Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2022 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-11-2022

Choose your words wisely! Understanding the strategic communication of differential privacy

Aycan Aslan
University of Goettingen, aycan_aslan@uni-goettingen.de

Maike Greve
University of Goettingen

Till Ole Diesterhoeft
University of Goettingen

Follow this and additional works at: https://aisel.aisnet.org/wisp2022

Recommended Citation

Aslan, Aycan; Greve, Maike; and Diesterhoeft, Till Ole, "Choose your words wisely! Understanding the strategic communication of differential privacy" (2022). *WISP 2022 Proceedings*. 3.
https://aisel.aisnet.org/wisp2022/3

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Choose Your Words Wisely! Understanding the Strategic Communication of Differential Privacy

Aycan Aslan[1]
University of Goettingen,
Goettingen, Lower Saxony, Germany

Maike Greve
University of Goettingen,
Goettingen, Lower Saxony, Germany

Till Ole Diesterhoeft
University of Goettingen,
Goettingen, Lower Saxony, Germany

ABSTRACT

As a possible solution addressing the growing tension for companies on wanting to collect data and not upset their customers through adverse events simultaneously, differential privacy (DP), an approach that allows the collection of data while ensuring privacy, is gaining in popularity. As many companies increasingly engage in deploying DP, they consequently try to communicate such efforts to their consumers. However, compared to traditional measures, DP has unique characteristics which pose special challenges in its communication. Despite this, prior research did not sufficiently address the user-perspective on DP. Consequently, we adopt an elaboration likelihood lens to investigate how two prevalent descriptions of DP are perceived. By conducting a between-subjects experiment (n=264) we identify powerful mediating effects in the perception of DP, not known before. We contribute to literature by demonstrating the full-mediation of these effects, and to practice by depicting how these can be incorporated in a successful communication strategy.

Keywords: Differential Privacy, Differential Privacy Communication, Elaboration Likelihood Model.

[1] Corresponding author. aycan_aslan@uni-goettingen.de, +49 0551 3921171

INTRODUCTION

"Incorporating differential privacy broadly into Apple´s technology is visionary, and positions Apple as the clear privacy leader" (Schroeder 2016).

This quote by Prof. Aaron Roth, a leading privacy researcher, was proudly presented by Craig Federighi the Vice President of software engineering at Apple, during a Conference (Schroeder 2016). The shown quote illustrates, which value differential privacy (DP) has for Apple in the context of its privacy and overall business strategy. Simply put, DP describes the modification of a dataset to reduce information about individuals while retaining the capability of statistical reasoning about the data (Hu et al. 2019). Besides Apple, a lot of influential companies, such as Microsoft or Google, test and deploy DP and respectively communicate that to their consumers (Cummings et al. 2021), which displays that DP, a novel privacy technique is purposefully communicated by companies to the public and directly to their consumers. Hence, with the growing relevance of DP and the respective communication of such through companies to their consumers, DP has increasingly become the subject of a wider public discourse. However, to this date, the consumer perception of DP is largely unclear.

This communication is further complicated by the unique properties of DP compared to traditional privacy techniques. While traditional privacy measures usually provide binary privacy (private or not private) and therefore are fairly easy to communicate, DP provides a statistical boundary on how much information can leak about individuals (Dwork and Roth 2013). Given these unique challenges present, the question arise how companies engage in communicating DP and how the respective communication is perceived by consumers. In this context, there are prior studies that analyze the influence of communicating DP, however with different findings. While some studies conclude that DP can positively influence the intention to disclose personal

information (Xiong et al. 2020), others comes to the opposite result and states that the communication of DP itself does not influence the intention to disclose information (Cummings et al. 2021). Driven by the increasing relevance of DP and these contradictory results, the goal of this paper is to deepen the understanding of DP communication by revealing possible mediating effects in the perception of DP. Hence, we state the following research questions (RQ):

