Managing Privacy Challenges in Digital Services and Machine Learning

TECHNISCHE UNIVERSITÄT DARMSTADT

Department of Law and Economics
at the Technical University of Darmstadt

Approved

Dissertation

submitted by

Anne Zöll, M.Sc.

for the award of the academic degree
Doctor rerum politicarum (Dr. rer. pol.)

First Assessor: Prof. Dr. Peter Buxmann
Second Assessor: Prof. Dr. Dr. Christian Reuter
Darmstadt 2024

Zöll, Anne: *Managing Privacy Challenges in Digital Services and Machine Learning*

Darmstadt, Technische Universität Darmstadt
Dissertation published on TUprints in the year 2024
Date of the viva voce: November 20, 2024

Declaration of Authorship

I hereby declare that the submitted dissertation is my own work. All quotes, whether word by word or in my own words, have been marked as such.

The dissertation has not been published anywhere else nor presented to any other examination board.

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

Anne Zöll

Darmstadt, 03.06.2024

Acknowledgements

Although research can be thrilling and fulfilling when achieving results, especially when recognized and respected by peers, the journey to these outcomes is often exhausting and lengthy. Gratefully, a multitude of remarkable individuals have supported and accompanied me along this journey, and I am sincerely grateful for their assistance.

First and foremost, I am deeply grateful to my supervisor, **Professor Peter Buxmann**, for his invaluable support. His guidance has not only provided opportunities for my professional growth, such as conference participations and publications, but also allowed me the freedom to pursue my research interests. His confidence in my abilities has been a source of motivation. I would also like to thank my co-supervisor **Professor Christian Reuter** for his expertise and support in the completion of my dissertation.

I would like to extend my heartfelt appreciation to my **colleagues** for their continuous exchange of ideas, unwavering support, critical discussions, and thought-provoking insights. Many of my colleagues have become dear friends, and I am grateful for their camaraderie.

I owe a special debt of gratitude to **Professor Ofir Turel** for his exceptional mentorship and the invaluable research experience he provided me with. His guidance has profoundly shaped my academic journey, offering insights into international research and motivating me to learn and grow. I am also thankful for his invitation to the University of Melbourne, which expanded my horizons.

I am indebted to **my husband** for his unwavering support throughout this process. He has not only been a pillar of strength but has also been my rock, providing endless encouragement, understanding, and love. His belief in me has been a guiding light, pushing me to strive for excellence even in the face of challenges.

Lastly, I am sincerely grateful to **my parents, my brother, and my grandma** for their lifelong support, understanding, and constructive questioning of my decisions. I wouldn't be the person I am today without them. I want to extend my heartfelt thanks to **my friends**, who accompanied me on this journey, bringing joy, laughter, and exiting moments into my life.

Abstract

Companies‘ data-driven digital services rely on the collection of personal data and its processing by self-learning algorithms. With the help of machine learning, companies can offer personalized services tailored to customer needs. As a result of the intensive collection of personal information by companies, customers have a sense of loss of control over their own personal information. They also have high privacy concerns about data handling. These concerns are amplified by high-profile data breaches such as the Cambridge Analytica scandal. Consequently, customers are increasingly hesitant to share their personal data with these companies, which could pose a risk to data-driven digital services. A smaller amount of data could compromise the performance of algorithms and thus reduce the quality of data-driven digital services. Therefore, the stated goal of this dissertation is to establish the complex balance between protecting customers‘ privacy and improving value creation processes. Thus, the central research question of this dissertation is how companies can mitigate the dilemma between protecting individual privacy and enhancing data-driven digital services.

This dissertation examines the issue from three different perspectives: technological, individual, and organizational. Over the past decades, privacy-enhancing *technologies* have been developed. These information and communication technologies protect individuals‘ privacy either by removing or minimizing personal information or by preventing unnecessary or unwanted processing of personal information while maintaining the functionality of information systems. Despite the advanced implementation of these privacy-enhancing technologies, they are rarely used in data-driven digital services. Therefore, this dissertation provides an overview of the reasons why these privacy-enhancing technologies are only reluctantly adopted by companies. In particular, it highlights the barriers that arise when integrating these technologies into data-driven digital services. Thus, this dissertation demonstrates that a purely technological solution is not sufficient to fully answer the research question. This is the starting point of this dissertation, which aims to find a solution to mitigate the aforementioned dilemma.

As privacy concerns are primarily customer-driven, this dissertation focuses on *individuals* as a further perspective. This perspective aims to examine how companies should design data-driven digital services to alleviate customer privacy concerns. To achieve this goal, the dissertation draws on theories from privacy research, focusing on individuals‘ control over their personal information and trust in data-driven digital services. Essentially, design principles are developed that are necessary to create data-driven digital services that allow individuals to regain control over their personal data. Furthermore, this dissertation continues to develop design principles to enhance costumers‘ trust in data-driven digital services, especially those based on machine learning.

As a third perspective, *organizations* are included, particularly examining how machine learning can be integrated into companies‘ value creation process to build data-driven digital services. The focus of this research is to identify the factors that either support or hinder the integration of machine learning into companies‘ value creation processes. Although many factors for the adoption of innovations have been examined in previous literature, a re-examination is important because the characteristics of machine learning are significantly different from other technologies. For instance, vast amounts of personal information are processed to generate personalized recommendations for individuals. The ability of machine learning to uncover hidden patterns can lead to the inadvertent disclosure of sensitive personal information, thereby intensifying privacy concerns. Additionally, this dissertation builds on previous research that highlights differences in the acceptance of innovations in different cultures and examines which different factors are important for the adoption of machine learning in data-driven digital services in different cultures. In this regard, this dissertation applies the organizational readiness concept for artificial intelligence within cultural research to gain deeper insights into this intersection.

In summary, this dissertation presents three important perspectives that aim to alleviate the dilemma between the protection of individuals‘ privacy and the use of machine learning for value creation in companies. It deals with privacy-enhancing technologies, prioritizes user-centered approaches, and the strategic design of value creation processes within companies. Particularly driven by the three perspectives, this dissertation motivates the development of a multilevel theory that aim to enable a holistic approach to alleviate the dilemma between privacy protection and value creation by bringing together technology, individuals, and organizations.

Abstract (German Version)

Schon längst basieren die datengetriebenen digitalen Dienste von Unternehmen auf der Sammlung von persönlichen Daten und deren Verarbeitung durch selbstlernende Algorithmen. Mithilfe von maschinellem Lernen können Unternehmen personalisierte Dienstleistungen anbieten, die auf die Bedürfnisse der Nutzer zugeschnitten sind. Aufgrund der intensiven Sammlung persönlicher Daten durch Unternehmen haben die Nutzer das Gefühl, die Kontrolle über ihre eigenen persönlichen Daten zu verlieren. Zusätzlich haben sie hohe Datenschutzbedenken bezüglich des Umgangs mit ihren Daten durch Unternehmen. Prominente Datenlecks wie der Cambridge-Analytica-Skandal verstärken diese Privatsphäre Bedenken. Infolgedessen sind Nutzer digitaler Dienstleistungen zunehmend zurückhaltend bei der Weitergabe ihrer persönlichen Daten, was ein Risiko für die datengetriebenen digitalen Dienste darstellen kann. Eine geringere Datenmenge könnte die Leistung der selbstlernenden Algorithmen beeinträchtigen und somit die Qualität der datengetriebenen digitalen Dienste mindern. Daher ist es das Ziel dieser Dissertation, das Dilemma zwischen dem Schutz der Privatsphäre der Nutzer und der Verbesserung der Wertschöpfungsprozesse durch selbstlernende Algorithmen herzustellen. Die zentrale Forschungsfrage dieser Dissertation lautet daher, wie Unternehmen das Dilemma zwischen dem Schutz der Privatsphäre des Einzelnen und die Verbesserung datengetriebenen digitalen Dienste entschärfen können.

Diese Dissertation betrachtet die Fragestellung aus drei verschiedenen Perspektiven: Aus der technologischen, individuellen und organisatorischen Perspektive. In den letzten Jahrzehnten haben sich *Technologien* zum Schutz der Privatsphäre entwickelt (Privacy-enhancing technologies). Diese Informations- und Kommunikationstechnologien schützen die Privatsphäre von Individuen entweder durch die Löschung oder Minimierung personenbezogener Daten oder indem unnötige oder unerwünschte Verarbeitung personenbezogener Daten verhindert wird, während gleichzeitig die Funktionalitäten der Informationssysteme erhalten bleiben. Trotz der weit fortgeschrittenen Implementierung dieser Technologien zum Schutz der Privatsphäre werden diese nur selten in datengetriebenen digitalen Diensten eingesetzt. Daher bietet diese Dissertation einen Überblick über die Gründe, warum diese Technologien zum Schutz der Privatsphäre von Unternehmen nur

zögerlich eingesetzt werden. Insbesondere werden die Barrieren aufgezeigt, die auftreten, wenn diese Technologien in datengetriebene digitale Dienste integriert werden. Somit wird durch diese Dissertation deutlich, dass eine rein technologische Lösung nicht ausreicht, um die Forschungsfrage vollständig zu beantworten. Dies ist der Ausgangspunkt meiner Dissertation, um weitere Lösungen für das zuvor angesprochene Dilemmas zu finden.

Da die Datenschutzbedenken insbesondere von den Nutzern datengetriebener digitaler Dienste ausgehen, wird in dieser Dissertation als weitere Perspektive der Fokus auf die *Individuen* gelegt. Diese Perspektive zielt darauf ab, zu untersuchen, wie Unternehmen datengetriebene digitale Dienste gestalten sollten, um die Privatsphäre Bedenken der Nutzer zu mildern. Um dieses Ziel zu erreichen, stützt sich die Dissertation auf Theorien aus der Privatsphäreforschung, wobei der Fokus auf der Kontrolle der Individuen über ihre persönlichen Informationen und dem Vertrauen in datengetriebene digitale Dienste liegen. Im Wesentlichen werden Designprinzipien entwickelt, die erforderlich sind, um datengetriebene digitale Dienste zu gestalten, die es Einzelpersonen ermöglichen, die Kontrolle über ihre persönlichen Daten zurückzugewinnen. Darüber hinaus werden in dieser Dissertation weiterhin Designprinzipien entwickelt, die das Vertrauen der Nutzer in datengetriebene digitale Dienste stärken, insbesondere in solche, die auf maschinellem Lernen basieren.

