Privacy in Digital Health Applications

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Knoke Vorname: Fabian

[redacted] [redacted]

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 29.09.2022

Contents

1 Introduction

There certainly are not a lot of individuals in the world doubting that the digital transformation has not only changed the economy in past years, but also created an ever-changing environment for everyone involved. It is no longer optional for business organizations to engage in this transformational process. If companies withdraw from this on-going development, they will not be able to keep up with competing organizations (Ezeokoli et al., 2016).

What sounds like a severe threat at first glance can just as much be a tremendous opportunity for organizations. Information technology (IT) provides the foundation for companies to foster new paths of value creation, for example enhanced collaboration in value-creation networks. More potential advantages include the implementation of a multichannel approach in the sales department or an increase in the agility of an organization, defined as the ability to rapidly adapt to changes in the environment. Unlocking the groundbreaking potential of the digital transformation will be the biggest challenge for businesses, but one that leads to unprecedented opportunities if the solution is appropriate (Vial, 2021).

Hence, with potential benefits stretching into more than one dimension it is intuitive that the digital transformation is not a single-dimensional topic but more of a multi-faceted research subject. Recent literature suggests that the digital transformation not only centers around technology-related components like technology integration, stakeholder interfaces or distributed value creation. Human-related aspects, namely transformative leadership and company culture as two examples turn out to be equally crucial in ensuring the digital transformation process to be a successful one. Therefore including humans proves to be an essential component in constructing information systems (Nadkarni and Prügl, 2021; Dinev et al., 2013).

Nobody is going to argue that the inclusion of humans is absolute necessary in this context. And even though the innovative technologies accompanying the digital transformation carry potentially game-changing advantages, they bring multiple severe threats along with them (Anderson and Agarwal, 2011). Perhaps the most important threat is definitely human-centered: Privacy. Privacy describes the individual control over personal data, including when, how and to what extent this information is collected and shared. With people spending an ever-increasing time online, privacy has become an essential aspect of every day life (Boerman et al., 2021).

Some researchers have a drastic outlook, but one that certainly does have a degree of truth to it. They state, that "If this is the age of information, then privacy is the issue of our times"(Acquisti et al., 2015). Therefore it is comprehensible that privacy will remain a topic of intense debate even in the distant future. The reasoning for this is that privacy will remain a fundamental human right and a pillar of democracy, even though it faces constant attacks from all angles (Birnhack, 2008).

If companies want to maximize the potential of the digital transformation, they will definitely require personal data in an attempt to provide personalized offerings. One could go as far as calling personal data not only "the oil of the internet" which keeps the engine running, but also the "currency of the digital world" (Hoofnagle et al., 2019). Therefore it is obvious that personal data acts as a basis in increasing customer loyalty and in the end result an increase in overall revenue. One could argue that being able to collect and analyze such data is a critical resource and the backbone of sustained competitive advantages. Bear in mind though, that the organizations are in constant clash with privacy policies. Managers need to be extremely cautious not to overstep legal boundaries for example imposed by the General Data Protection Regulation (Awad and Krishnan, 2006; Kerber, 2016).

Nonetheless, the individuals will find that disclosing personal information often brings considerable benefits as well. Everyone affected will ponder providing the personal information required for the respective service. This creates a trade-off between perceived privacy risk and perceived benefit which is captured by a theory commonly regarded as privacy calculus. In this approach the decision process of personal data disclosure revolves around this trade-off. As a valuable tool in this risk-benefit analysis, this theoretical approach also includes other factors which could possibly affect the decision whether an individual provides the information required or declines to (Li et al., 2010; Dinev and Hart, 2006).

Researching factors that influence the disclosure of personal information is by no means a new topic, considering that ample of studies were already performed in different research fields connected to information systems (IS). Publications in finance (Ryu, 2018) and marketing (Beke et al., 2022) are two examples serving as proof that privacy concerns extend into a multitude of research areas.

Indeed, privacy concerns stretch into the healthcare sector too. There already exists extensive research on disclosure of healthcare information. Subjects related to this includes electronic health records (Dinev et al., 2016), healthcare wearable devices (Li et al., 2016) and even contact tracing applications in the current and highly-relevant COVID-19 pandemic (Hassandoust et al., 2021; Harborth and Pape, 2022).

The digital transformation created an ever-changing environment though. This means new innovations will launch at a rapid pace requiring new research on technology adoption including the disclosure of personal data. One topic that is gaining steam lately was the introduction of digital health applications.