RQ1*: What is the influence of communicating DP and its benefits to consumers?*

RQ2*: What are mediating effects in this DP perception by consumer?*

To answer these research questions, we will draw on current DP literature to present two descriptions of DP, which are representative of real-world DP descriptions. We conduct a vignette-study through an online experiment (n=264), to investigate the effects of the respective descriptions on the perception of consumers. Here, we utilize the elaboration likelihood model as our theoretical lens to derive an understanding of how the two descriptions of communicating DP is processed. We find that while the communication of DP itself does not have a direct influence on the intention do disclose information, *technical effectiveness* and *transparency* act as powerful mediators. We contribute to literature by showing mediating effects in the perception of DP, which were formerly unknown and provide implications for practice with showing factors that must be managed and addressed for a successful DP communication strategy for companies.

RESEARCH BACKGROUND

This section will provide the theoretical and conceptual background for our work, terms of understanding DP in detail and reviewing DP communication.

Differential Privacy and its Communication

DP was proposed by Dwork and Roth (2013) and is formally defined as follows:

$$\Pr[M(D1) \in S] \leq \exp(\varepsilon) \Pr[M(D2) \in S] + \delta]$$

where the difference between both datasets is identical but only differs in epsilon (ε) and delta (δ), the so-called privacy parameters. Therefore, the modification of one dataset is achieved by a noise-adding mechanism, i.e., primarily changes to epsilon. DP has several unique characteristics when compared to traditional privacy techniques. DP allows for the distinct quantification of privacy itself (Dwork and Roth 2013). As traditional privacy techniques are usually heuristic-based techniques, they do not provide provable guarantees regarding the level of privacy ensured. However, DP provides a privacy budget whereby the privacy loss is quantifiable and therefore statistically bounded. While research on DP communication is scarce, our review identified multiple relevant studies for our work. For example, prior studies have analyzed how the understanding of DP of lay consumers influences their willingness to share information (Xiong et al. 2020). Additionally, prior studies have collected and categorized DP descriptions by companies, to generate main themes in the communication of DP (Cummings et al. 2021). Reviewing these themes, we note that the descriptions generally vary with the level of technicality displayed, whereby some are more technical than others. Some companies focus on explaining the technical and mathematical characteristics of DP, while others focus on explaining what DP enables them to do and emphasize the benefit of DP for the consumer.

In summary, DP is fairly technical and complex, as its privacy protection is dependent on parameters in a mathematical formula. However, these technical characteristics, are the foundation for the benefits that DP offers. The communication of DP can be grouped into technical descriptions and descriptions which focus on the benefit for the consumer.

Investigating DP Communication through the Elaboration Likelihood Lens

When we try to understand how humans process and judge information, prior literature demonstrates, that humans engage in so-called dual-processes (Maheswaran and Chaiken 1991).

These processes depict that information can be processed in two ways: One effortful processing when capacity to process the given information is high, and one low-effort processing when capacity is low (Gerlach et al. 2019). A prominent representative of such is the elaboration likelihood model (ELM). The ELM is based on the idea, that when a message is presented to individuals, the recipients will vary how much cognitive energy they devote to processing the message, leading to two routes: A high effort central route which reflects a deep engagement and a low-effort peripheral route that relies on cues and heuristics in analyzing the message.

Table 1. Instantiation of Real-World DP Descriptions through the ELM Lens

Theory	Instantiation	Differential privacy description	Company
Central	*Technical*	"At its core, differential privacy operates by adding enough random noise to data such that there are mathematical guarantees of individuals' protection from reidentification. As such, the results of analysis are the same whether or not a given individual is included in the data, meaning that people have plausible deniability that their information is contained within it."	Meta (Nayak 2020)
Peripheral	*Benefit*	"This technology can help Huawei improve relevant services and products and avoid collecting information related to you."	Huawei (Huawei 2022)