Als dritte Perspektive werden *Organisationen* einbezogen und insbesondere untersucht, wie maschinelles Lernen in die Wertschöpfungsprozesse der Unternehmen integriert werden kann, so dass datengetriebene digitale Dienste aufgebaut werden können. Im Mittelpunkt dieser Untersuchung steht die Identifizierung der Faktoren, die entweder die Integration von maschinellem Lernen in die Wertschöpfungsprozesse der Unternehmen unterstützen oder erschweren. Obwohl in vorangegangener Literatur bereits viele Faktoren für die Adoption von Innovationen untersucht wurden, ist eine erneute Betrachtung wichtig, da sich die Charakteristika von maschinellem Lernen stark von anderen Technologien unterscheiden. Beispielsweise werden große Mengen an (personenbezogenen) Daten verarbeitet, aus denen Empfehlungen für Individuen abgeleitet werden können. Die Fähigkeit des maschinellen Lernens, versteckte Muster aufzudecken, kann dazu führen, dass versehentlich sensible personenbezogene Daten offengelegt werden, was wiederum zu verstärkten Datenschutzbedenken führen kann. Zudem baut diese Dissertation auf früherer Forschungen auf, die Unterschiede bei der Akzeptanz von Innovationen in verschiedenen Kulturen aufzeigen, und untersucht, welche unterschiedlichen Faktoren in verschiedenen Kulturen für die Adoption von maschinellem Lernen für datengetriebenen digitalen Diensten wichtig sind.

Dabei wendet diese Dissertation das „Organizational Readiness Concept for Artificial Intelligence“ innerhalb der kulturellen Forschung an, um tiefere Einblicke in diese Schnittstelle zu gewinnen.

Zusammenfassend stellt diese Dissertation drei wichtige Perspektiven vor, die darauf abzielen, das Dilemma zwischen dem Schutz der Privatsphäre von Individuen und der Nutzung von maschinellem Lernen zur Wertschöpfung in Organisationen aufzulösen. Sie beschäftigt sich mit Datenschutz-Technologien, priorisiert nutzerzentrierte Ansätze und der strategischen Gestaltung von Wertschöpfungsprozessen. Diese Dissertation hebt hervor, dass die Berücksichtigung mehrerer Perspektiven erforderlich ist, um das Dilemma auflösen zu können. Dies soll weitere Forschung dazu motivieren, eine Multilevel-Theorie zu entwickeln. Ziel dieser Theorie ist es, eine umfassende Betrachtungsweise zu ermöglichen, um das Dilemma zwischen dem Schutz der Privatsphäre von Individuen und der Gestaltung von Wertschöpfungsprozessen zu finden.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

α	Cronbach's alpha
AVE	Average variance extracted
AI	Artificial Intelligence
AIS	Association for Information Systems
CEO	Chief executive officer
CFIP	Concern for information privacy
CM	Complexity
CMB	Common method bias
CR	Composite reliability
CP	Competitive pressure
CRM	Customer relationship management
CW	Collaborative work
DDBM	Data-driven business models
DOI	Diffusion of innovation
DP	Data protection; Design principles
DRs	Design requirements
DQ	Data quality
DSR	Design science research
ECIS	European Conference on Information Systems
ERP	Enterprise resource planning
FEAS	Federal enterprise architecture framework
FHE	Fully-homomorphic encryption
FR	Financial resources
FS	Firm size
G	Group
GDPR	General data protection regulation
GER	Germany
GPT	General-purpose technology
H	Hypothesis
HICSS	Hawaii International Conference on System Sciences
HIPPA	U.S. Department of Health and Human Services
HTMT	Heterotrait-monotrait ratio
ICIS	International Conference on Information Systems

IND	Industries
IUIPC	Internet Users' Information Privacy Concern
IT	Information technology
IS	Information Systems
MGA	Multigroup analysis
MICOM	Measurement invariance of composite models
ML	Machine learning
MRs	Meta-requirements
MPC	Multi-party computation
OMSs	Online messaging services
P	Problem
PACIS	Pacific Asia Conference on Information Systems
PC	Process compatibility
PETs	Privacy-enhancing technology
PF	AI-process fit
PIPC	Peer-related information privacy concern
PLS	Partial least squares
PSIPC	Peer-shared information privacy concern
P3P	Platform for privacy preferences project
RA	Relative advantage
RFID	Radio frequency identification
RQ	Research question
ROI	Return on invest
SLR	Structured literature review
SaaS	Software as a Service
SPSS	Statistical package for the social sciences
TAM	Technology acceptance model
TAI	Trustworthy Artificial Intelligence
TC	Technology competence
TM	Top management involvement
TOE	Technology-organization-environment
TR	Transparency
UPS	Upskilling
UTAT	Unified theory of acceptance and use of technology
US	United States
USP	Unique selling point
VPN	Virtual private network
WI	Wirtschaftsinformatik
YoE	Years of experience

1 Introduction

"Privacy means people knowing what they sign up for. […] Let them know precisely what you gonna do with their data."

Steve Jobs, co-founder and former CEO of Apple *(D8 Conference, 2010)*

1.1 Overarching Motivation and Problem Description

In the digital environment characterizing our modern age, companies have access to a valuable commodity — the personal information of their customers. Companies driven by the promise of innovation and economic gain leverage the power of customer data to provide personalized and data-driven digital services (Gerlach et al. 2019; Gimpel et al. 2018; Karwatzki et al. 2017; Schneider et al. 2017). Possessing an extensive reservoir of user information along with advanced machine learning (ML) algorithms has created possibilities to collect and infer knowledge about their customers (Brynjolfsson and Mitchell 2017; Dinev and Xu 2022). "Inferred knowledge" refers to insights or conclusions drawn about customers based on their data, even if that data itself does not explicitly provide that information. For example, by analyzing an individual's browsing history, purchase behavior, and social media interactions, a company might infer that they are interested in certain products or have specific preferences, even if the individual has not directly stated those preferences.

Through the use of ML algorithms, companies may anticipate customer needs and tailor content recommendations to shape their digital experiences, fundamentally altering the way customers engage with the world. With every tap, click, or interaction customers leave traces of data, contributing to a mosaic of customer preferences and personal habits available to companies. In their pursuit of understanding and catering to customer needs, companies utilize these data to deliver data-driven digital services that seamlessly integrate with their customers' lifestyles (Gimpel et al. 2018; Karwatzki et al. 2022; Rai et al. 2019; Schneider et al. 2017). While this digital symbiosis promises unparalleled convenience, it raises a crucial question: at what cost do costumers provide their data to companies?

Customers are typically confronted with an internal conflict. On the one hand, many customers desire the benefits of personalized digital services. On the other hand, there might be a lingering worry that every search query, every health app entry, every message sent adds another detail to the big picture companies build of their personal life. Thus, proliferation of data-driven digital services has raised critical concerns regarding the protection of personal information (Culnan and Williams 2009; Smith et al. 2011; Xu 2008). In addition, inferred knowledge raises privacy concerns as it involves making assumptions about individuals based on their data, which they may not have explicitly shared or consented to. As a result, growing concerns about privacy cause people to be less willing to share their personal information. Consequently, this leads to a decline in the quality of services. As a result, customers use fewer services and therefore share less data. At this point, a "vicious cycle" kicks in. As soon as customers become less inclined to provide the information due to privacy concerns, the effectiveness of digital services that rely on such data becomes limited. Thus, in turn, triggers further customers to refrain from using digial services (Krasnova et al. 2010; Malhotra et al. 2004; Taddei and Contena 2013). Thus, companies gradually lose access to data needed to offer customers personalized data-driven digital services.

Previous scandals of data breaches underscore customers' privacy concerns and intensifies their internal conflict, as evidenced by the Facebook and Cambridge Analytica case. From the company perspective, privacy intrusions could result in economic damages, such as penalties or market value loss (Acquisti et al. 2006; Muntermann and Roßnagel 2009). Companies associated with data breaches may also suffer severe reputation damage (Gerlach et al. 2019). This entails that the upkeep of a positive public image becomes challenging, which may result in the loss of loyal customers. The Facebook and Cambridge Analytica scandal triggered widespread erosion of trust among customers, subjecting companies — particularly those handling personal information — to intensified skepticism from their customer base (Acquisti et al. 2016). Considering these situations, companies have started to reconsider their data-driven digital services. The focus has shifted toward aligning data collection and usage with privacy standards and user expectations.

In this dissertation, I aim to help managing the dilemma between the protection of personal information and the value creation process of companies (e.g., extracting individual behavioral patterns using self-learning algorithms). Addressing recent calls for research for exploring ways to mitigating the dilemma (Acquisti et al. 2016; Bélanger and Crossler

2011; Gerlach et al. 2019; Pavlou 2011; Smith 2008), I ask the overarching research question (RQ): *How can companies mitigate the dilemma between the protection of individual privacy and the generation of value within data-driven digital services?*

1.2 Derivation of the Research Question from the Previous Literature

The dilemma between privacy concerns of individuals and organizations' pursuit of value generation through data-driven digital services can be approached in different ways. In this dissertation, I consider three dimensions. First, I try to understand how technological solution can mitigate the dilemma. Second, I design different privacy-enhancing technologies (PETs) and aim to understand how individuals perceive their privacy is more protected. Finally, I turn the attention to organizations with the aim of understanding the driving forces behind the implementation of data-driven digital services. Given the influence of ML in leveraging data, especially customer data, to deliver personalized digital services, my focus is on the investigation of drivers and hindrances shaping the integration of data-driven digital services within organizations, providing insights into the factors impacting the dilemma between privacy concerns and value generation. As cultures embrace technologies in multiple ways, I also explore the cultural dimensions of ML adoption.

Previous research has examined different technologies for protecting personal information in data-driven digital services. For instance, encryption algorithms such as homomorphic encryption or secure authentication protocols have all been investigated for their roles in enhancing privacy protection (Cramer et al. 2000, 2001). However, these technologies are rarely used in practice. Therefore, I want to dig deeper and aim to understand why PETs are not widely used in data-driven digital services although researchers promise that this technological solution could protect information privacy (Goldberg 2003; Xu 2007), without losing efficiency (Rossnagel et al. 2010). To explore this question further, I follow the call of research and aim to answer the following RQ (Acquisti et al. 2016):

RQ1: To what extent can privacy-enhancing technologies mitigate the dilemma of protecting the privacy of individuals while creating value for businesses in the context of data-driven digital services?

Current research has highlighted the relevance of technological measures, such as PETs, in mitigating privacy concerns and promoting value creation processes. However, these solutions face several obstacles and represent only one aspect of the overall strategy to

address this dilemma (Zöll et al. 2021). To mitigate the dilemma, researchers are also encouraged to consider individual and user-centered perspectives (Acquisti et al. 2016; Bélanger and Crossler 2011; Smith et al. 2011). Given the lack of user-centered solutions on the market to protect the privacy of individuals, in this dissertation I conceptually develop a PET that is rooted in the concept of control. This technology empowers customers with greater control over their personal information within digital services. The concept of control was first introduced in general privacy theories by Westin (1968) and Altmann (1975), and it has become a widely accepted concept in the field of privacy research (Smith et al. 2011). Control is widely recognized as an essential factor influencing privacy concerns among customers (Dinev and Hart 2006; Hong and Thong 2013; Malhotra et al. 2004; Xu et al. 2011). Empirical research has demonstrated that when individuals perceive greater control over their privacy, their level of privacy concerns decrease (Xu 2007; Xu et al. 2011). In other words, individuals are less likely to be concerned about their privacy when they feel they have more control over the disclosure of their personal information (Culnan and Armstrong 1999; Milne and Boza 1999).

