consumers need to share their private data with service providers. However, users are reluctant to provide such data as they fear a loss of privacy. A major concern is the loss of privacy due to a data breach (e.g., [3-5]). For example, when 150 million users of the MyFitnessPal fitness app were hacked at Under Armour in 2016 [6]. Since users anticipate the risk of a data breach, privacy concerns reveal to be one of the main inhibitors for service adoption and information disclosure. In turn, this becomes a major challenge for service providers whose business models rely on the user's data. One of the most common measures to mitigate concerns regarding data security is to provide assurance to those concerned through privacy seals (e.g., [7-8]). This gives customers the impression of knowing that they can expect service providers to treat their data confidentially and comply with security standards [9]. Confidence-building mechanisms constantly reinforce this trust and willingness to share data. As mentioned, companies often use assurances that are usually expressed through privacy seals. These privacy seals have, for example, the subforms statements about how secure the data is within the company (hereinafter "privacy statements") or commonly known labels certifying security (hereinafter "privacy labels") in order to give consumers greater confidence in the data security of the application and thus make them more reckless when exchanging data. [8]. Without considering that these privacy seals do not necessarily increase security but are often just low-cost statements to elicit more data from the customers and give them a sense of security, data breaches pose a high risk especially for fitness trackers [8], [10]. First of all, they are particularly vulnerable to data breaches due to their interconnectivity and data transfer via mobile data , just in the same way as any other mobile device [11]. Secondly, however, fitness trackers have a special characteristic that sets them apart in the field of health apps. Like other applications, they collect highly sensitive personal health data [12]. In contrast, they do not officially belong to the category of health apps and are therefore not subject to strict security guidelines

URI: https://hdl.handle.net/10125/71085
978-0-9981331-4-0

[13], which makes them a perfect target for data breaches. Therefore, the present paper focuses on the application example fitness tracker.

In general, there is a considerable amount of literature in the research on privacy seals, which has gathered evidence that different privacy seals increase customer trust and encourage them to share their data trust (e.g., [7]). Different mechanisms are being tested to address the concerns regarding data security (e.g., [5], [8], [14]). Also, in the literature on data breaches, some interesting results have already been published. For example, an entire body of literature has been devoted to investigating the financial impact of data breaches (e.g. [15–19]). Another considerable number of articles deal with the prevention of data breaches and investigate how the risk of data breaches can be reduced or mitigated (e.g., [20–22]). Other studies focus on reducing the negative impact after a data breach has occurred. There are a few studies that test recovery actions to increase satisfaction after a data breach (e.g., [23-24]). For example, it has been identified that recovery actions such as compensation are always very effective, and customer satisfaction increases [23], [25], [26]. However, not only the recovery actions are considered in isolation, it can be shown that there is an impact on satisfaction with the recovery actions expected and whether those actions are received. Masuch et al. [26] found, for example, that the confirmation of the expected recovery action leads to higher satisfaction and vice versa. In addition, it could be identified that exceeding expectations also have a positive effect. Besides these research streams, this study examines aspects of the impact of privacy seals in the run-up to a data breach on customer response after a data breach and how these can be influenced. The need to examine whether privacy seals have a negative impact in the event of a data breach is identified. This study aims to determine the impact of privacy seals, especially in the sensitive use of fitness trackers, when security promises are not confirmed. First, the literature on privacy seals is considered from the perspective of a data breach and thus failure to comply with the seal, to add another dimension. Second, the literature on data breaches will be examined to see if there are ways to influence customer behaviors' negative consequences after a data breach in advance. Based on this identified problem in the literature on privacy seals for data breaches, this research paper investigated the following research question an experimental investigation:

RQ1: Which impact do privacy assurance statements as a shaping of privacy seals have on consumer expectations

RQ2: Can they contribute to manipulate expectations in advance of a data breach to mitigate the impact?

The structure of the paper is as follows: The theoretical foundations of the paper are discussed next. First of all, the focus on privacy seals is addressed, emphasizing the privacy assurance statements used in the experiment. Afterward, the theoretical foundations of the expectation-confirmation theory (ECT) are presented. Subsequently, the research model is established, and the five hypotheses are developed. This is followed by a description of the data collection and the evaluation of the data. In conclusion, the results are discussed against the theoretical and practical background, the limitations of this study are pointed out, and topics for future research are identified.

2. Theoretical Background

The following section presents the theoretical foundations for our research model. First, privacy assurance is discussed, and second, the ECT is explained.

2.1. Privacy Assurance

Previous studies have been conducted in the field of privacy assurance and its effects. These have already provided crucial insights into the impact of privacy assurance. Privacy assurance is primarily considered in consumer privacy concerns (e.g., [27]). These concerns relate to consumers' fear of losing their data due to, for example, unauthorized access to personal data [4-5], and have been widely studied in different contexts by the IS literature (e.g.,[12], [28-29]). In addition to privacy assurance, other factors, such as possible privacy controls or personality traits, have been identified as relevant factors that may influence the level of concerns. Nevertheless, privacy assurance is a fundamental mechanism to reduce concerns regarding data security and build trust (e.g., [7]). Other research even considers it to be the most important mechanism for creating a trusted environment for the customer (e.g., [30-31]).