In this context, we argue that the communication of DP can be analyzed through the lens of the ELM. Therefore, based on the analyzed literature on the communication of DP, we can derive two prevalent DP descriptions: **1) Technical description**, and **2) Benefit description**. Here, the technical description includes information regarding the statistical working of DP and the resulting strong mathematical boundaries offered. Whereas the benefit description covers information regarding what is enabled using DP. In our context, the technical description reflects the central route, while the benefit description reflects the peripheral route. As can be seen in Table 1 through real-world examples, the technical description of DP contains dense technical lingo which require higher levels of cognitive energy, hence we assume that consumers will recognize the technical benefits offered by DP. In contrast, benefit description reflects the peripheral route since recipients can rely stronger on heuristics, such as the communication of the benefits of DP deployment. Understanding our descriptions within the central and peripheral

route can help us to deepen our understanding on how the different routes influence the cognitive processes that are in play when the consumer is exposed to them, as the respective processing is different, why different mediators must be considered (Gerlach et al. 2019).

HYPOTHESIZING THE EFFECTS OF DP COMMUNICATION

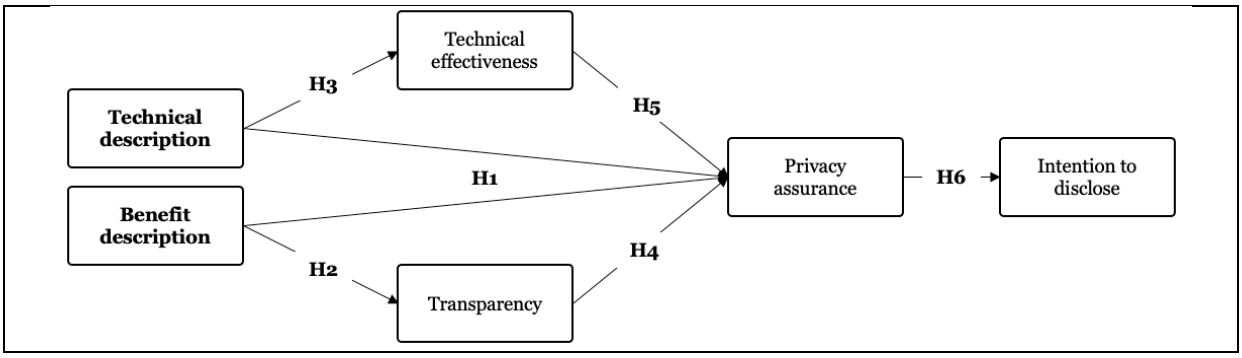

Figure 2. Proposed Research Model

Before proceeding to the proposed research model with its respective hypotheses, the relevant constructs of investigation are clarified. As constructs that will be tested for their mediating effects for the descriptions, we will investigate *technical effectiveness* and *transparency*. Technical effectiveness describes to which degree the deployed privacy technology is perceived as effective and technically reliable of protecting consumers. Transparency describes the level to which consumers can assess in which form their data is being used by the company. Moreover, we will utilize the constructs *privacy assurance* and *intention to disclose*. While privacy assurance depicts to which degree the consumers feel protected by the deployed privacy measure, intention to disclose describes the intention of consumers to disclose information given the deployed privacy measure. The research model can be seen in Figure 2.

Considering the protection offered by DP against the possibility of data leakages (Kaissis et al. 2020), we argue that the communication of DP will increase the confidence of consumers in the level of privacy guaranteed, i.e. privacy assurance. As prior studies have demonstrated, consumer value being protected against privacy threats by protective privacy measures (Bansal et

al. 2015). Consequently, as the probability of privacy threats can be reduced through the deployment of DP, we argue that this will increase their perceived level of privacy assurance, given that they are informed that DP is being used. Hence, we hypothesize that:

Hypothesis 1: The communication of differential privacy increases the consumers perceived confidence in the privacy protection and therefore the level of privacy assurance.

Building on the ELM, we derive that the information processing conducted in the peripheral route is characterized by lower levels of cognitive energy invested (Angst and Agarwal 2006; Petty and Cacioppo 1986). As stated, this results in the consumers relying more heavily on heuristics. To trigger this mental shortcut, we argue that level of transparency displayed plays an important role. For the consumers to evaluate whether the communicated DP descriptions represents a benefit for them, the communication must first make transparent and traceable what the benefits of deploying DP are. Hence, we hypothesize that:

Hypothesis 2: Communicating the benefit description of DP will increase consumers perception of the level of transparency on how their data is being used.