I intend to examine how the element of control influences individuals' privacy decision-making regarding the sharing of personal co-owned information, specifically in the domain of online messaging services. The objective is to investigate how control can be leveraged to mitigate peer privacy concerns and generate value for digital services. This research is guided by the need to further explore how individuals can actively manage their privacy settings and concerns, gaining more control over their privacy (Acquisti et al. 2016; Pu and Grossklags 2017). To enhance control in privacy decision-making, the second RQ shifts from a technological standpoint to an individual-centric and control-focused perspective concerning the disclosure of personal information. Therefore, I aim to address the following RQ:

RQ 2.1: *How does an individual's ability to control over their personal information influence privacy concerns within digital services?*

Trust in data-driven digital services can serve as an additional concept to address the dilemma between privacy protection and value creation (Glikson and Woolley 2020; McKnight et al. 2011; Thiebes et al. 2020). Trust operates on two levels: first, individuals must believe that their personal information will be kept protected, and second, they need confidence in the data-driven digital services powered by machine learning.

Regarding the first level, it is important to note that a comprehensive dataset of personal information improves the quality of digital services. Thus, responsible handling of personal information by companies is crucial for building trust in data-driven digital services. When customers trust data-driven digital services, they are more likely to share their personal information with the provider, leading to improved recommendations for customers. Previous literature indicates that trust is a significant factor that influences individuals' self-disclosure behavior (Dinev and Hart 2006; Wakefield 2013; Xu 2009).

Concerning the second level, it should be added that data-driven digital services are based on ML. The inherent opacity of ML can create uncertainties among users (Berente et al. 2021). For example, it is often unclear how the ML system arrives at a certain result, leading to users not understanding how the result is achieved. To overcome such uncertainties, it is crucial to understand how data-driven digital services should be designed so that individuals can trust them. To gain a comprehensive understanding of how trust functions as a bridge between privacy protection and value creation, I align with the research call by Bansal et al. (2016) and endeavors to answer the RQ:

RQ 2.2: *To what extent does trust contribute to protect individuals' privacy and encouraging users to engage with data-driven digital services?*

In the following, the perspective is directed towards organizations. Since data-driven digital services are often based on ML to generate added value for the company, this dissertation investigates the barriers and drivers for the adoption of ML in companies. ML algorithms possess the potential to revolutionize operational methodologies and digital service delivery within companies. The integration of ML does not only change decision-making processes but also necessitates adjustments to existing business workflows (Coombs et al. 2020). The adoption of ML allows organizations to convert their data into valuable insights (Jöhnk et al. 2021), create innovative digital services (Davenport 2018; Ransbotham et al. 2019), and optimize organizational efficiency through data-driven decision-making (Brynjolfsson et al. 2011). Furthermore, ML has the capacity to augment human work by efficiently performing specific tasks (Bean 2018; Brynjolfsson et al. 2017). Thus, understanding the drivers and inhibitors underlying the adoption of these algorithms is essential for comprehending their impact on value creation.

Although ML is considered one of the most promising innovations in the digital age, enabling companies to maintain their competitive edge (Dremel et al. 2020; May et al. 2020; Seddon et al. 2017), there are significant challenges to successfully utilizing ML in

the value creation process. In contrast to preceding technologies, ML presents unique hurdles concerning privacy, inscrutability, algorithmic fairness, bias mitigation, and inherent inaccuracies (cp. subchapter 2.2.3). Therefore, it is essential for research to identify the drivers and inhibitors in the adoption of ML models in companies concerning value creation. In summary, there is a gap in current research regarding the investigation of ML-specific factors that can facilitate the success of data-driven digital services and promote their adoption in organizations. This dissertation thus answers the following RQ:

RQ3.1: What are the key factors driving or inhibiting the adoption of machine learning in data-driven digital services?

Looking at the intersection between culture and innovation, Leidner and Kayworth (2006) emphasize the profound influence of national culture on how groups interact with technology. Awad et al. (2018) study delves into the impact of national cultural dynamics on adoption of artificial intelligence, revealing divergent ethical preferences across cultures. The study specifically examines the effects of training an AI model in one culture and then actively applying the already trained AI model in another culture. This mismatch may lead to the development of decision support systems incongruent with the values and norms of the respective culture. Thus, conducting cultural studies in the AI context are essential to identify these nuances and differences. Failing to consider cultural intricacies during the development and adoption of AI algorithms may result in biased or inappropriate decision-making, potentially causing harm or misunderstanding. Consequently, the following RQ address the inquiry:

RQ3.2: How do cultural dimensions affect the adoption of artificial intelligence in data-driven digital services, and what role do cultural nuances play in influencing decision making when developing and deploying artificial intelligence in different cultures?

1.3 Structure of the Thesis

Figure 1 provides an overview of the dissertation. Chapter 2 presents the research context and positioning of this dissertation based on the motivation outlined in Chapter 1. Chapters 3-7 then unfold the presentation of the five papers included in this dissertation. Finally, Chapter 8 serves as a conclusion, drawing out the overarching contributions.

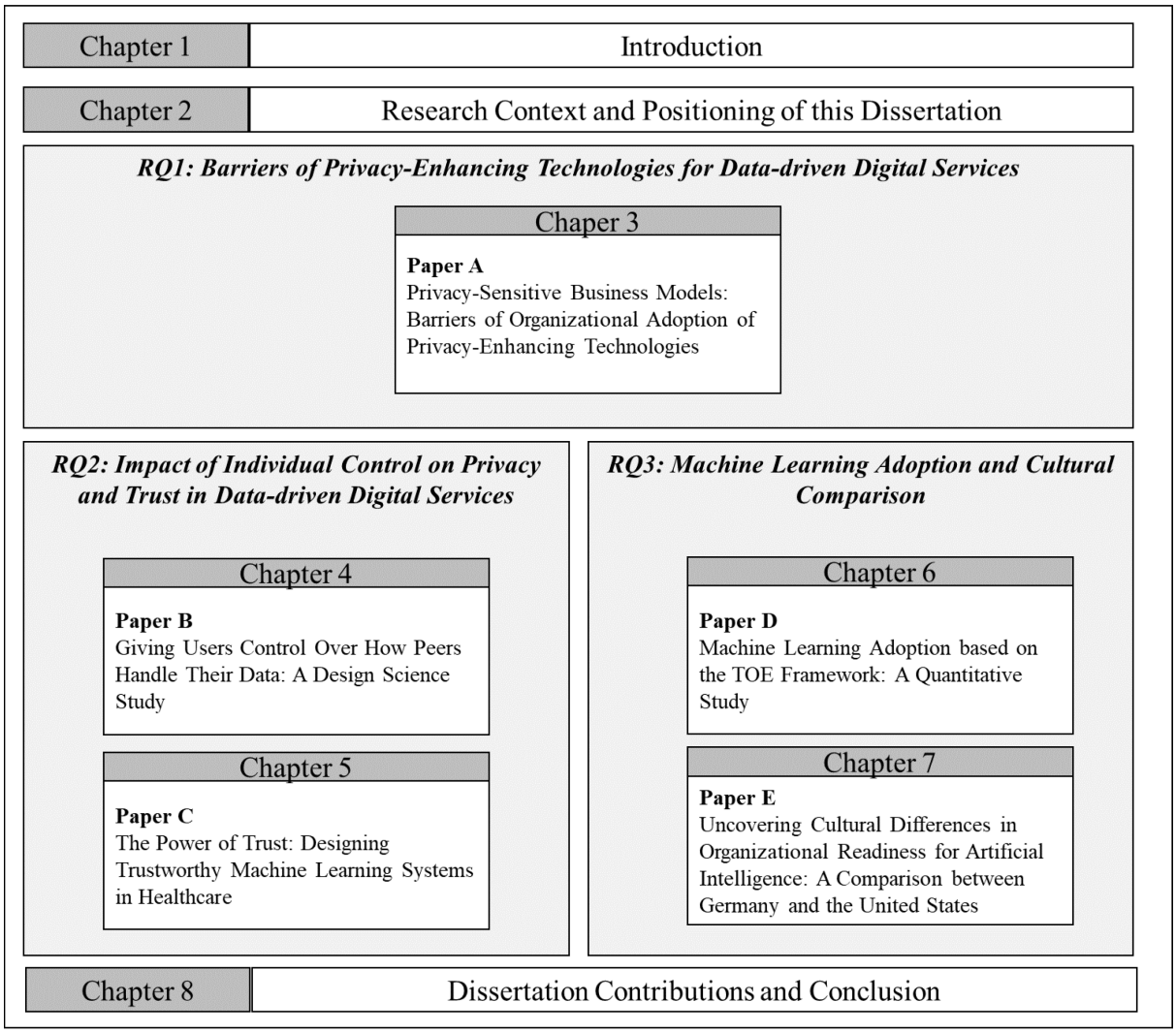

Figure 1. Overview of dissertation

Drawing on the RQs of subchapter 1.2, this dissertation considers five researcher papers[1] that have been published on peer-reviewed conferences (see Table 1).

[1] To ensure a consistent layout throughout this dissertation, slight modifications have been made to the original versions of the papers. Additionally, the papers are written in the first-person plural perspective (i.e., "we") to reflect the contributions of multiple co-authors to each publication.

Table 1. Overview of the research papers involved

RQ	Paper	Publications
Study assuming the technological perspective		
RQ1	**Paper A**	Anne Zöll, Christian M. Olt, Peter Buxmann (2021): **Privacy-Sensitive Business Models: Barriers of Organizational Adoption of Privacy-Enhancing Technologies.** European Conference on Information Systems (ECIS), Marrakesh, Marocco. VHB-Rating[2]: A.
Studies assuming the individual's perspective		
RQ2.1	**Paper B**	Anne Zöll, Amina Wagner, Melanie Reuter-Oppermann (2022): **Giving Users Control Over How Peers Handle Their Data: A Design Science Study.** International Conference on Information Systems (ICIS), Kopenhagen, Denmark. VHB-Rating: A.
RQ2.2	**Paper C**	Mariska Fecho*, Anne Zöll* (2023): **The Power of Trust: Designing Trustworthy Machine Learning Systems in Healthcare**. International Conference on Information Systems (ICIS), Hyderabad, India. VHB-Rating: A *) shared first authorship
Studies assuming the organizational's perspective		
RQ3.1	**Paper D**	Anne Zöll, Verena Eitle, Peter Buxmann (2022): **Machine Learning Adoption based on the TOE Framework: A Quantitative Study.** Pacific Asia Conference on Information Systems (PACIS), Taipei, Sydney. VHB- Rating: C.
RQ3.2	**Paper E**	Anne Zöll, Verena Eitle, Patrick Hendriks (2024): **Uncovering Cultural Differences in Organizational Readiness for AI: A Comparison between Germany and the United States.** Hawaii International Conference on System Sciences (HICSS), Waikiki, Hawaii, United States. VHB-Rating: B.

Having indicated which papers answer which RQs, I will now provide a concise summary of each paper.