According to previous research, the most common form of privacy assurance are privacy seals. These in turn have two relevant characteristics, namely the labels of third parties (purchased certifications) and self-commitments (self-created, not purchased), which are examined on numerous occasions ([8]). In the present study, only the self-exposure assurance statements are considered, as they are, in contrast to the assurance labels, self-designed statements of the company. They are mostly words or promises made by companies connected with the product or service used to inform the customer about the handling and control of sensitive information [32]. The purpose and intended use of the information is explained to the customer and contributes to a higher level of perceived control by the customer

over his information [9]. They thus provide the customer with a guarantee and reassure him [9].

Also, these privacy assurance statements give the customer the feeling that his data is safe and that his personal information is protected by the company, in particular that it is inaccessible to unauthorized third parties [33]. Thus, some studies have shown that privacy seals, in particular, privacy assurance statements, increase customer confidence in the company. This perceived security is also reflected in behavior in which customers are more willing to share data with the company [8].

To summarize, this research stream informs our study by the aspect that privacy assurance statements are a simple, cost-effective way for companies to influence the behavior and thinking of their customers and thus increase their fear of uncertainty and a breach of confidentiality of their data. Thus, it can be summarized that the positive aspects have been researched. However, there is still a need for research into what happens if the promised security cannot be kept, since in reality it is not increased, but only promised.

2.2 Expectation-Confirmation Theory

We consider the phenomenon of privacy assurance statements in the theoretical background of ECT. This theory was first used in psychology and marketing literature [34-35], but has been applied over time by other research disciplines, such as IS research [36–38]. It considers the effects of comparing expectations with perceived performance on the repurchase intention and customer satisfaction [34]. It explains the satisfaction or dissatisfaction of a customer by confirming or not confirming his expectations. In this case, the decision for (dis)satisfaction influences the intention to repurchase [35]. The model has already been considered in various contexts and areas. For example, Brown et al. [36] discuss six competing models of expectation confirmation from different contexts that have been meaningfully supported throughout empirical research. They examine assimilation, contrast, generalized negativity, assimilation contrast, and only expectations and only experiences. These different approaches all yielded novel and different results. The generalized negativity model, for example, developed from the hypothesis of fulfilled expectations, claims that positive or negative discounting will negatively affect the resulting outcome evaluations [39-40]. While the leading factor in the model of expectations is the prognosis of outcomes, experience alone is essential [36]. Bhattacherjee [38], combined the expectation-confirmation model with additional aspects, here with perceived usefulness, to create the post-acceptance model of IS continuation. Furthermore, the theory is also used by the literature on data breaches, derived from the literature on service failure. Thus, expectations and experiences with compensation as a recovery action were investigated as precursors for the perception of service quality, continuation intention, and repurchase intention. In particular, research focuses on how the different actions of response strategies after a data breach affect satisfaction [23]. Studies examine hypotheses on the effects of compensation and remorse on crucial customer outcomes after a major data breach and the resulting efforts to rebuild the service [23], [25], [26]. One longitudinal analysis of the phenomenon is conducted, starting from the fact that customers were first made aware of a breach until the compensation associated with the breach was paid [23]. On the other hand, it is also investigated in a direct context, and the recovery action follows shortly after the consumers have been notified of the data breach. It is also investigated whether the severity of a data breach causes different expectations regarding the recovery strategies [25], [26]. Overall, the studies show that the ECT explains the perception of service quality and the intention to purchase again and trust the company.

3. Research Model and Hypotheses

To investigate customer satisfaction with a company's data security after a data breach, a research model based on the ECT was established [35]. The construct assurance supplemented the ECT to determine whether the expectations of data security can be influenced and therefore cause different satisfaction reactions after a data breach. In the developed model, the manipulated expectations and the perceived performance (the actual data security) should be taken into account to explain the satisfaction (see Figure 1).

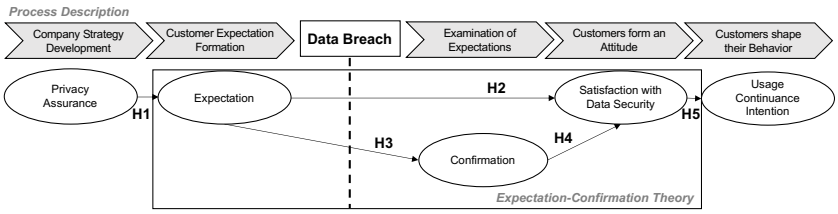

Figure 1: Research Model

As explained above, privacy assurance statements are used to make customers more confident that their information is secure and protected from unauthorized third parties [33]. Based on the mechanism of trust transfer [41–43], Mousavizadeh et al. [8] already define that customers tend to develop a high degree of trust concerning other qualities of the company through the trust generated by privacy assurance statements. Therefore, it can be concluded that customers assume that a company that cares about its customers' privacy will behave similarly to other important issues. For example, customers might think that they can assume that the company is just as conscientious about the security. Thus, we conclude that the privacy assurance statements mitigate customers' concerns that their data may be compromised by an unauthorized access, a so-called data breach. Accordingly, customers may be less concerned about disclosing their data and have higher expectations about the security of their data. Therefore, we formulate the following hypothesis:

H1*: Privacy assurance statements positivly influences users' expectations.*

For this study's purposes, we have defined the expectation as the customer's expectation in terms of the company's data security after a data breach. Since the ECT suggests that general expectations influence satisfaction, these expectations are primarily surveyed in the so-called pre-consumption phase (ex-ante). They represent a fundamental level of expectations with which the consumer can compare their perceived performance [38]. The theory of adaptation levels explains that stimuli are perceived as a function of a principal stimulus level [44]. Thus, it can be concluded from the ECT that expectations tend to lead to higher satisfaction if the initial value of the expectation is high. This statement also applies conversely to the conclusion that low expectations tend to reduce satisfaction [38]. However, since the data breach is always detrimental, the ex-ante expectations will always be disappointed, the expectations are expected to react inversely to satisfaction. This means that high expectations of data security hurt satisfaction with data security. Therefore the following hypothesis can be made:

H2*: Users' expectation of data security is negatively associated with their satisfaction with data security.*

The confirmation compares the perceived performance with the expectations, in this case, with the actual data security received in case of a data breach. Consequently, confirmation is defined as the user's perception of the actual perceived performance compared to a benchmark standard that matches expectations. As a result, there is a direct relationship between expectations and confirmation, as shown by the hypothesis:

H3*: Users' expectation of data security is negatively associated with confirmation.*

Within the ECT, the actual use explains satisfaction by confirming the expectation [35]. Therefore, it can be concluded that the confirmation of expectations and satisfaction are positively related. Satisfaction occurs when a match between the expectation and the actual situation can be established, whereas a mismatch implies that the expectation has not been achieved. If the perceived performance is higher than the expectations, this leads to a positive confirmation and, thus, to a high level of satisfaction. If, in contrast, the performance is below expectations, this leads to a negative confirmation and lower satisfaction. Therefore, satisfaction is the result of an evaluation and comparison process [36–38]. Since the expectations are never positively confirmed in our case, instead there is only a variation in how much the expectations are disappointed, we conclude that with lower expectations the discrepancy for confirming the expectations is smaller and therefore leads to higher satisfaction. Conversely, high expectations lead to a higher gap between expectations, confirmation, and lower satisfaction. We make the following hypotheses:

H4: *Users' extent of confirmation is positively associated with their satisfaction with the actual data security.*

It is considered that satisfaction is the key to building and maintaining a loyal base of long-term users [45]. Nevertheless, satisfaction is an effect recorded as a positive (satisfied), indifferent, or negative (dissatisfied) feeling. In order to identify the long-term effect of the survey measures, the IS continue component is integrated in order to be able to analyze a long-term influence on customer behavior. Under the consideration of the IS continued usage, a satisfied customer tends to continue to use the IS and vice versa. This has already been confirmed by Bhattacherjee [38], who found an influence of positive satisfaction on the continued use of the IS. We, therefore, assume the following hypothesis:

H5: *Users' level of satisfaction with the data security is positively associated with the users' IS continuance intention.*

4. Methodological Approach

A vignette design with an independent variable was created to test the defined hypotheses in an online experiment. The independent variables were queried by a scenario-based experimental manipulation with two variants, where one manipulation includes a privacy assurance statement and the other does not include one. Thereby it is possible to measure the effect of the assurance. The two scenarios were randomly assigned to the participants [46]. In terms of content, the scenarios differ in the aspect that, in one case, the company provides a high level of privacy assurance statement for their product, while in another case, this is omitted. In the following sections, we describe the data collection of the sample and the test design and the dependent measurements.

4.1 Procedure

In the survey, participants were asked to imagine that they had a fitness tracker that they regularly use for running. Activity tracking technologies include all portable electronic devices that can be used to record fitness and health-related data. In this study we focused on fitness tracker apps and watches. Participants were asked to imagine that they would use the tracker to run for the first time when a message appeared in front of operators explaining the need for personal data:

> *"Dear user, thank you for choosing our Fitness Tracker! In order to use the app, it is necessary that we collect the following personal data from you:*
>
> *E-mail address, Date of birth, Size, Weight, Running behavior via GPS, and registration of the credit card.[…]*
>
> *If you have any questions, please contact us."*

The experimental design includes two dimensions regarding the privacy assurance statement of the vendor. At random, participants received the second part (in place of […]) of the message containing the provider's security assurance of the personal data:

> *"The protection of your data is our top priority. For this purpose, we use the latest IT security technology. Thus, we can assure you that we always protect your data and avoid misuse."*

Subsequently, each participant received two manipulation check questions, one concerning the general scenario of receiving a message by the provider regarding the personal data ("The described message informs you that your new fitness tracker collects personal data"), and second a question addressing the assurance of the data in the message ("In the described message I am assured of the privacy of my data"). Additionally, the expectations regarding the security of the data were measured by a latent construct.