Building further on the ELM, we know that the central route is characterized by deep engagement with the shown information (Bansal et al. 2008; Petty and Cacioppo 1986). Mapping this to our context, we note that a high level of cognitive energy is needed to comprehend the dense technical lingo used in the technical description. However, if such high level of cognitive energy is given and the consumer engages in the systematic consideration of the information presented, we can expect that the technical benefits of DP will be recognized. As stated prior, in the context of DP, these technical benefits consist in being technically robust through mathematical boundaries. Hence, we argue that when this technical robustness is communicated

to consumers, it will have an influence on how technically potent of a privacy measure, i.e., technical effectiveness, DP is perceived. Hence, we hypothesize that:

Hypothesis 3: Communicating the technical description of DP will increase consumers perception of the technical effectiveness of DP as the mathematical guarantees become apparent.

As stated in the derivation of H1, one factor in the formation of privacy assurance is the level of uncertainty perceived by the consumers regarding the privacy measure deployed. One way to address this uncertainty which influences the privacy assurance perceived, is to ensure sufficient levels of transparency. We argue, that if companies make transparent how the data of the consumer is being handled and analyzed, this increase in transparency will reduce possibly present uncertainty of consumers. When such uncertainty of consumers is proactively addressed by the company by making their data use transparent, they reduce the probability that the consumers get worried about adverse ways in which companies might handle and use their personal data, which is supported by prior studies (Tan et al. 2014). Hence, we hypothesize that:

Hypothesis 4: Higher levels of perceived transparency will have a positive influence on the level of privacy assurance as it addresses possible uncertainty regarding the data use.

In line with our argumentation for H4, we argue that the level of technical effectiveness influences the uncertainty that consumers perceive with respect to the deployed data privacy measure. We argue that the level of technical efficiency will influence privacy assurance, since reliable privacy measures reduce the uncertainty of possible adverse events for consumers regarding their data. When the communicated privacy measures are perceived as technically potent in protecting them, consumers will feel safer against adverse events as the privacy measures act as a "firewall" for them, which is supported by prior studies (Dinev et al. 2016). Hence, we hypothesize that:

Hypothesis 5: Higher levels of technical effectiveness perceived will have a positive influence on the level of privacy assurance as consumers feel safer against adverse events.

Considering that privacy assurance represents the level of confidence that consumers have in privacy measures deployed, we argue that this will influence the intention to disclose personal information with the company. We know that consumer value their personal information and balance when they share those and when not (Cichy et al. 2017). In this internal decision-making whether to disclose information or not, we argue that the confidence in the privacy measures employed is an important factor. As consumers evaluate risks that might occur if they share their data, such as leakages or breaches, one important factor is how they evaluate the measure that would protect them against such risks. This argument is supported by prior studies as well and shows that privacy assurance is a strong antecedent for the intention to disclose information (Cichy et al. 2017; Yun et al. 2014). Thus, we hypothesize:

Hypothesis 6: Higher levels of privacy assurance will have a positive influence on the intention to disclose information as consumers feel sufficiently protected.

RESEARCH DESIGN AND EXPERIMENTAL SETTING

To validate the derived hypotheses, we conducted a 2x2 between-subject, full-factorial design in an online scenario experiment. To test our stated hypotheses with regard to the descriptions of DP, we opted for a scenario in which a learning app is downloaded and supposed to be used (see Table 2). This impartial scenario was chosen, to highlight and analyze findings regarding the description of DP, rather than contextual factors such as the type of app used. The participants surveyed were recruited from Prolific. After removing 21 responses due to being incomplete or missing build in attention checks, the final sample contained 264 survey responses. We surveyed and obtained constructs, control variables, and demographic

information. Manipulation and attention checks were performed to ensure participants were able to relate to the scenario. The survey was conducted in March 2022.