Paper A aims to answer RQ1 and explores the challenges that organizations face when adopting PETs to protect individuals' privacy in their data-driven business models.

[2] In my doctoral study program, the Technical University of Darmstadt has chosen the VHB Publication Media Rating 2024 (VHB-Rating 2024) as the primary resource for evaluating the research paper quality. The VHB-Rating 2024 was released in 2024 by the German Academic Association of Business Research and is the most recent rating as of the writing of my dissertation.

Scholars argue that while PETs have the potential to create new privacy-sensitive business opportunities, they are often not fully integrated into business processes due to various barriers. First, technological barriers comprise compatibility issues or complex technology since PETs are relatively difficult to understand and use. Second, organizational barriers such as unclear economic risks or high adoption fees. Finally, environmental barriers such as customer readiness and regulatory challenges may rise. We suggest that by addressing these barriers and adopting a more comprehensive approach, organizations can create more privacy-sensitive business models that benefit both individuals and the organizations.

Paper B responds to RQ2.1 and explores the design and evaluation of a user-centered peer-privacy friendly control system in the context of online messaging services. The system is intended to enable users to have greater control over their personal information and to determine how their data is handled by other peers in online social networks. These networks often lack effective privacy controls, which can lead to privacy violations and data breaches. The paper proposes a solution to this problem by developing a peer-privacy friendly control system that is user-centered, easy to use, and can be applied to different types of online messaging services. This system offers two benefits: first, senders can manage how their personal information is processed by peers, and second, receivers can understand the sender's privacy expectations. The study follows a design science approach, where we first define the problem and its requirements, and then develop and evaluate the peer-privacy friendly control system. In particular, we developed five design principles drawing on the Malhotra et al.'s (2004) Internet Users' Information Privacy Concerns framework, which include principles such as control and awareness. The information system is developed and evaluated through a series of user experiments, which assess the user satisfaction and the effectiveness of mitigating peer privacy concerns. The results of this study reveal that the proposed privacy control system is effective in enabling users to have greater control over their personal information in online messaging services. Finally, we recommend further research to refine and extend the proposed design.

Paper C addresses RQ2.2, focusing on the widespread skepticism among end users regarding the application of ML systems. The complexity of ML output, often challenging even for experts, highlights a significant issue for end users in accepting and acting upon recommendations from ML systems. Moreover, since these systems rely on vast amounts of data, including personal information, privacy concerns among customers using data-driven digital services are also prevalent. Within the domain of healthcare, paper C

specifically examines these challenges, as they are particularly pronounced in this sector. Without understanding the system's decision-making process, individuals may rely on these systems to provide accurate and reliable recommendations that directly impact their health and well-being. The paper emphasizes the significant burden on the healthcare system, underscores the potentially transformative impact of ML in medical diagnostics, and acknowledges the existing skepticism and low acceptance rates associated with ML systems in healthcare. Highlighting an existing research gap, the paper identifies the absence of user-centered ML system designs that enhance trust in ML systems. Therefore, the study revolves around a fundamental RQ: What design principles should be applied to create trustworthy ML systems in healthcare?

Utilizing design science research, the paper integrates meta-requirements and design principles derived from the Trustworthy Artificial Intelligence (TAI) principles to guide the development of the user-centered ML system. The iterative design process involves three cycles comprising focus group discussions, evaluations of existing applications, and an online survey. The design undergoes refinement based on valuable end users' feedback throughout the iterative cycles. The effectiveness of the designed ML system is assessed through an empirical test involving 80 end users, gauging their perception of the system's trustworthiness. The outcomes reveal that end users indeed perceive the designed ML system as more trustworthy, implicitly validating the efficacy of the applied design principles and adherence to the TAI principles.

Paper D aims to answer RQ3.1. It presents a quantitative study that explores the adoption of ML in organizations using the Technology-Organization-Environment (TOE) framework. ML algorithms are utilized to sustain data-driven digital services. While ML has become a widely used technology in various industries, there is still a lack of understanding of evaluating which factors foster ML adoption in organizations. The study aims to fill this gap by examining the impact of technological, organizational, and environmental factors on ML adoption. We collected data through an online survey across different industries in Germany. The survey measures the adoption of ML algorithms, as well as various technological, organizational, and environmental factors that could influence adoption. We analyzed the data using structured equation modeling to identify the significant factors that influence ML adoption. The results reveal that the technological and organizational have a significant impact on ML adoption in organizations but environmental factor not. Technological factors, such as complexity and compatibility, are

the most significant predictors of ML adoption. Organizational factors, such as top management support and firm size, also have a significant impact on ML adoption. We did not find a significant impact of the environmental factor of data protection on ML adoption. Our results revealed that complexity is a hindrance for ML adoption due to the complex nature of ML algorithms. Hence, we suggest reducing complexity to foster a user-centered perspective by involving them at the earliest stage during the adoption process. Furthermore, this study contributes to the role of firm size on ML adoption. Our research indicates that bigger corporations tend to be more inclined to implement ML applications because they have greater access to technological, human, and financial resources. Generally, this study provides valuable insights for organizations seeking to adopt ML technologies and highlights the need for further research to refine the factors which foster ML adoption to sustain successful data-driven digital services.

Paper E responds to RQ3.2. It discusses the transformative impact of ML on data-driven digital services and emphasizes the need to understand how national culture influences the implementation of AI applications in organizations. It emphasizes how cultural disparities shape educational approaches, workforce development, and the deployment of AI in different industries. For example, Germany focuses on vocational training and skills enhancement, integrating AI into traditional sectors such as manufacturing. In contrast, the US tailors AI education toward technology and software development, applying AI across diverse industries such as transportation, supply chain management, and technology services. Noting the lack of empirical cross-cultural studies, the goal is to identify cross-cultural differences in AI adoption between Germany and the United States through a multi-group analysis. The study combines Hofstede's national cultural framework with the concept of organizational readiness for AI, examining the moderating role of cultural dimensions on factors such as AI-process fit, financial resources, upskilling, collaborative work, and data quality. The overall RQ aims to explore how national cultural differences between Germany and the United States impact the adoption of AI, shedding light on the cultural nuances that organizations should consider for successful AI implementation in diverse cultural contexts.

In addition to the publications included in this cumulative dissertation (see Table 1), I co-authored the following peer-reviewed publications during my time as a Ph.D. candidate at the Technical University of Darmstadt, Germany:

Published:

- Adrian Glauben, Anne Zöll, Bhavika Sharma, Filip Kristo (2024): **The Dialog Trap: Exploring Potentially Detrimental Effects of Dialog-Based Interfaces for Generative AI Content Creation**. Pacific Asia Conference on Information Systems (PACIS), Ho-Chi-Minh-City, Vietnam. VHB-Rating: C.
- Miriam Gräf, Anne Zöll, Nihal Wahl (2024): **Navigating Virtual Frontiers: The Willingness of Virtual Teams to Use the Metaverse**. European Conference on Information Systems (ECIS), Cyprus. VHB-Rating: A.
- Peter Buxmann, Anne Zöll (2023): **Ökonomische Effekte von ChatGPT.** Controlling & Management Review, 67 (5), S. 16-21, Wiesbaden, Springer Gabler, ISSN 2195-8262. VHB-Rating: C.
- Jonas Witte, Kevin Gao, Anne Zöll (2023): **Artificial Intelligence: The Future of Sustainable Agriculture? A Research Agenda.** Hawaii International Conference on System Sciences, Maui, Hawaii. VHB-Rating: B.
- Maren F. Mehler, Merve Turan-Akdag, Anne Zöll (2023): **Exploring the Effect of National Culture on Emerging Technologies: A Glimpse into the Future**. Pacific Asia Conference on Information Systems (PACIS), Nanchang, China. VHB-Rating: C.
- Miriam Gräf, Anne Zöll, Nihal Wahl, Sara Ellenrieder, Florentina Hager, Timo Sturm, Oliver Vetter, (2023): **Designing the Organizational Metaverse for Effective Socialization.** Pacific Asia Conference on Information Systems (PACIS), Nanchang, China. VHB-Rating: C.
- Mirheta Omerovic Smajlovic, Anne Zöll, Rami Alhasan (2023): **Building Sustainable Business Practices: Design Principles for Reusable Artificial Intelligence.** 18. Internationalen Tagung Wirtschaftsinformatik (WI), Paderborn, Germany. VHB-Rating: B.
- Verena Eitle, Anne Zöll, Peter Buxmann (2022): **Organizational Readiness Concept for AI: A Quantitative Analysis of Multi-Stage Adoption Process from the Perspective of Data Scientists**. European Conference on Information Systems (ECIS), Timișoara, Romania. VHB-Rating: A.

- Luisa Pumplun, Amina Wagner, Christian Olt, Anne Zöll, Peter Buxmann (2022): **Acting Egoistically in a Crisis: How Emotions Shape Data Donations.** Hawaii Conference on Systems Science (HICSS), Maui, Hawaii, United States. VHB-Rating: B.

Submitted for publication:

- Anne Zöll, Mingxin Zhang, Ofir Turel. **Group Closeness Effects on Co-owned Information Sharing: A Multilevel Perspective.** (under review at the *European Journal of Information Systems*). VHB-Rating: A.
- Anne Zöll, Anjuli Franz, Ofir Turel. **Dyadic Privacy Management: An Examination of Co-owned Information Disclosure in Romantic Partnerships.** (under review at the *Information Systems Journal*). VHB-Rating: A.

2 Research Context and Positioning of this Dissertation

This chapter introduces the fundamental concepts and theories underpinning the five included papers. These encompass topics such as information privacy, data-driven digital services leveraging AI and ML technologies, and how this dissertation fits into the existing literature on the dilemma between data protection and value creation.

2.1 Theoretical Foundation of Privacy Research

In this chapter, we delve into the theoretical basics of privacy, beginning with concepts such as information privacy, privacy calculus and the use of privacy concerns as a proxy of privacy (Smith et al. 2011). Additionally, various measurements of privacy concerns are presented, providing a comprehensive overview of the theoretical foundations. Then, the attention will be directed towards PETs and their role in bolstering individuals' privacy within digital serivces. Moreover, the intricate relationship between trust and privacy within digital contexts will be examined. Trust assumes an essentiell role in users' willingness to engage with digital services, particularly concerning the handling of their personal information.

2.1.1 Information Privacy

The concept of information privacy[3] is rooting back to a time preceding the development of communication technologies. Across various disciplines such as marketing, law, management, psychology, and others, diverse definitions have evolved. One central definition by Westin (1967) characterizes "information privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent digital information about them is communicated to others" (Westin 1968, p. 7). This notion of general privacy as control originates in theories by Westin (1968) and Altmann (1975). Altman's definition describes general privacy as "the selective control of access to the self" (Altmann 1975, p. 24). Privacy researchers align with this definition of privacy as "the ability of individuals to control the terms under which their personal information is

[3] In this dissertation, I will use the term "privacy" as a shorthand for information privacy.

acquired and used“ (Culnan and Bies 2003, p. 326). Margulis (1977a, 1977b) went on to consolidate and expand upon the viewpoints presented by Westin and Altman, suggesting a comprehensive definition of general privacy centered around the notion of control: “Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability“ (Margulis 1977b, p. 10). This definition centered on control has gained widespread acceptance in privacy research (Smith et al. 2011).