The survey continues, by a text that encourages the participant to imagine that he/she used the fitness tracker for a few months, as a new message by the provider pops up that showing that an unauthorized third party had violated some of his/her data:

> *"Dear user, we have discovered a security incident with your Fitness Tracker account on May 25, 2020. Some of your personal information was stolen by an unauthorized third party.*
>
> *The data accessed by a third party includes your name, email address, date of birth, and GPS data of your runs and your credit card information.*
>
> *If you have any questions, please contact us."*

The text provided was derived from real data breach responses that are publicly available. A questionnaire, including demographic assessment, followed this information.

4.2 Dependent Variable Measurement

All constructs described in the hypotheses were taken from established literature and adapted to the study's context. Expectation and continuance intention is adopted from Goode et al. [23], and the satisfaction is adjusted from Kantsperger and Kunz [47]. Each construct consists items checked for their consistency with the construct definition in this research context and their measurement quality. The loadings were checked to extend the threshold of 0.7 [48]. The loadings of the model are in the range of 0.749-0.913. The confirmation was measured by the single item "Overall, most of my expectations regarding the data security of the fitness tracker provider after the data misuse were confirmed." We further included some single-item control variables such as security concerns ("I have security concerns when using applications that collect personal information from me?"). All items were formulated in German and were measured in by a 7-step Likert scale from 1 (" fully disagree") to 7 ("fully agree"). The option "no answer" was not given.

4.3 Sample

The survey was conducted in June 2020 among university students. The participants needed about eight minutes to complete the questionnaire. Only fully completed surveys were considered. In addition, the data was cleaned up by removing invalid answers, e.g., participants who did not pass the attention checks. Overall, a sample size of n = 270 participants with age between 19 and 58 years (M=24.94, SD= 3.27 years) and 55.55% men and 44.44% women were used for the

analysis. The participants stated that they do sport-related activities on average 2.9 times a week and run on average 1.22 times per week. While running, 57.8% of respondents stated that they "occasionally" or more frequently (20% always) use a fitness tracker.

5. Data analysis and results

We test our hypotheses using a Partial Least Squares (PLS) structural equation modeling approach. In experimental research designs with latent variables, a structural equation model (SEM) is preferable over other methods because it can account for measurement errors and multidimensional structures of theoretical constructs [49]. As the PLS estimator offers advantages in terms of fewer restrictive assumptions [49], it finds broad application in experimental research designs [50]. The analysis was performed with the SmartPLS 3.0 software, and other calculations were performed with R (RStudio version 1.1456, R version 3.5.1).

5.1. Measurement Validation

As the dependent variables “expectation” and “satisfaction” are latent variables measures by constructs with items, we consider the validity and reliability of these constructs. The criteria composite reliability (CR) and average variance extracted (AVE) (see Table 1) are evaluated. The constructs need to exceed the threshold of the requirements. The CR value has to be larger than 0.7 and an AVE value larger than 0.5 [51]. In our model, all values are above the threshold. The AVE’s square root (see Table 1 bold value) is compared with the correlations between the constructs to assess the discriminatory validity [47]. All constructs have a higher value for the square root of the AVE than for the correlation with other constructs. Therefore, we conclude that our model has acceptable and significant measurement characteristics.

Table 1. Correlation and measurement validation

	CR	AVE	ASS	CON	EXP	SAT	CIN
ASS	n.a	n.a	**1**				
CON	n.a	n.a	-.228	**1**			
EXP	.883	.716	.325	-.574	**.846**		
SAT	.840	.725	.116	.201	-.221	**0.851**	
CIN	.895	.740	.146	-.138	.155	.283	**.860**

AVE = Average Variance Extracted; CR = Composite Reliability; ASS = Assurance; CON = Confirmation; EXP = Expectation; SAT= Satisfaction; CIN= Continuance Intention

5.2 Partial-Least Square Analysis

We used the PLS method to estimate the SEM. The bootstrapping re-sampling method with 5000 samples was used to assess the significance of the paths. The results of the calculation are shown in Figure 2 at the respective paths.

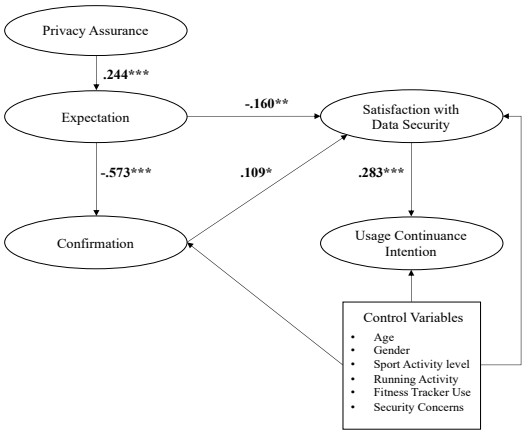

Figure 2. Structural model with path coefficient (Notes: * p<.10; **p<.05; ***p<.01)