Table 2. Scenario Setting

Introduction

Imagine that you have downloaded the learning app "EazyLearn" from the App store, in order to explore and learn new skills.
Upon starting the app, you get notified that the app would like to collect some personal information before starting and collect your usage data while interacting and using the "EazyLearn" app. The "EazyLearn" app informs you, that the collection of data and respectively you sharing your data, is essential for using the app in the first place and ensuring a high-quality user experience.

Control scenario (n=68)

With regard to the respective data privacy measure, you get following information:

In the context of this app, your data will be protected using appropriate data privacy measures.
Control

Scenario with technical description (n=54)

With regard to the respective data privacy measure, you get following information:

In the context of this app, your data will be protected using an appropriate data privacy measure, which means that we use "Differential Privacy".

Differential Privacy is a privacy technique that provides *formal mathematical privacy guarantees* by introducing *statistical noise*. Compared to traditional privacy methods, it provides *provable mathematical guarantees and boundaries* with regard to possible information leakage.

Scenario with benefit description (n=74)

With regard to the respective data privacy measures, you get following information:

In the context of this app, your data will be protected using an appropriate data privacy measure, which means that we use "Differential Privacy".

Differential Privacy allows for protecting the privacy of your personal user data, while *still gaining valuable insights for us as a service provider*. These insights are used to *further improve the services for you*, in a private manner.

Scenario with technical and benefit description (n=68)

With regard to the respective data privacy measure, you get following information:

In the context of this app, your data will be protected using an appropriate data privacy measure, which means that we use "Differential Privacy".

Differential Privacy is a privacy technique that provides *formal mathematical privacy guarantees* by introducing *statistical noise*. Compared to traditional privacy methods, it provides *provable mathematical guarantees and boundaries* with regard to possible information leakage.
Differential Privacy allows for protecting the privacy of your personal user data, while *still gaining valuable insights for us as a service provider*. These insights are used to *further improve the services for you*, in a private manner.

The survey started for each participant with the introduction text (see Table 2). Following this introduction, participants were randomly assigned to one of four scenarios, which represented the control scenario, the scenario with the technical descriptions, scenario with benefit description and the combination of both descriptions. The descriptions were designed based on the literature and real-world examples presented (see Table 1). The participants were asked to put themselves in the situation of downloading an app to explore and learn new skills. However, when starting the app, they get informed, that the app would like to collect personal user information. Subsequently, each participant received the same questionnaire to measure the dependent variables and manipulation control. To measure the perceived DP communication, we included two single items in the survey. Both statements had to be evaluated by the participants on a seven-point Likert scale (1 = Strongly disagree, 7 = Strongly agree).

DATA ANALYSIS AND RESULTS

In order to test the presented research model with the presented hypotheses, we deployed the partial least squares structural equation modeling (PLS-SEM) approach (Hair et al. 2011). Given the novel investigation regarding the perception of different description of DP, our study pertains to an exploratory investigation. Hence, PLS-SEM is suitable for our context as we can focus on the effects between the investigated latent variables (Goodhue et al. 2012).

Table 3. Construct Measurement, Reliability, and Convergent Validity

Constructs and Items	Loadings
Technical effectiveness (α = .970, CR = .980, AVE = .943) (Dinev et al. 2016)	
I think that the "EazyLearn" app uses an effective privacy technology to protect my privacy.	.972
I think that the "EazyLearn" app uses a reliable privacy technology to protect my privacy.	.976
I think that the used privacy measure is a good technology to protect my privacy.	.967
Transparency (α = .935, CR = .951, AVE = .794) (Schnackenberg et al. 2021)	
The deployed data privacy measure is well traceable.	.827
The deployed data privacy measure is clear.	.917
The approach of the deployed data privacy measure was transparent to me.	.911
The relevant information with regard to the data privacy measure have been provided.	.912
I have all the information I need with regard to the deployed data privacy measure.	.886
Privacy assurance (α = .961, CR = .972, AVE = .896) (McKnight et al. 2002)	
The "EazyLearn" app has enough privacy safeguards to make me feel comfortable using it.	.931
I feel assured that the deployed data privacy measure adequately protects me from problems.	.957
I feel confident that the deployed data privacy measure makes it safe to interact with the app.	.966
In general, due to the deployed data privacy measure the "EazyLearn" app is a robust and safe environment.	.931
Intention to disclose (α = .934, CR = .958, AVE = .884) (Malhotra et al. 2004)	
The extent to which I would reveal my information to the “EazyLearn” app is: (Extremely unlikely - extremely likely)	.956
The extent to which I would reveal my information to the “EazyLearn” app is: (Not probable – very probable)	.942
The extent to which I would reveal my information to the “EazyLearn” app is: (Very unwilling – very willing)	.922