In the Information Systems (IS) literature, this is further supported by Bélanger and Crossler (2011), who investigated various privacy definitions. They concluded that control over personal information, particularly its secondary use, is a predominant aspect in most privacy studies. Building upon this conceptualization in IS literature, information privacy is particularly defined as the control over digitized personal information (Bélanger et al. 2002; Hong and Thong 2013; Malhotra et al. 2004; Smith et al. 2011; Stone et al. 1983; Zhang et al. 2022). As ensuring control over individuals’ personal information is indispensable in providing digital services, and considering that the control-based perspective is foundational in IS literature and utilized in measurements (Smith et al. 2011), it serves as the cornerstone for this dissertation. While this definition serves as the foundation, it should not be regarded as definitive. Achieving a comprehensive and unambiguous interpretation is challenging due to the many facets of privacy, and its meaning can vary among individuals (Acquisti et al. 2016). The challenge further arises from the inherently subjective nature of privacy, as it holds varied meanings for different individuals (Skinner et al. 2006).

2.1.2 Privacy Calculus

The privacy calculus is a cognitive process which individuals undergo to determine the dilemma between disclosing personal information and enjoying the benefits of digital services, involving careful consideration of potential risks and benefits (Dinev and Hart 2006). This concept acknowledges that individuals conduct a nuanced and rational evaluation, weighing perceived benefits such as financial incentives (Hui et al. 2007) and personalized services (Awad and Krishnan 2006) against potential drawbacks, including privacy loss, data breaches (Acquisti et al. 2006), and identity theft risks (Krasnova et al. 2010). Individuals also grapple with concerns about spam, the potential sale of personal information to other firms, and the misuse of their personal identity for financial or fraudulent activities (Dinev et al. 2015). In essence, individuals engage in a cost-benefit

analysis, evaluating the benefits of information disclosure in relation to perceived risks (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 2011).

Privacy calculus is grounded in the assumption that individuals act rationally (Culnan and Armstrong 1999; Dinev and Hart 2006). This suggests that individuals engage in thorough information processing before making privacy decisions (Dinev et al. 2015). Consequently, empirical research underscores the significance of rationality in shaping privacy decisions (Acquisti and Grossklags 2005; Jiang et al. 2013).

Recent research, however, has shown that many individuals spontaneously engage in privacy-related behaviors, often without much deliberation, placing them at the mercy of simple heuristic processing, cognitive shortcuts, or undue influence from extraneous factors (Dinev et al. 2015). In this context, scholars highlight the role of behavioral economics principles, such as bounded rationality and cognitive biases, in shaping privacy decisions (Acquisti and Grossklags 2005; Dinev et al. 2015). In exploring the duality of perspectives, namely rationality versus heuristics, the dual processing theory becomes central. This theory is particularly relevant in the privacy context. It delineates two distinct cognitive processing modes, System 1 and System 2. System 1 entails intuitive, automatic thinking, while System 2 involves more deliberate, analytical reasoning. This theoretical framework is instrumental in understanding how individuals navigate decision-making processes concerning privacy (Kahneman 2011).

In the digital age, where information is constantly gathered and exchanged online, the importance of privacy calculus has been amplified. In addition to the earlier-discussed antecedents and influencing factors in subchapter 2.1.2, the decision-making process is dynamic, influenced by further aspects such as individuals' control and awareness within the privacy domain (cp. chapter 4) (Malhotra et al. 2004; Smith et al. 2011) and trust in data-driven digital services (cp. chapters 2.1.6 and 5) (Krasnova et al. 2010). As technology continues to advance (cp. chapters 2.2, 6 and 7) (Dinev and Xu 2022), a nuanced understanding of privacy decision-making is essential for different stakeholders, including individuals and organizations, to naviagte a delicate the dilemma between safeguarding personal privacy and reaping the benefits of digital services. However, before delving into the details of these topics, I take a deeper dive into the concept of privacy concerns and their measurements.

2.1.3 (Peer) Privacy Concerns

The widespread and accessible character of digital services enable the collection, storage, processing, and utilization of personal information by various entities (e.g., organizations, platform providers, social media providers, etc.) (B. Liu et al. 2022). Consequently, this renders concerns about privacy a significant challenge in the era of information technology (IT) (Smith et al. 2011).

The majority of IS studies have traditionally framed privacy concerns as general apprehensions reflecting individuals' inherent worries of potential information privacy loss (Malhotra et al. 2004; Smith et al. 1996). However, recent observations from social scholars suggest that privacy may be more context-specific than dispositional. Therefore, it becomes crucial to distinguish between overall privacy concerns and those specific to particular situations (Margulis 2003; Solove 2006, 2018). In response to the growing recognition of the need for a context-dependent approach to privacy concerns, the prevailing conceptualization views them as situation-specific contexts. Privacy concerns are defined as "consumers' concerns about possible loss of privacy as a result of information disclosure to a specific external agent (e.g., a specific website)" (Xu et al. 2011, p. 800).

Historically, the focus of existing literature has predominantly centered on investigating privacy concerns stemming from providers of digital services. This research has particularly emphasized exploring users' perceptions of privacy issues related to secondary data usage, unauthorized access, and insufficient information on data practices by providers (Bélanger and James 2020; Smith 2008). Consequently, prior studies have primarily delved into understanding privacy threats posed by providers and addressing users' organizational privacy concerns within interactions from user to provider.

While existing research has predominantly concentrated on examining the privacy risks associated with digital service providers (Bélanger and James 2020; Smith 2008), there is an increasing acknowledgment that users' privacy can also be jeopardized by their peers who may store, share, or process their personal information without consent (Zhang et al. 2022). Consequently, a limited yet growing body of studies has emerged, delving into the phenomenon of peer privacy concerns (Chen et al. 2015; Franz and Benlian 2022; Humbert et al. 2019; Pu and Grossklags 2017). For example, Ozdemir et al. (2017) investigate the factors contributing to peer privacy concerns and their impact on information disclosure. Their findings reveal that heightened awareness of peer privacy issues lead to increased

concerns and a reduced willingness to disclose personal information. Jia and Xu (2015) have devised a measurement tool for assessing peer privacy concerns, while Zhang et al. (2022) have conceptualized and measured peer privacy concerns, distinguishing them from organizational privacy concerns. These concerns stem from users' inability to control the privacy behavior of their peers, particularly in the absence of clear mechanisms outlining the permissible use of shared personal information (Squicciarini et al. 2009).

2.1.4 Measurements of (Peer) Privacy Concerns

In this subchapter, various scales utilized to measure privacy concerns, particularly in the context of peer interactions, are presented. Table 2 provides a comprehensive overview of the scales which I used in this dissertation.

Table 2. Measurements of (peer) privacy concerns

Scales		**Dimensions**	**Sources**
Concern for Information Privacy (CFIP)		Collection, unauthorized secondary use, improper access, errors	(Smith et al. 2011)
Internet Users' Information Privacy Concern (IUIPC)		Collection, control, awareness	(Malhotra et al. 2004)
Peer-Related Information Privacy Concern (PIPC)	Self-Shared Information Privacy Concern (SSIPC)	Unauthorized secondary usage by online peers, unintentional secondary dissemination	(Zhang et al. 2022)
	Peer-Shared Information Privacy Concern (PSIPC)	Lack of control over peers' sharing	

The following presents detailed descriptions of the measurements for privacy concerns as outlined in Table 2. Concern for Information Privacy (CFIP), as conceptualized by Smith et al. (1996), is an instrument to measure privacy concerns. The dimensions of CFIP encompass *collection, unauthorized secondary use, improper access, and errors*. *Collection* refers to concerns related to the initial gathering of personal information. Individuals may worry about how and why their personal information is being collected. Concerns in this dimension focus on the worries about the extensive gathering and storage of large amounts of personally identifiable information in databases. *Unauthorized secondary use* encompasses concerns about the use of personal information for purposes other than what was originally intended or disclosed. Individuals may express

apprehension about their data being used for digital services beyond the scope of their initial agreement or the context in which the information was provided. *Improper access* involves concerns about unauthorized access to personal information. Individuals worry about the possibility of their data being accessed by individuals or entities without the proper authorization. This dimension reflects concerns about the security of personal information and the potential for privacy breaches. Finally, *errors* relate to concerns about inaccuracies or mistakes in the handling of personal information. Individuals may express concerns about the potential for errors, inaccuracies, or mistakes in the processing, storage, or transmission of their personal information. This dimension reflects worries about the quality and reliability of the information collected.

Malhotra et al.'s (2004) Internet Users' Information Privacy Concerns (IUIPC) measurement emphasize the three key dimensions of privacy concerns: *collection of personal information, lack of control over personal information, and non-awareness of secondary data usage*. *Collection* of personal information refers to the individuals worries about how and why their personal information is being collected. Concerns in this dimension revolve around the practices involved in obtaining data, such as the methods used, the purposes of data collection, and whether individuals are adequately informed about these processes. *Lack of control over personal information* encompasses concerns about the perceived inability of individuals to manage or control the use and dissemination of their personal information. Concerns regarding information privacy center on the level of control individuals have over their personal information, as evidenced by the presence of mechanisms like voice (e.g., approval or modification) or exit options (e.g., opting out). This dimension underscores worries about privacy settings, consent procedures, and the overall control individuals possess in managing their own data. *Non-awareness of secondary data usage* refers to the involvement of how much a consumer worries about being informed regarding the privacy practices of organizations. Individuals may express concerns about not being fully aware of how their data is being used by organizations after the initial collection. This dimension reflects worries about potential uses of personal information that were not explicitly communicated or consented to by the individuals.

Zhang et al. (2022) introduce the concept of Peer-Related Information Privacy Concern (PIPC), which is characterized "as the control of when, how, by whom, and to what extent information about an individual is communicated to others by online peers" (Zhang et al. 2022, p. 497). PIPC is further divided into two dimensions: Self-Shared Information

Privacy Concern (SSIPC) and Peer-Shared Information Privacy Concern (PSIPC). SSIPC is primarily driven by concerns related to *unauthorized secondary usage* of information by online peers who possess authorized access to the focal user's data, as well as *unintentional secondary dissemination* through actions such as retweeting and sharing by online connections. *PSIPC* stems from the focal user's *lack of control* over how peers share their personal information online and the accuracy of this shared information. Online peers, acting as the primary source of disclosure, may divulge information without the focal user's consent, posing challenges in assessing the commitment of peers to safeguard others' privacy and prevent the posting of sensitive personal details online.