The results show that all hypotheses can be supported. The analysis shows the privacy assurance statement has a positive effect on the pre-breach expectation towards the fitness tracker (0.224; significant at 0.01). Furthermore, the expectation negatively affects the confirmation, which was measured after the data breach (-0.573; significant at 0.01). Furthermore, the expectation negatively affects the satisfaction with the data security after the data (-0.160; significant at 0.05). Additionally, the confirmation has a positive effect on satisfaction (0.109; significant at 0.10). Lastly, the satisfaction with the data security passively affects the usage continuance intention of the fitness tracker (0.283; significant at 0.01). Therefore, all five hypotheses can be confirmed. Furthermore, the following control variables were used: age, gender, sports activity level, running activity level, use of a fitness tracker, and security concerns. All of them were tested through a direct effect on the dependent variable’s confirmation, satisfaction, and continuance intention. We identified that gender (0.227; significant at 0.01), security concerns (-0.227; significant at 0.01) and running activity level (-0.165; significant at 0.01) have an effect on continuance intention. None of the other control variables had a significant effect on the dependent variables.

6. Discussion

The following is a summary of the results. After that, the implications for theory, literature, and practice are discussed. Moreover, the limitations of the work and possibilities for future research are addressed.

6.1. Summary of findings

This paper examines how expectations of data security can be influenced to be as well prepared as possible in the event of a data breach and to continue experiencing positive customer behavior. In particular, the paper explains how privacy seals, using privacy assurance statements as an example, affect expectations and their impact on confirmation and satisfaction after a data breach. In summary, it can be said that privacy assurance statements influenced expectations. People who received a statement from the company regarding the security of their data had significantly higher expectations regarding the application's security. Therefore, a higher discrepancy with the confirmation could be identified after the data breach was announced. These expectations also had a negative influence on satisfaction with data security. However, the satisfaction with the data security had a positive effect on the continuance intention. It can be summarized that the topic is a current and highly relevant topic with strong practical relevance, although the possibility of influencing customer expectations after a data breach has not yet been investigated. So far, the impact of different strategies on data breaches has only been researched in the area of responses to data breaches. Consequently, this paper offers both theoretical and practical implications. However, this paper is not free of limitations but also provides opportunities for future research.

6.2. Implications for Theory and Contributions to Literature

This study provides a theoretical contribution by placing the ECT in a general theoretical context with the privacy assurance literature, adding an upstream construct for influencing expectations to the ECT. It is also shown that the theory is transferable and practical to other contexts, such as the fitness tracker example. This will generate a better understanding of the fact that expectations, as explained in the ECT, are a construct fixed in advance and can also be influenced by underlying mechanisms. It can be shown that a privacy assurance statement is a suitable mechanism to influence expectations and thus allows to create different effects along the theory paths. Furthermore, our study contributes to the existing literature. First, we could show that the literature around privacy assurance is applicable and thus transferable to the context of data breaches. Consequently, the present work can also complement the privacy seal literature, in which it could be shown that the use of privacy assurance statements does not always have a positive effect. The study represents a further step in the direction of long-term effects of privacy seals, in which it could be shown that privacy assurance statements do not have a positive effect on customer opinion and behavior in case of a data breach, but only a negative one. Secondly, we could expand the existing literature on data breaches. This could be achieved by investigating, through experimental research, how customer expectations, and thus customer behavior, can be influenced in the event of a data breach, which complements the existing security literature. It can illustrate how further research can explain customer reactions to help companies define data security communication strategies. While previous research has focused on how companies can prevent data breaches and how security policies are managed [52], research and companies need to understand and, if necessary, rethink mechanisms for influencing customer behavior in case of unfulfilled promises. It is also essential that research and practice address the problem, as data breaches are unavoidable and unplanned [53]. In addition, both companies and customers incur unplanned costs following a data breach, which could be reduced by appropriate practices [54].

6.3. Practical Implications

In addition to the theoretical contribution, the identified results help companies optimize their strategies for future company communication regarding data security and to adapt them in a way that ensures the best possible results even in case of a data breach. While Goode et al. [23], Greve et al. [25], and Masuch et al. [26] found that recovery actions can mitigate the generalized negativity effect of a data breach, this paper focuses specifically on how customers can be influenced in the run-up to a data breach not to perceive the negativity as strongly. As already mentioned, data protection violations can have fatal consequences for the affected companies. For example, data breaches can result in users not continuing to use the fitness tracker after a data breach but rejecting it. Therefore, it is relevant to investigate how to reduce the consequences of data breaches. The results of our study suggest that in this case, it is better not to offer customers any assurance regarding data security. A privacy assurance statement leads to a strong expectation that their data is completely secure on the part of the study participants. However, it is known from the literature that a company cannot guarantee total security (e.g., [53], [55]). If this security is nevertheless promised and broken in the end, this harms the expectation confirmation and the satisfaction and, therefore, the intention of the users to continue using the fitness tracker. Besides, it could be shown that satisfaction with data security always positively influences the continued use of the fitness tracker. This means that participants who did not completely expect

the fitness tracker's data security, because they did not receive a privacy assurance statement from the company, were more satisfied with the data security provided despite data breach. This resulted in a higher probability of continuing to use the fitness tracker. For this reason, companies should consider investigating customer expectations in the event of a potential data breach. They should also be aware that privacy assurance statements can also have negative consequences and therefore consider the right balance between data security insurance and no insurance. The probability of being affected by a data breach increases over time and digitalization.