α – Cronbach’s alpha, CR – Composite Reliability, AVE – Average Variance Extracted. Unless indicated otherwise, items were measured on a 7-point Likert scale (1 = Strongly disagree, 7 = Strongly agree).

For the measurements of the constructs, all items were adapted based on literature and adjusted to our context. In order to follow presented best practices, before analyzing the structural model, we assessed the validity and reliability of the model (Fornell and Larcker 1981). Therefore, ensuring indicator reliability, internal consistency reliability, convergence validity, and discriminant validity. Therefore to address respective indicator reliability, we checked that the indicators of the constructs explain more variance than the measurement error (Hair et al. 2019). This is given for all used items (see Table 3).

Table 4. Discriminant Validity

	Technical effectiveness	Transparency	Privacy assurance	Intention to disclose
Technical effectiveness	**0.971**	*0.762*	*0.867*	*0.696*
Transparency	0.726	**0.891**	*0.746*	*0.540*
Privacy assurance	0.838	0.706	**0.946**	*0.734*
Intention to disclose	0.665	0.507	0.697	**0.940**

FL-criterion in bold, HTMT in italics

Structural Model Results

The structural model shows that there is no significant relationship between both technical description and benefit description directly with privacy assurance (**H1 is not supported)**. However, even more interestingly our model shows that the effect of the descriptions is mediated by technical effectiveness and transparency. Our results show that the technical description has a positive effect on technical effectiveness (β=.260, p<.001) and the benefit description has a significant positive effect on transparency (β=.407, p<.001), **supporting H2 and H3**. Our model shows that technical effectiveness (β=.689, p<.001) and transparency (β=.226, p<.001) have a positive effect on privacy assurance, **supporting H4 and H5.** Finally, our model shows that assurance increases intention to disclose (β=.697, p<.001), **supporting H6**.

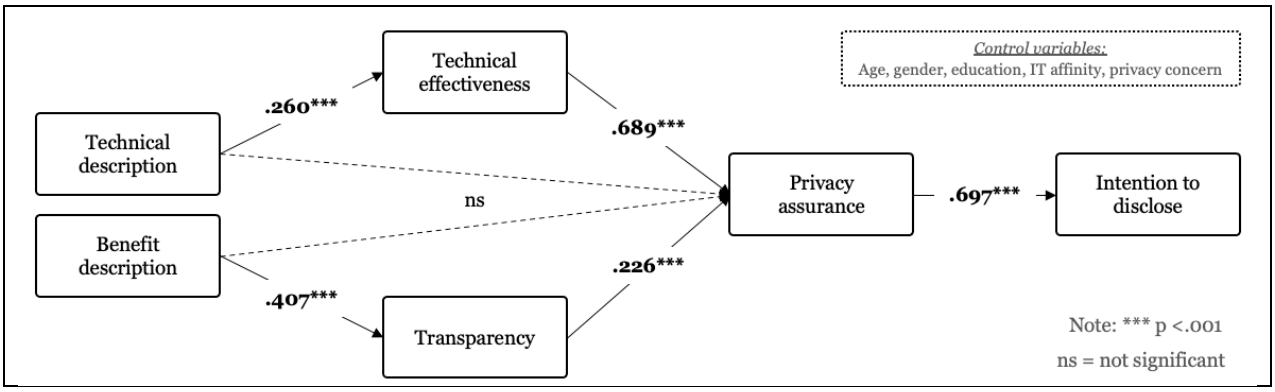

Figure 3. Structural Model

We further controlled for some additional effect on our dependent variables privacy assurance and intention to disclose: Age, gender, education, and IT affinity do not have a significant effect on both dependent variables, while general privacy concern has a negative significant effect on the intention to disclose (β=-.151, p<.001), which is to be expected.