2.1.5 Privacy-Enhancing Technologies (PETs)

PETs is an umbrella term for a broad category of tools, techniques, and measures designed to protect and enhance the privacy of individuals in digital services. These technologies aim to empower individuals, organizations, and developers to mitigate privacy risks and ensure responsible data handling (Borking and Raab 2001). A widely accepted definition of PETs is articulated as "information and communication technology measures that protect privacy by eliminating or reducing personal information or by preventing unnecessary or undesired processing of personal information; all without losing the functionality of the data system," (Borking and Raab 2001, p. 1). The literature contains numerous papers that categorize the intricate landscape of PETs (van Blarkom et al. 2003; Burkert 1997; Deswarte and Aguilar Melchor 2006; Goldberg 2003, 2008; Goldberg et al. 1997; Oppliger 2005; Seničar et al. 2003; Tavani 2000). Broadly, PETs encompass various categories, including encryption methods, anonymization tools, and other technologies explicitly crafted to minimize the collection and processing of personal information (Borking and Raab 2001). This dissertation focuses on technologies that aim to alleviate privacy concerns for individuals while enhancing value creation processes in digital services. Specifically, it addresses the area of digital services using ML algorithms, given the significant data requirements of these algorithms.

In addition to the technologies developed by computer scientists such as asymmetric encryption (Diffie and Hellman 1976) or differential privacy (Dwork 2006) applicable to various digital services, IS researchers have pioneered numerous mechanisms to safeguard the privacy of individuals while simultaneously advancing digital services. Besmer and Lipford (2010) introduced a privacy-enhancing mechanism for tagged photos, complementing this approach, Wang et al. (2011) focused on crafting an user interface

specifically tailored for managing privacy settings within third-party apps integrated into Facebook. In the automotive domain, Paefgen et al. (2012) designed a privacy enhancement for a usage-based car insurance system, eliminating the necessity for location information to mitigate privacy concerns. Additionally, Oetzel and Spiekermann (2012) conducted a step-by-step privacy impact assessment, systematically addressing users' privacy concerns. To bridge cognitive gaps in Internet-of-Things environments, Choi et al. (2020) developed personalized privacy risk scores. Finally, Gerlach et al. (2022) formulated comprehensive design requirements and principles aimed at fostering privacy-friendly personal information processing in smart energy services, with a focus on alleviating organizational privacy concerns.

Adopting these technologies not only addresses the root causes of privacy concerns, but also secures the economic benefits that organizations gain from using advanced technologies such as ML algorithms. As a result, PETs play an essential role in reducing the need for a dilemma between privacy protection and value creation. However, what remains somewhat underexplored in the IS literature on PETs is the user-centered design of such PETs (Li and Hahn 2022), taking into account privacy concepts such as control or awareness (Malhotra et al. 2004) and the concept of trust (Riedl 2022).

2.1.6 Trust within the Privacy Context

In the following, I elucidate the significance of trust in information privacy research and furnish a definition of trust grounded in the IS literature.

The concept of trust is multidimensional and contingent on the context (Mayer et al. 1995). Notably, trust has emerged as a significant factor in various privacy studies (e.g., Bansal et al. 2010; Dinev et al. 2015; Dinev and Hart 2006; Metzger 2004; Smith et al. 2011). In particular, trust is linked to information privacy, with studies proposing diverse relationships. Some consider trust as a mediator between information privacy and the willingness to disclose private information (e.g., Dinev and Hart 2006), while others see trust as an antecedent (e.g., Bélanger et al. 2002), a consequence (Bansal et al. 2010; Malhotra et al. 2004), or a moderator (Bansal and Gefen 2008). Interestingly, privacy concerns exhibit a weaker impact on online consumer behavior compared to trust (Ba and Pavlou 2002; Pavlou and Gefen 2004). While reducing privacy concerns is closely associated with trust, the exact causal direction remains debated in the literature (Zheng and Pavlou 2010). Additionally, there is an observable positive influence of a consumer's

trust in the vendor on their intent to use personalization services. Findings from Krasnova et al. (2010) suggest that online vendors can enhance their capacity to acquire and utilize customer information through trust-building activities.

Trust is defined here as the "willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. 1995). This definition, previously employed in the context of interpersonal connections (McKnight et al. 2011), underscores the idea that trust involves the trustor's vulnerability. It suggests that the trustor relies on the actions of the trustee and lacks the ability to compel the trustee to meet their expectations. Scholars contend that this trust definition extends beyond interpersonal relationships into the domain of technology (Glikson and Woolley 2020; McKnight et al. 2011) which is demonstrated in the Trustworthy Artificial Intelliegnce (TAI) principles (cp. subchapter 2.2.5) (Thiebes et al. 2020).

2.2 Data-driven Digital Services based on Artificial Intelligence

In this chapter, I discuss the integration of artificial intelligence (AI) into digital services. The focus is on how AI, particularly machine learning (ML), enhances digital services by deriving inferred knowledge from data. Concepts such as organizational readiness concept for AI adoption, principles of trustworthy AI, and the influence of national cultural dynamics on AI deployment are explored.

2.2.1 Digital Services

Organizations strategically navigate the terrain of digital transformation by harnessing the power of innovation (Baines et al. 2017; Kohli and Melville 2019). This development involves the integration of digital technologies into various facets of business operations, fostering the emergence of new and enhanced digital services (Ardolino et al. 2018). Digital innovation has created synergies within digital services as a catalyst for value creation (Yoo et al. 2012). This transformative process underscores a transition from a product-centric economy to one predominantly centered around digital services (Williams et al. 2008).

The concept of digital service design is defined across four design dimensions: Service delivery, malleability, pricing/funds, and service maturity and three design objectives:

Business, interaction, and technology (Williams et al. 2008). In scholarly works, the definition of digital services presented "as services, which are obtained and/or arranged through a digital transaction (information, software modules, or consumer goods) over Internet Protocol" (Williams et al. 2008, p. 506). Consequently, I adopt this definition characterizing 'digital services' as activities or benefits transferred from one party to another through a digital transaction (Williams et al. 2008).

Service providers develop and offer digital services to users and in particular to customers (Williams et al. 2008). These services often focus on enhancing the user experience and meeting evolving user needs, with user-centered design playing a central role (Brhel et al. 2015; Norman and Draper 1986). For instance, Adler et al. (2023) employed a user-centered approach in developing an AI system. This system facilitates user access to information regarding the functions of the United States federal court system. In consumer-facing industries, digital services foster closer relationships with consumers and present innovative value propositions (Wulf et al. 2017). Building on this, prior research has predominantly focused on the selection of appropriate methods and techniques for the design of digital services, engaging customers in specific situations (e.g., Maguire 2001; Tuunanen and Peffers 2018; Zomerdijk and Voss 2010). In addition, research has explored how digital services can be designed to enable value co-creation between service providers and users (Tuunanen et al. 2023).

Digital services rely heavily on costumer data to optimize service quality and generate revenue globally. This data, encompassing identity details like email addresses, location, demographics, and lifestyle information, is crucial for personalizing services to better meet costumer needs and interests. Additionally, it aids in understanding usage patterns and addressing costumer concerns, thereby improving overall service quality. However, the same data can be exploited for financial gains, either through targeted advertising or selling information to third parties (Karwatzki et al. 2017).

Furthermore, the integration of AI intensifies the capabilities of digital services to provide personalized experiences. AI algorithms analyze vast amounts of costumers data to derive patterns and behaviors, enabling the delivery of tailored recommendations and services. AI-driven insights enable digital service providers to refine their strategies, optimize user experiences, and ultimately deliver higher-quality services to their customers. This not only enhances user satisfaction but also contributes to service quality improvement by ensuring that offerings are more closely aligned with individual preferences and needs

(Dinev and Xu 2022). In this dissertation, I use the term "data-driven digital services" to refer to AI-driven digital services.

2.2.2 Artificial Intelligence (AI)

It is noteworthy that while numerous definitions of AI have been proposed and continue to surface, none has unequivocally asserted dominance (e.g., Berente et al. 2021; Russell 2021; Wang 2019). Nevertheless, there exists a substantial consensus regarding fundamental concepts surrounding AI, which are widely recognized for exhibiting intelligent behavior in various capacities (e.g., Russell 2021; Schuetz and Venkatesh 2020). A central concept in the field is the idea of the rational agent, which has garnered widespread acceptance among IS scholars (e.g., Berente et al. 2021; Russell 2021; Schuetz and Venkatesh 2020). Based on this concept, an intelligent agent can be defined as "anything that can be viewed as perceiving its environment through sensors and acting upon that environment through actuators" (Russell 2021, p. 54). As a result, the capabilities of intelligent agents empower AI systems to engage in cognitive tasks associated with human minds, including reasoning, self-learning, problem-solving, and decision-making (Rai et al. 2019).

The development of unprecedented computing capacity, growing volumes of data, and the availability of data through cloud computing have led to the emergence of AI technologies in organizations (Benbya et al. 2021; Collins et al. 2021). These advancements have propelled AI forward, resulting in the active integration of AI systems by organizations. In particular, AI distinguishes itself from other technologies for the following reasons: First, AI technologies are characterized by their ability to augment, complement, or potentially replace human labor in organizational settings (Murray et al. 2021). This shift redistributes roles, choices, and authority, requiring a nuanced understanding of the dynamic interaction between humans and AI systems (Benbya et al. 2021). Second, AI technologies are challenging long-held assumptions that delineate the boundaries between human capabilities and machine functions. Recent advances in AI enable machines to perform tasks traditionally reserved for humans, including conversational skills and even aspects of creativity (Benbya et al. 2024). This expansion into previously human-only domains is prompting debates about the appropriate role of machines in decision-making processes (Benbya et al. 2021). Third, the complexity of AI technologies is on the rise, resulting in unforeseen outcomes and uncertain results. While implementing AI systems brings numerous advantages to organizations, it can also yield unintended or deliberate

consequences for individuals and entities involved. Neglecting the diverse viewpoints of stakeholders during the initiation, adoption, and implementation of AI systems can culminate in system failures (Wright and Schultz 2018).

2.2.3 Machine Learning (ML)

AI encompasses a spectrum of technologies, including ML, robotics, natural language processing, and machine vision (Collins et al. 2021), providing a versatile array of application scenarios across multiple industries and within organizations. This dissertation focuses primarily on ML, which warrants closer examination in the following. ML is data-driven learning, employing algorithms to extract patterns from data and construct models (Brynjolfsson and Mitchell 2017; Jordan et al. 2015; Mitchell 1997; Russell 2021). This marks a notable shift in the programming paradigm: whereas traditional IS rely on human experts to solve specific problems and encode solutions into code, ML systems autonomously generate solutions based on data-derived patterns, potentially rendering manual programming obsolete for certain tasks (Russell 2021; Samuel 1959).

The use of ML offers many *opportunities* for businesses, particularly in how business processes can be supported by ML as follows: (i) *Process automation*: It involves the use of algorithms and statistical models to automate structured or semi-structured tasks and processes traditionally performed by humans (Benbya et al. 2021; Brynjolfsson and Mitchell 2017; Collins et al. 2021). (ii*) Cognitive insight:* It involves deriving valuable insights by examining structured (or semi-structured) data and transform their data into valuable assets (Jöhnk et al. 2021). For instance, by applying ML algorithms, healthcare providers can identify patterns and trends in patient data to improve diagnostics, predict disease risk, and personalize treatment plans (Thrall et al. 2018). (iii) *Cognitive engagement* with customers and employees: Organizations can use ML to innovate and introduce new products and services, including the delivery of targeted digital offers tailored to customers' previous online behavior (Davenport 2018; Ransbotham et al. 2019).