6.4. Limitations and future research

Several significant limitations for interpreting the results must be taken into account when considering the presented study. Nevertheless, it also offers opportunities for future studies. The first limitation is that even if the data were reduced to the fact that participants often use a fitness tracker and put themselves in the scenario, it was a fictitious situation. This means that no actual data breach with a fitness tracker was investigated. In the best case, future studies will ideally also offer a comprehensive validation of measurements where participants are affected by a data breach. Besides, the same fictionality should be mentioned for the privacy assurance statement. Although the statement used was created based on actual company statements by fitness trackers regarding their data security, it is not a real statement. The experiment also focuses on privacy assurance statements. All other privacy seals are not considered. Therefore, it cannot be excluded that different formulations and other seals would have had a different effect on the expectation. This means that in the future, different formulations of privacy assurance statements, as well as different privacy seals, should be examined to determine the extent to which they affect expectations. In addition to the influence on expectations, participants' satisfaction was also surveyed and directly related to the continuance intention. Other variables that may also have a direct impact on customer behavior, such as loyalty, word of mouth, and trust, were not investigated. These should be taken up by future research to get a more precise overview of the long-term effects of influencing expectations. Finally, it is worth mentioning that the sample was taken from university students in Germany. Future research should consider a more diverse sample to identify cultural influences and an impact of the stricter data protection laws by the GDPR in Germany.

7. Conclusion

This study deals with the effects of privacy assurance statements on the expectations on fitness trackers' data security and how these different expectations influence the behavior after a data breach. By formulating a privacy assurance statement, the expectations of 270 study participants could be influenced. A SEM was used to analyze the data set collected in June 2020. This study's results provide valuable insights into the possibilities of influencing the expectations regarding the data security of fitness trackers using privacy assurance. It was shown that participants who received an assurance statement had higher expectations of the data security of the fitness tracker and were therefore significantly more dissatisfied with the data security after a data breach because their expectations were not confirmed. Also, they were often no longer willing to use the fitness tracker. Participants who had not received assurance from the company regarding their data security had lower expectations and were, therefore, less disappointed and thus more satisfied after a data breach so that they were more willing to continue using the fitness tracker. In summary, it can be concluded that customer expectations can be influenced in advance of a data breach to achieve better results after a data breach. It should be noted that privacy assurance statements do not always have a positive effect and should be used with caution.

8. References

[1] S. H. W. Chuah, P. A. Rauschnabel, N. Krey, B. Nguyen, T. Ramayah, and S. Lade, "Wearable technologies: The role of usefulness and visibility in smartwatch adoption," *Computers in Human Behavior*, vol. 65, no. August, 2016, pp. 276–284, doi: 10.1016/j.chb.2016.07.047.

[2] M. Kranz, A. Möller, N. Hammerla, S. Diewald, T. Plötz, P. Oliver, and L.Roalter, "The mobile fitness coach: Towards individualized skill assessment using personalized mobile devices," *Pervasive and Mobile Computing*, 2013, doi: 10.1016/j.pmcj.2012.06.002.

[3] L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, "The Rise of Consumer Health Wearables: Promises and Barriers," *PLoS Medicine*, vol. 13, no. 2, Feb. 2016, p. e1001953.

[4] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, vol. 20, no. 2, Jun. 1996, pp. 167–196, doi: 10.2307/249477.

[5] T. Zhou, "Understanding location-based services users' privacy concern," *Internet Research*, vol. 27, no. 3, Jun. 2017, pp. 506–519.

[6] M. R. Dickey, "Under Armour says MyFitnessPal data breach affected 150 million users | TechCrunch," 2018. https://techcrunch.com/2018/03/29/under-armour-says-myfitnesspal-data-breach-affected-150-million-users/ (accessed Aug. 10, 2019).

[7] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust," *Computers in Human Behavior*, vol. 28, no. 3, May 2012, pp. 889–897, doi: 10.1016/j.chb.2011.12.008.

[8] M. Mousavizadeh, D. J. Kim, and R. Chen, "Effects of assurance mechanisms and consumer concerns on online purchase decisions: An empirical study," *Decision Support Systems*, vol. 92, Dec. 2016, pp. 79–90, doi: 10.1016/j.dss.2016.09.011.

[9] M. Arcand, J. Nantel, M. Arles-Dufour, and A. Vincent, "The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust," *Online Information Review*, 2007, doi: 10.1108/14684520710832342.