Mediation Analysis

As previous literature on the effect of DP has neglected possible mediating effects, conducting a respective mediation analysis provides valuable insights. Here, we see that for both technical and benefit description a full mediation can be statistically shown. For the indirect effect of the technical description on privacy assurance **(Technical description → Technical effectiveness → Privacy assurance)** we note a positive significant effect via technical effectiveness (β=.179, p<.001). Consequently, this results in a full mediation effect of the technical description on privacy assurance via technical effectiveness. As for the indirect effect of the benefit description on privacy assurance **(Benefit description → Transparency → Privacy assurance)** we find a positive effect through the mediating effect of transparency (β=.092, p=.002). Therefore, there is a full mediation effect for the benefit description on privacy assurance, since H1 was not supported. Going one step farther, the indirect effects of the descriptions on the intention to disclose information is investigated. For the indirect effect of technical description on intention to disclose **(Technical description → Technical effectiveness → Privacy assurance → Intention to disclose)** we note a serially mediating effect through technical effectiveness and privacy assurance (β=.125, p<.001). Similarly, there is an indirect effect of the benefit description on intention to disclose **(Benefit description → Transparency → Privacy assurance → Intention to disclose)** which is serially mediated through transparency and privacy assurance (β=.064, p=.003). These pathways fully accounted for the overall impact of the two descriptions on intention to disclose as the direct effects being insignificant.

DISCUSSION

As prior literature showed that companies vary in the level of technicality they communicate regarding DP, a thorough understanding of how technical and benefit descriptions are perceived, and mediating effects in this perception were unclear. Addressing the stated research question, our results, in particular the mediation analysis, show that technical effectiveness, transparency, and privacy assurance function as powerful mediating effects. Highly important to note is, that there is not a significant effect of DP communication (both via technical and benefit description) on privacy assurance, when mediating effects are left out.

Contribution to Literature and Practice

Our work and findings contribute to literature and practice in several ways. We contribute to literature by demonstrating the role of mediating effects for DP communication. While prior research on the communication of DP focused on direct effects, mediating effects in the perception of DP were not sufficiently covered (Bullek et al. 2017; Cummings et al. 2021). We fill this gap in academic literature by respectively showing one powerful mediating path for the technical and benefit description. These findings can be used to build upon with the investigation of further mediating effects in future studies. Hence, we can emphasize that mediating effects provide a statistical indication on how DP communication influences consumer behavior (i.e., perceived level of privacy assurance or the intention to disclose personal information). Additional to the contributions to literature, our work also has several managerial implications. Our results show that the details in which companies communicate matter. Our findings show that the communication of DP itself is not sufficient. Companies rather must actively engage in building a DP communication strategy, with respect to the DP feature that is supposed to be communicated to the consumer. Here, considering the unique DP feature they are trying to communicate, the communication strategy must involve and address the respective mediating

effects identified in our work. If companies wish to describe the mathematical rigor in form of a technical description, they should address the perceived technical effectiveness accordingly. However, if companies want to address the possibility of privately improving products and services to increase the intention to disclose information, they should address transparency.

Limitations and Opportunities for Future Research

Besides our demonstrated contribution, we note an important area in which future research could strengthen and extend our results. We recognize that in our experiment, the respective formulation of descriptions is crucial, why different formulations might lead to other effects. However, in designing our descriptions we followed both prior literature on DP communication themes presented by literature and real-world examples how companies communicate DP. Therefore, we are convinced that the presented results are representative for the respective descriptions. Nevertheless, future research should experiment with different formulations and framing of DP to investigate further interesting aspects in the perception of DP.