However, the use of ML also presents many moral and ethical challenges related to the employees, labor, and costumer in terms of privacy, inscrutability, algorithmic fairness, bias mitigation, and inherent inaccuracies (Berente et al. 2021; Fjeld et al. 2020; Floridi et al. 2018; Rai et al. 2019).

Privacy: ML enables the extraction of knowledge from data. Nevertheless, as these algorithms grow in complexity, elucidating the specific input data utilized to acquire

particular insights becomes challenging, if not impossible, even for experts in ML (Rahwan et al. 2019). Consequently, the origins of certain knowledge remain shrouded in ambiguity when employing self-learning algorithms (Berente et al. 2021). This inscrutability is vividly illustrated by well-known incidents such as the Cambridge Analytica scandal, where the correlation between psychological profiles and voting patterns remains elusive (Hu 2020). Additionally, uncertainty persists regarding the extent to which individual Facebook profiles played a role in the learning process (Gibney 2018), further emphasizing the opaqueness surrounding the use of personal information in algorithmic decision-making processes. Because of the opacity of the relationship between input data and output results in the context of self-learning algorithms, the MISQ guest editorial highlights the continuing importance of privacy (Dinev and Xu 2022).

Inscrutability: Inscrutability denotes the challenge of comprehending and interpreting the output of ML systems (Berente et al. 2021). This difficulty can be attributed to the probabilistic nature of ML, introducing uncertainty that renders the model's output and its underlying decision-making process incomprehensible for users (Adadi and Berrada 2018; Berente et al. 2021). Inscrutability encompasses various dimensions, including opacity, transparency, explainability, and interpretability (Berente et al. 2021). ML models are often reffered to "black boxes", signifying that the decision-making processes within these models pose challenges for full interpretation or understanding (Peters et al. 2020; Rudin 2019). The inherent opacity within ML systems can lead to a sense of distrust among customers, potentially leading them to discontinue their utilization of such systems. This lack of transparency distinguishes ML from previous analytical technologies, where decision-making processes were typically more interpretable.

Algorithmic Fairness and Bias: Bias and discrimination manifest in ML systems when the training data utilized to construct the model inadvertently contains inherent biases, causing the model to mirror and potentially amplify these biases in its predictions (Berente et al. 2021; Rai et al. 2019).. This issue arises when the training data lacks representation of the true diversity existing in the real world. The consequences of biased ML systems can manifest in inaccurate or unreliable predictions and recommendations, posing potential harm or negative impacts on costumers. As an illustration, ML-driven image recognition systems trained on biased datasets may erroneously identify or exclude specific racial or ethnic groups, thereby perpetuating discriminatory surveillance practices (Köchling et al. 2021).

The presence of inscrutability has the potential to worsen biases, creating challenges in identifying and rectifying issues that might affect the system's effectiveness (Lebovitz et al. 2021). When users perceive ML systems as exhibiting bias or discrimination, their trust in the system's outputs is likely to diminish. This diminished trust can lead to heightened skepticism or even outright rejection of the system (Lebovitz et al. 2021).

Inaccuracy: The term "prediction accuracy" pertains to the capacity of a ML system to generate precise outputs or forecasts, directly associated with achieving optimal performance (Lebovitz et al. 2021; Thiebes et al. 2020). Prediction inaccuracy occurs when ML systems fall short in making precise predictions for new or unseen data. This challenge can be attributed to various factors, including inadequate training data, insufficient representation of features, model overfitting, or inappropriate model selection (Rai et al. 2019). The reliability of prediction accuracy serves as a critical metric for ML systems (Baskerville et al. 2015). In cases where ML systems lack reliability or accuracy, users may question the effectiveness or utility of the ML system.

With the advent of ML, organizations are undergoing a significant transformation, largely driven by shifts in programming paradigms. Consequently, researchers have formulated a framework to effectively navigate this transition, which will be detailed in the following subsection.

2.2.4 Organizational Readiness Concept for AI

Organizations embarking on the journey of adopting AI face numerous challenges, not least in identifying appropriate use cases to harness the potential of AI. As highlighted by Hofmann et al. (2020), this initial hurdle can significantly impede progress. In addition, the adoption of AI requires significant organizational changes, requiring a readiness that goes beyond technological capabilities. To effectively manage these changes, organizations need to achieve a state of readiness at the organizational level. Jöhnk et al. (2021) outlines 18 AI readiness factors, grouped into five distinct areas, that provide a blueprint for organizations to develop their AI readiness: strategic alignment, resources, knowledge, culture, and data (Jöhnk et al. 2021). These factors, accompanied by illustrative indicators, serve as valuable guidelines that outline actionable steps across multiple domains to foster a conducive environment for successful AI integration. By comprehensively addressing these factors, organizations can not only overcome barriers, but also harness the potential of AI.

2.2.5 Trustworthy Artificial Intelligence (TAI) based on Thiebes et al. (2020)

Thiebes et al. (2020) introduced the concept of TAI by arguing that the full potential of AI will only be realized for organizations if trust can be established in its development, deployment, and use. The TAI principles are characterized by: 1) Beneficence, 2) non-maleficence, 3) autonomy, 4) justice, and 5) explicability. They formulated these principles based on established frameworks and guidelines associated with the trustworthy use of AI. These five principles are interconnected with beliefs in the trustworthiness of technology and automation. As I employ the TAI principles in paper C, I will elaborate on these principles.

Beneficence refers to the development, deployment, and use of AI that serves the well-being of humanity, prioritizing the best interests of costumers, and striving to contribute to positive outcomes while upholding fundamental human rights (Floridi et al. 2018; McKnight et al. 2002; Thiebes et al. 2020). *Non-maleficence* refers to the development, deployment, and use of AI in a way that prevents harm to individuals, with a specific focus on safeguarding people's privacy (Thiebes et al. 2020). *Autonomy* revolves around enhancing human autonomy, agency, and control, which may involve limiting the autonomy of AI systems when deemed essential. Although lacking a precise definition, the autonomy principle serves as a strategy to address integrity and reliability risks by finding a balance between human and machine-led decision-making. In organizational contexts, adherence to this principle implies the implementation of effective oversight mechanisms, such as maintaining human involvement, when integrating AI into electronic services and products. *Justice* describes the use of ML to correct past injustices, to beneficially employ ML for society, while also preventing harm and injustices (Thiebes et al. 2020). *Explicability* entails the development, deployment, and use of explainable AI aiming to generate AI models that are more interpretable while ensuring they maintain a high level of performance and accuracy (Thiebes et al. 2020).

2.2.6 National Cultural Dynamics in the Innovation of Artificial Intelligence

Investigating the influence of national culture (cross-culture[4]) is a challenge for research, mainly because culture is so differently defined in research. The first hurdle in studying (national) culture is grasping its essence amidst a many of definitions, conceptualizations,

[4] In research, the term "cross-culture" is often used synonymously with "national culture" to analyze the cultural differences between countries or regions. In this paper, however, I explicitly use the term "national culture" to emphasize that I am focusing on the unique cultural characteristics and values that are specific to nations.

and dimensions proposed by scholars (Straub et al. 2002). Among the definitions, some scholars emphasize cultural aspects such as norms, practices, and symbols, while others emphasize more general elements such as language, ideology, rituals, myths, and ceremonies (De Long and Fahey 2000). Despite various definitions of national culture, Hofstede's definition stands out as one of the most widely accepted (for a review of national cultural definitions, see Straub et al. (2002)). Hofstede defines culture as "the collective programming of the mind which distinguishes the members of one human group from another" (Hofstede 1980, p. 260). In addition, Hofstede's framework has garnered significant attention in IS literature, emerging as one of the most frequently referenced models (Mehler et al. 2023). However, it has not been immune to criticism (Myers and Tan 2002). Hofstede's framework delineated culture along dimensions of power distance, uncertainty avoidance, individualism–collectivism, and masculinity–femininity. Dimensions such as long-term orientation and indulgence were subsequently added to the framework later (see Table 3).

Table 3. Hofstede's dimensions

Dimensions	Definitions
Power Distance	Individuals within societies do not possess equal degrees of power. This dimension reflects cultural attitudes towards these inherent inequalities between individuals. Power distance refers to the extent to which less influential members of organizations within a nation expect and tolerate an unequal distribution of power.
Uncertainty Avoidance	This dimension refers to the extent to which individuals in a culture experience discomfort or anxiety in response to ambiguous or unfamiliar situations, and how they have developed beliefs and institutions to alleviate these feelings.
Individualism vs. Collectivism	This dimension explores the level of interdependence within a society. In individualist societies, individuals are expected to prioritize themselves and their immediate families. Conversely, in collectivist societies, individuals are part of "in-groups" that provide support in return for loyalty.
Masculinity vs. Femininity	This dimension measures an individual's endorsement of gender inequalities. Those who endorse masculine values prioritize work-related objectives like earnings, career advancement, competitiveness, performance, and assertiveness. Conversely, those who endorse feminine values prioritize personal goals such as fostering a friendly atmosphere, ensuring a comfortable work environment, enhancing quality of life, and nurturing warm personal relationships.
Long-term Orientation	This dimension delves into how societies balance their connection to the past with addressing present and future challenges, with varying priorities. Societies scoring low on this dimension tend to prioritize

	preserving traditional values and norms, often regarding societal change with skepticism. Conversely, cultures scoring high on this dimension take a more practical stance, promoting thrift and investing in modern education to prepare for the future.
Indulgence	This dimension assesses the degree to which individuals attempt to regulate their urges and impulses, influenced by their upbringing. "indulgence" refers to a relatively lenient control over desires, while "restraint" indicates a stronger inclination towards control.

The Hofstede framework has been used in research to investigate the influence of national culture on innovation (Mehler et al. 2023). Innovation scholars emphasize the importance of understanding cultural differences for global organizations deploying IT. National culture research aids organizations in identifying both commonalities and differences in technological needs across societies, facilitating more effective global technology strategies (Bharadwaj et al. 2013). Previous research examined national culture in the context of big data analytics (Alyoussef and Al-Rahmi 2022), intention to use mobile applications (Hoehle et al. 2015), ERP systems (Miller et al. 2006), and how national culture influence individual-level technology acceptance behaviors (Srite and Karahanna 2006).

While prior research recognizes the substantial impact of national culture on innovation adoption, studies examining the influence of national culture on AI adoption are scarce. Given that AI represents a significant departure from previous innovations (cp. subchapters 2.2.2 and 2.2.3), there exists a gap in research regarding the intersection of national culture and AI, offering an avenue for further investigation. The importance of studying national culture in the context of AI is exemplified by the research conducted by Awad et al. (2018). They developed a web-based experimental platform for moral decisions made by AI, which uncovered relevant differences in ethical preferences among various national cultures.