Howbeit, using mobile applications to augment existing healthcare services is nothing new. Some potential opportunities were recognized multiple years ago, namely improved access to medical services, as well as another potential option in controlling and monitoring particular health conditions (Christensen and Hickie, 2010; Yuan et al., 2015).

Regarding those mobile applications the circumstances in Germany underwent drastic change recently. In late 2019 a law was passed to allow certain digital health applications to enter the service catalogue of the German statutory health insurance. Subsequently, physicians received the approval to prescribe those apps to their patients starting in late 2020 (Weitzel et al., 2021).

At first glance there are no exceptionally huge differences compared to mobile health applications available for free in a variety of app stores. Nonetheless, the change in the legal framework could ignite a shift in both technology adoption and behavior regarding personal data disclosure. It is significant to mention that there already exists privacy calculus research on disclosing personal information in mobile applications in general (Wang et al., 2016). And even though the digital health applications under the changed German circumstances have also garnered scientific attention recently (Gensorowsky et al., 2022; Dahlhausen et al., 2021; Stern et al., 2022), they have remained largely untouched in research related to the privacy calculus.

In consequence, the main goal of this thesis is evaluating potential factors which could affect the individual decision of technology adoption and more importantly disclosure of personal information in the context of digital health applications in the German healthcare system. These mobile applications bring a wide array of potential benefits for patients, improved disease management or improved health care access to name two examples (Dahlhausen et al., 2021).
On the another hand, personal health data is often perceived to have a high degree of sensitivity which puts further spotlight on the risk-related aspect in providing personal information (Vidmar and Flaherty, 1985). This inner conflict between perceived benefit and risk that has been slightly touched upon, together with the fact that there is an existing literature gap on information disclosure in digital health applications, which are included in the German health insurance, undoubtedly emphasizes the importance of this topic.
Going back to the beginning of the paragraph, the research goal mentioned there is going to be the foundation of the central research question covered in this thesis. This paper will try to provide an appropriate answer to the following research question:

Research Question: Which factors influence perceived benefits and perceived privacy risks of personal data disclosure when using digital health applications?

In order to fulfill the goal of providing a definitive answer, the following structure has been built. Section two is dedicated towards an extensive literature research on digital transformation in the healthcare sector and concerns about data protection while also providing an overview about the privacy calculus theory. With this second chapter providing the theoretical foundation, the third one is going to focus on drawing up the hypotheses which this research is based on. This part is especially crucial, because the hypotheses provide the pillars of the research model constructed in this thesis. In the following fourth chapter the data collection process will be explained. This includes insight on how the questionnaire was designed along with an detailed description about the approach used to gather the necessary data. Rounding out the fourth section is an introduction into structural equation modelling as the statistical tool of choice. The fifth chapter centers around the data analysis, divided into three parts. The first one focuses on the characteristics of the underlying data set, while the second discusses the evaluation of both the measurement model and the structural model. The third and final subsection as the pivotal part in this thesis will revolve around validating the hypotheses from the third section. The sixth section focuses on implications and strategie recommendations based on the results from the previous chapter. In addition to that, limitations of this study will be highlighted. The chapter also provides a short overview about potential directions of future research. In the seventh and final chapter a short summary will lead into the research question receiving an appropriate answer. Finally, the thesis will finish with some concluding thoughts on digital health applications and the future of the digital transformation in the healthcare sector.

2 Literature Analysis

This thesis starts by adding research context to the topic of digital heath applications. From a thematic point of view, disclosure of personal information in digital health applications can placed on an intersection of three other popular research fields. Those subjects are digital transformation in healthcare, concerns about data protection and privacy and the privacy calculus theory. This chapter will provide an extensive literature review centered around discussing these three aspects in their respective research fields.

2.1 Digital Transformation in Healthcare

In past years, the digital transformation started to change processes all throughout economy along with politics and this change did not take an exception to the healthcare sector. But how is digital transformation actually defined?

Morakanyane et al. (2017) attempt to tackle this question. They propose to define digital transformation as an "evolutionary process that leverages digital capabilites and opportunities to enable business models, operational processes, and customer experiences to create value". The authors note, that this phenomenom can be described as a disruptive, evolutionary and highly complex approach to drastically alter value creation and operational efficiency with the aim to create sustainable competitive advantages as well as improved relationships. It is worth mentioning that the terms "digital transformation" and "digitisation" and their definitions have a small tendency to be mixed up.