CONCLUSION

In conclusion, our work provides valuable insights into the communication and the respective perception of DP. We demonstrate that for the successful communication of DP, respective mediating effects must be considered. We show that technical effectiveness for the technical description and transparency for the benefit description act as powerful mediators that impact the level of privacy assurance. The achieved higher levels of privacy assurance ultimately led to higher levels of intention to disclose personal information. Therefore, our study suggests highly practically relevant insights for the communication of DP, a privacy measure that is gaining in popularity in both academic discussion and company use.

REFERENCES

Angst, C. M., and Agarwal, R. 2006. "Digital Health Records and Privacy Concerns: Overcoming Key Barriers to Adoption," *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*, pp. 1331–1340.

Bansal, G., Zahedi, F. M., and Gefen, D. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," *ICIS 2008 Proceedings - Twenty Ninth International Conference on Information Systems*.

Bansal, G., Zahedi, F. M., and Gefen, D. 2015. "The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern," *European Journal of Information Systems* (24:6), pp. 624–644.

Bullek, B., Garboski, S., Mir, D. J., and Peck, E. M. 2017. "Towards Understanding Differential Privacy: When Do People Trust Randomized Response Technique?," *Conference on Human Factors in Computing Systems - Proceedings* (2017-May), pp. 3833–3837.

Cichy, P., Salge, T. O., and Kohli, R. 2017. "Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Car," *MIS Quarterly* (45:4), pp. 1863–1892.

Cummings, R., Kaptchuk, G., and Redmiles, E. M. 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. (https://doi.org/10.1145/3460120.3485252).

Dinev, T., Albano, V., Xu, H., D'Atri, A., and Hart, P. 2016. *Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective*.

Dwork, C., and Roth, A. 2013. "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science* (9:3–4), pp. 211–487.

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.

Gerlach, J. P., Buxmann, P., and Dinev, T. 2019. "'They're All the Same!' Stereotypical Thinking and Systematic Errors in Users' Privacy-Related Judgments About Online Services," *Journal of the Association for Information Systems* (20:6), pp. 787–823.

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.

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

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.

Hu, Y., Ge, L., Zhang, G., and Qin, D. 2019. "Research on Differential Privacy for Medical Health Big Data Processing," *20th International Conference on Parallel and Distributed Computing*, pp. 140–145. (https://doi.org/10.1109/PDCAT46702.2019.00036).

Huawei. 2022. "Protect Your Privacy in Our Products."

Kaissis, G. A., Makowski, M. R., Rückert, D., and Braren, R. F. 2020. "Secure, Privacy-Preserving and Federated Machine Learning in Medical Imaging," *Nature Machine Intelligence* (2:6), Springer US, pp. 305–311.

Maheswaran, D., and Chaiken, S. 1991. "Promoting Systematic Processing in Low-Motivation Settings: Effect of Incongruent Information on Processing and Judgment," *Journal of Personality and Social Psychology* (61:1), pp. 13–25.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334–359.

Nayak, C. 2020. "New Privacy-Protected Facebook Data for Independent Research on Social Media's Impact on Democracy." (https://research.facebook.com/blog/2020/02/new-privacy-protected-facebook-data-for-independent-research-on-social-medias-impact-on-democracy/).

Petty, R. E., and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," *Advances in Experimental Social Psychology* (19:C), pp. 123–205.

Schnackenberg, A. K., Tomlinson, E., and Coen, C. 2021. "The Dimensional Structure of Transparency: A Construct Validation of Transparency as Disclosure, Clarity, and Accuracy in Organizations," *Human Relations* (Vol. 74).

Schroeder, S. 2016. "With IOS 10, Apple May Have Solved a Huge Privacy Riddle." (https://mashable.com/article/apple-differential-privacy).

Tan, J., Nguyen, K., Theodorides, M., Negrón-Arroyo, H., Thompson, C., Egelman, S., and Wagne, D. 2014. "The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior," *Conference on Human Factors in Computing Systems - Proceedings*, pp. 91–100.

Xiong, A., Wang, T., Li, N., and Jha, S. 2020. "Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 392–410.

Yun, H., Lee, G., and Kim, D. J. 2014. "A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators," *35th International Conference on Information Systems "Building a Better World Through Information Systems", ICIS 2014*, pp. 1–13.