[10] J. Liu and W. Sun, "Smart Attacks against Intelligent Wearables in People-Centric Internet of Things," *IEEE Communications Magazine*, vol. 54, no. 12, Dec. 2016, pp. 44–49.

[11] G. Piccoli, J. Rodriguez, B. Palese, and M. Bartosiak, "The Dark Side of Digital Transformation: The case of Information Systems Education," in International Conference on Information Systems 2017.

[12] H. Haddadi and I. Brown, "Quantified self and the privacy challenge," *Technology Law Futures*, 2014.

[13] A. Behne and F. Teuteberg, "A Healthy Lifestyle and the Adverse Impact of its Digitalization : The Dark Side of Using eHealth Technologies," 2020.

[14] Hui, Teo, and Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, vol. 31, no. 1, 2007, p. 19, doi: 10.2307/25148779.

[15] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," *Journal of Computer Security*, vol. 11, no. 3, 2003, pp. 431–448, doi: 10.3233/JCS-2003-11308.

[16] M. L. Ettredge and V. J. Richardson, "Information Transfer among Internet Firms: The Case of Hacker Attacks," *Journal of Information Systems*, vol. 17, no. 2, Sep. 2003, pp. 71–82, doi: 10.2308/jis.2003.17.2.71.

[17] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, 2004, pp. 70–104, doi: 10.1080/10864415.2004.11044320.

[18] A. Hovav and J. D'Arcy, "The Impact of Virus Attack Announcements on the Market Value of Firms," *Information Systems Security*, vol. 13, no. 3, May 2004, pp. 32–40.

[19] A. A. Yayla and Q. Hu, "The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors," *Journal of Information Technology*, vol. 26, no. 1, Mar. 2011, pp. 60–77, doi: 10.1057/jit.2010.4.

[20] L. M. Butcher-Powell, "Better Securing an Infrastructure for Telework," *Journal of Cases on Information Technology*, vol. 8, no. 4, Oct. 2006, pp. 71–86, doi: 10.4018/jcit.2006100106.

[21] S. Goode, C. Lin, J. C. Tsai, and J. J. Jiang, "Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers," *Decision Support Systems*, vol. 70, Feb. 2015, pp. 73–85, doi: 10.1016/j.dss.2014.12.005.

[22] A. C. Johnston and M. Warkentin, "Fear appeals and information s ecurity behaviors: An empirical study," *MIS Quarterly: Management Information Systems*, vol. 34, no. 3, 2010, pp. 549–566.

[23] S. Goode, H. Hoehle, V. Venkatesh, and S. A. Brown, "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach," *MIS Quarterly*, vol. 41, no. 3, 2017, pp. 703–727, doi: 10.25300/misq/2017/41.3.03.

[24] T. Kude, H. Hoehle, and T. A. Sykes, "Big data breaches and customer compensation strategies," *International Journal of Operations & Production Management*, vol. 37, no. 1, Jan. 2017, pp. 56–74, doi: 10.1108/IJOPM-03-2015-0156.

[25] M. Greve, K. Masuch, and S. Trang, "The More, the Better? Compensation and Remorse as Data Breach Recovery Actions – An Experimental Scenario-based Investigation," in *WI2020 Zentrale Tracks*, GITO Verlag, 2020, pp. 1278–1293.

[26] K. Masuch, M. Greve, and S. Trang, "Does It Meet My Expectations? Compensation and Remorse as Data Breach Recovery Actions-An Experimental Scenario Based Investigation," in *European Conference on Information Systems* 2019.

[27] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems*, vol. 12, no. 12, Dec. 2011, pp. 798–824, doi: 10.17705/1jais.00281.

[28] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model.," *Information Systems Research*, vol. 15, no. 4, 2004, pp. 336-355.

[29] W. Hong and J. Y. L. Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly*, vol. 37, no. 1, Jan. 2013, pp. 275–298, doi: 10.25300/MISQ/2013/37.1.12.

[30] G. R. Milne and M. J. Culnan, "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys," *The Information Society*, vol. 18, no. 5, Oct. 2002, pp. 345–359, doi: 10.1080/01972240290108168.

[31] G. R. Milne and M. J. Culnan, “Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices,” *Journal of Interactive Marketing*, vol. 18, no. 3, Jan. 2004, pp. 15–29, doi: 10.1002/dir.20009.

[32] E. Singer, H.-J. Hippler, and N. Schwarz, “Confidentiality assurances in surveys: reassur- ance or threat?,” *International Journal of Public Opinion Research*, vol. 4, no. 3, 1992, pp. 256–268.

[33] F. Belanger, J. S. Hiller, and W. J. Smith, “Trustworthiness in electronic commerce: the role of privacy, security, and site attributes,” *The Journal of Strategic Information Systems*, vol. 11, no. 3–4, Dec. 2002, pp. 245–270, doi: 10.1016/S0963-8687(02)00018-5.

[34] R. L. Oliver, “Effect of expectation and disconfirmation on postexposure product evaluations: An alternative interpretation,” *Journal of Applied Psychology*, vol. 62, no. 4, 1977, pp. 480–486.