7 Conclusion

Digital health applications are bound to become a topic that is not only going to surge in both general interest, but also as a point of heated discussion and this development is not solely based on the disclosure of personal information. If DiGA are supposed to be established as another viable therapy option in Germany, both politics and developers need to be able to identify factors which drive potential users towards implementing DiGA into their respective therapies as well as determinants refraining them from doing that. These mobile application were approved just recently though.

Therefore, DiGA rose to prominence as a research field not long ago and existing research is not widespread yet. This thesis contributes as one of the first studies to apply the privacy calculus theory on the both highly-recent and still-ascending technological approach of DiGA in Germany. The project adds another view to this topic while managing to provide some insight into determinants that influence the individuals' decision to implement DiGA into their therapy and disclosing personal information in the respective mobile applications.

This entire thesis is build around a single research question. This research question centers around which factors do have an influence in the individuals' perceived privacy risk and perceived benefits when making a decision on disclosure of personal health information in DiGA. In order to reach a conclusion, PLS-SEM was deemed a suitable statistical approach to model the complex dependiences in this study.

By using this method, multiple factors in perceived privacy risk and perceived benefit have been identified. Prior research in the field of technology adoption in healthcare technology does point towards there being more aspects with the potential to be highly influential in the privacy calculus. The small sample size used for this research potentially limits the opportunity do discover more factors in the field of digital health applications though.

In spite of the limitations imposed by the sample size, this study still identified three determinants in the decision process whether individuals adopt DiGA or refrain from it. Health information sensitivity has to named as the major driving force in perceived privacy risk. This finding not only is in line with numerous other publications, but also the fact, that the GDPR emphasizes additional protection measures for highly sensitive data, which includes health information. On the other hand, both perceived informativeness and personal innovativeness in IT do positively affect the individuals' perceived benefit of disclosing personal information in DiGA. For perceived informativeness, it is plausible that an individual generates a higher level of utility if he receives more information. For personal innovativeness in IT, multiple other publications with similar findings underpin the assumption that IT-savvy individuals are much more inclined to see the benefits in technology adoption.

These findings are the foundation of the definitive answer for the research question. The answer is that health information sensitivity, perceived informativeness and personal innovativeness in IT are the three factors identified in this thesis which influence perceived benefits and perceived privacy risks of personal data disclosure when using digital health applications.

The remaining constructs, namely regulatory expectations, previous experience with privacy invasion as well as perceived application quality were found not to impact the privacy calculus. These findings are in disagreement with previous literature, although the very small sample size could factor into the non-existence of those relationships in this model. This can be a point of discussion for future research. Moreover, research can also experiment with additional, behavior-altering constructs to extend the initial model.

Research in the field of healthcare technology adoption and especially on digital health applications will undoubtedly remain a focal point in future research. There are two huge arguments to support this assumption.

The first argument is that digital health applications are a rather young topic with just two years having passed since German physicians were allowed to prescribe DiGA to their patients. In addition to that, Germany as the worldwide initiator became the pioneer of including digital health applications into the array of basic therapy options. These mobile application provide wide-ranging benefits as they allow personalized health services and provide additional support in dealing with the ever-growing issue of chronic diseases. This thesis does enhance the spotlight on the concerning points related to the inclusion of digital health applications into the service catalogue of the statutory health insurance though. Those weaknesses are heavily privacy-related.

The second reason is the digital transformation itself. This process keeps evolving, the degree of intelligence in enterprises increases at an unparalleled pace. The digital transformation puts aspects like value creation networks or ways of working in a state of constant change. This ever-changing environment in the digital transformation will constantly create new gaps in scientific literature for researchers to fill. Those gaps can open up in a variety of paths, for instance through new technologies. Nevertheless, seizing the near limitless potential of the digital transformation in most cases requires access to personalized data. This knowledge will lead to consumers acting cautiously with their data. In addition to that, the GPDR helps to protect personal information. Again, the huge weakness is privacy-related.

Both those arguments help come to following conclusion: Digital health applications serve as a prime example for the fact that stakeholders can expect even more innovative technologies to provide world-changing opportunities and accelerate further change in the healthcare sector. But even the most groundbreaking technologies or the most complete regulatory framework will be unable to completely erase one of the biggest issues in the today’s digitized world: Privacy-related concerns.