[35] R. L. Oliver, “A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions,” *Journal of Marketing Research*, vol. 17, no. 4, 1980, pp. 460–469.

[36] S. A. Brown, V. Venkatesh, and S. Goyal, “Expectation Confirmation in Information Systems Research: A Test of Six Competing Models,” *MIS Quarterly*, vol. 38, no. 3, 2014, pp. 729–756.

[37] V. Venkatesh and S. Goyal, “Expectation Disconfirmation and Technology Adoption: Polynomial Modeling and Response Surface Analysis,” *MIS Quarterly*, vol. 34, no. 2, 2010, pp. 281–303.

[38] A. Bhattacherjee, “Understanding information systems continuance: An expectation-confirmation model,” *MIS Quarterly*, vol. 25, no. 3, 2001, pp. 351–370.

[39] P. G. Irving and J. P. Meyer, “Reexamination of the met-expectations hypothesis: A longitudinal analysis.,” *Journal of Applied Psychology*, vol. 79, no. 6, 1994, pp. 937–949, doi: 10.1037/0021-9010.79.6.937.

[40] J. P. Wanous, T. D. Poland, S. L. Premack, and K. S. Davis, “The effects of met expectations on newcomer attitudes and behaviors: A review and meta-analysis.,” *Journal of Applied Psychology*, vol. 77, no. 3, Jun. 1992, pp. 288–297, doi: 10.1037/0021-9010.77.3.288.

[41] B. L. Delgado-Márquez, N. E. Hurtado-Torres, and J. A. Aragón-Correa, “On the Measurement of Interpersonal Trust Transfer: Proposal of Indexes,” *Social Indicators Research*, vol. 113, no. 1, Aug. 2013, pp. 433–449, doi: 10.1007/s11205-012-0103-z.

[42] Y. Lu, S. Yang, P. Y. K. Chau, and Y. Cao, “Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective,” *Information & Management*, vol. 48, no. 8, Dec. 2011, pp. 393–403, doi: 10.1016/j.im.2011.09.006.

[43] K. J. Stewart, “Trust Transfer on the World Wide Web,” *Organization Science*, vol. 14, no. 1, Feb. 2003, pp. 5–17, doi: 10.1287/orsc.14.1.5.12810.

[44] H. J. Eysenck, “Adaptation-level theory: An experimental and systematic approach to behavior,” *Behaviour Research and Therapy*, vol. 4, no. 1–2, 1966, p. 69, doi: 10.1016/0005-7967(66)90044-1.

[45] C. L. Anderson, R. Agarwal, and C. L. Anderson, “The Digitization of Healthcare: Boundary Risks , Emotion , Information,” *Information Systems Research*, vol. 22, no. 3, 2011, pp. 469–490.

[46] C. Atzmüller and P. M. Steiner, “Experimental vignette studies n survey research,” *Methodology*, vol. 6, no. 3, 2010, pp. 128–138, doi: 10.1027/1614-2241/a000014.

[47] R. Kantsperger and W. H. Kunz, “Consumer trust in service companies: a multiple mediating analysis,” *Managing Service Quality: An International Journal*, vol. 20, no. 1, 2010, pp. 4–25, doi: 10.1108/09604521011011603.

[48] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling*. SAGE, 2014.

[49] R. P. Bagozzi and Y. Yi, “On the evaluation of structural equation models,” *Journal of the Academy of Marketing Science*, vol. 16, no. 1, Mar. 1988, pp. 74–94, doi: 10.1007/BF02723327.

[50] P. W. Fombelle, S. A. Bone, and K. N. Lemon, “Responding to the 98%: face-enhancing strategies for dealing with rejected customer ideas,” *Journal of the Academy of Marketing Science*, vol. 44, no. 6, 2016, pp. 685–706, doi: 10.1007/s11747-015-0469-y.

[51] N. Urbach and F. Ahlemann, “Structural Equation Modeling in Information Systems Research Using Partial Least Squares,” *Journal of Information Technology Theory and Application (JITTA)*, vol. 11, no. 2, 2010, pp. 5–40.

[52] S. Romanosky, D. Hoffman, and A. Acquisti, “Empirical Analysis of Data Breach Litigation,” *Journal of Empirical Legal Studies*, vol. 11, no. 1, Mar. 2014, pp. 74–104, doi: 10.1111/jels.12035.

[53] A. Evdokimov, “What It Takes to Be a CISO: Success and Leadership in Corporate IT Security.,” 2018. .

[54] K. M. Gatzlaff and K. A. McCullough, “The Effect of Data Breaches on Shareholder Wealth,” *Risk Management and Insurance Review*, vol. 13, no. 1, Mar. 2010, pp. 61–83, doi: 10.1111/j.1540-6296.2010.01178.x.

[55] H. Cavusoglu, B. Mishra, and S. Raghunathan, “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers,” *International Journal of Electronic Commerce*, vol. 9, no. 1, Oct. 2004, pp. 70–104, doi: 10.1080/10864415.2004.11044320.