2.3 Positioning This Dissertation Within the Existing Literature

Previous research describe a dilemma between using personal information to enhance the customer experience, such as personalizing services, and implementing data privacy measures, which are often viewed as hindrances to profitability (Gerlach et al. 2019; Gimpel et al. 2018; Karwatzki et al. 2022; Schneider et al. 2017).

Identity-related costumer data (e.g., email addresses, location, demographics, and lifestyle details) are utilized to develop personalized products and services, aiming to better address customer needs and interests, and to improve service quality. While some individuals perceive data collection as an intrusion into their privacy, associating it with high privacy risks, others welcome data collection as it allows for better addressing of their needs. Given diverse privacy preferences, it is crucial for service providers to tailor their services accordingly. Karwatzki et al. (2022) developed a framework on a multidimensional perspective on privacy risks to help service providers understand how to configure their services to encourage consumers' willingness to share personal information. In addition, previous studies have examined why companies prioritize one need (e.g., value creation) over the other (e.g., data protection). Some argue that companies seeking competitive advantage through customer knowledge prioritize data collection over privacy protection. Conversely, those emphasizing trustworthiness prioritize privacy protection (Chan and Greenaway 2005). Greenaway et al. (2015) categorize companies based on their approach to privacy to understand their positioning along the privacy spectrum. Overall, companies struggle to satisfy both interests of exploiting the inherent value of customer data and protecting customer privacy. Gerlach et al. (2019) explore challenges organizations face when balancing value creation and customer data protection. They provide strategies on how companies can handle the tensions between organizational information needs and customer privacy concerns.

Companies prioritizing costumer data protection develop strong privacy protection measures, such as privacy protection policies (Gimpel et al. 2018). B. Liu et al. (2022) found that privacy policy negotiation with an active-recommendation feature reduces privacy concerns and increases consumers' willingness to disclose personal information, fostering a more privacy-friendly environment. Schneider et al. (2017) proposed measures to protect costumer data during second-party sharing by using synthetic segment memberships for each customer instead of true segment memberships in the lists that are shared with the provider. The key implication of this protection mechanism is that if the protected customer list is breached by an intruder at the provider, true segment membership is not disclosed. Finally, a research stream on PETs has emerged, aiming to protect costumer data without compromising digital service profitability (cp. subchapter 2.1.5).

Previous literature has focused on identifying the challenges and measures for organizations, but what remains unexplored is how a user-centered technology should be designed to mitigate the tension between value creation and data protection. Thus, there is an urgent need for the development and design of technologies that prioritize user-centricity and enhance user trust. Therefore, this dissertation aims to explore how to design effective privacy-enhancing mechanisms for data-driven digital services. Given the unique characteristics of ML, which are integrated into data-driven digital services, studies are needed to understand the factors influencing ML adoption. By understanding these factors, value creation processes can be tailored to ensure individuals privacy protection. Additionally, insights into ML adoption and its determinants, particularly in intercultural contexts, will contribute to the design of data-driven digital services. By addressing the lack of research in user-centered PETs for data-driven digital services, this dissertation lays the groundwork for more privacy-friendly and user-centric technological advancements.

3 Paper A: Privacy-Sensitive Business Models: Barriers of Organizational Adoption of Privacy-Enhancing Technologies

Title

Privacy-Sensitive Business Models: Barriers of Organizational Adoption of Privacy-Enhancing Technologies

Authors

Anne, Zöll; Olt, Christian M.; Buxmann, Peter

Publication Outlet

European Conference on Information Systems

Abstract

Organizations pursuing data-driven business models (DDBM) rely on processing user data to improve and provide their services. However, collecting personal information is often criticized by consumers due to concerns about the potential misuse of such data. While these two interests stand in an unsolved conflict - and organizations need to balance these interests - advances in the field of privacy-enhancing technologies (PETs) promise a resolution to achieve both goals simultaneously. Yet, organizations barely use PETs within their DDBMs. Based on the TOE framework, we review the literature on barriers of PET adoption to shed light on the unsolved question why organizations resist adopting PETs. We reflect the state of research on the trade-off between creating value using data and information privacy. We particularly find that multiple research streams call for the organizational adoption of PETs. Nevertheless, the main barriers we identified are unclear economic impact as well as the lack of relative advantage of PETs.

Keywords

Information Privacy, Privacy-Enhancing Technology, Data-driven Business Model

3.1 Introduction

In recent years, organizations have collected and analyzed more and more data of all different kinds –especially from customers and other online users. In particular, organizations collect and process personal information of their customers in order to improve their own businesses (Li et al. 2014). They use these collected personal data to gain new insights (Hartmann et al. 2016), to create new businesses (Zolnowski et al. 2016), and to generate value (Lusch and Nambisan 2015). Organizations are able to gain benefits from personal data because they can collect, aggregate, and analyze it on a large scale and at low cost (Malhotra et al. 2004). To produce a higher value from the data, more organizations begin building data-driven business models (DDBMs) (Engelbrecht et al. 2016; Kühne and Böhmann 2019).

However, the massive data collection does not only offer opportunities, but also poses multiple risks for organizations. In fact, data practices can also pose a challenge and become a burden for companies (Spiekermann et al. 2015). This could be the case if, for example, practices appear to be privacy intrusive and incidents occur that result in reputation loss (Acquisti et al. 2016; Feri et al. 2016; Gerlach et al. 2019). As a consequence, these intrusions can make it difficult for organizations to attract new users and retain existing ones.

Users increasingly perceive common data practices as unfair if personal information are used or shared for other purposes without their consent (Culnan and Bies 2003; Culnan and Armstrong 1999; Li 2011). For example, a study has shown that 67% of respondents think that companies benefit most from disclosing their data, while only 6% see themselves as having an advantage (Orange 2014). Moreover, research on information privacy finds that customers are concerned due to the loss of control on how organizations process their personal information (Bélanger and Crossler 2011; Zibuschka et al. 2019). Privacy concerns can influence users' decision to use a service (Bélanger and Crossler 2011; Harborth and Pape 2020). As a result of data-practices being too aggressive, existing customers could even stop using a data-driven service (Gerlach et al. 2019), yielding an economic loss for organizations. Thus, there is a need for better controls of information privacy (Bélanger and Crossler 2011; Conger et al. 2013; Smith 2008).

Regardless of privacy concerns, companies must infringe on the privacy of their users, at least to some extent, to obtain and use data. Thus, they are exposed to a field of tension in dealing with user data to remain competitive and profitable (Shapiro et al. 1998). These

approaches should be as user-friendly as possible to respect individuals' privacy. One particular characteristic of individuals' privacy is that they gain more control over which data they disclose in order to balance advantages and disadvantages of data practices for organizations as well as users (Gopal et al. 2018; Li et al. 2014).

Given this imbalance and tension, companies' current data practices should be revised in order to balance the potential of the ever-increasing volume of data for the economy and society with the potential risks (Hirsch 2014). Up to now, privacy research has urged companies from the users' perspective to refrain from collecting user data and profit from it without returning any benefit to their users (e.g., Hui et al. 2007; Smith et al. 1996). As this traditionally results in less potential data-driven value creation, changing current data collection practices seems unattractive and hence unfeasible for companies. Nevertheless, recent work on data-driven value creation on the one hand – and consumers' information privacy concerns on the other hand – shows that organizations must begin to carefully balance these competing directions (Gerlach et al. 2019).

To overcome the trade-off between users' privacy and value creation and to better balance these opposing interests, we investigate the strong potential of privacy-enhancing technologies (PETs). PETs renounce unnecessarily processing personal data to consequently protect consumers' privacy. Simultaneously, PETs offer the same functionalities of data analysis (Borking and Raab 2001, p. 1) and hence the equal opportunity to create value. This could be a game-changer if organizations would deploy PETs within their processes of data collection and transformation as their interest of pursuing DDBMs would remain to be achievable while adding the competitive advantage of handling sensitive data respectfully (Lee et al. 2011).

Even though PETs are technologically already available, organizations pursuing DDBMs rarely deploy them in practice. To give an example of a PET, the paradigm of anonymous credentials are in limited use, even though this allows for users to authenticate without revealing their identity. The question of what keeps organizations from using PETs is the main motivation for this study:

RQ: What are the barriers keeping organizations from adopting PETs?

Rowe (2014) suggests that a comprehensive literature analysis can open up the path for finding an answer to the question and also paves the way for subsequent empirical studies. In this vein, we follow the advised procedure from vom Brocke et al. (2015) and conduct a comprehensive literature review on the adoption of PETs within organizations pursuing

DDBMs. Our aim is to identify previous studies that relate to the organizational adoption of PETs. Thereon, we elaborate on future research avenues to foster the establishment of PETs in organizations pursuing DDBMs.

3.2 Conceptual Background of Related Literature

In the last years, organizations have collected more and more data from different sources (e.g., collecting customer data via smart devices or sensors). Analysis of service models become more effective when utilize customer-provided data because the storage costs for collecting data have become cheaper (Zolnowski et al. 2016). In addition, different data analysis tools have emerged which make the collection and processing of data easier available (Parmar et al. 2014). These are just a few of many factors that make the use of data interesting for new services (Kühne and Böhmann 2019). To give one example how organizations can create value through its users' personal data: Uber collects massive amounts of data from its drivers and its customers: the time the ride took place, who the passenger was, or where the car stopped (Greenaway et al. 2015). Uber analyzes the usage pattern of its services to, e.g., predict where demand will be strong. This allows drivers to adequately prepare for the next ride. In this way, Uber creates business value through data analysis of personal information (Rogers 2015).

3.2.1 Data-driven business models

Uber earns money by what is called a data-driven business model (DDBM) in research literature (Kühne and Böhmann 2019; Manyika 2011). A DDBM is creating revenue based on the collection and analysis of data (Chen et al. 2011; Hartmann et al. 2014). Following Hartmann et al. 2016, p. 2), we define DDBMs as "Business models supporting data-related ventures to capture value".

The advent of DDBMs shows that data is an essential resource, and organizations are able to obtain a significant advantage compared to competitors based on a DDBM (Bulger et al. 2014; Muhtaroğlu et al. 2013). They gain these advantages by improvement of internal processes (Davenport 2013), improvement of performance (LaValle et al. 2011; McAfee and Brynjolfsson 2012), supporting decision making (Chen et al. 2012), developing long-lasting customer relationships (Ostrom et al. 2015), and by forming new or enhanced service offerings (Goduscheit and Faullant 2018). Organizations not exploring their potential based on the available data tend to miss opportunities which are perceived by their competitors (Brownlow et al. 2015; Hunke and Wambsganß 2017). Capturing large

amounts of data goes hand in hand with collecting an increasing volume of personal information. Organizations can easily access this personal information because customers carry their mobile devices with them at all time (e.g., tablets, wearable technologies) (Kyriacou and Davis 2008; Shimojo et al. 2010). Since organizations work with their customers' personal information, which are regularly sensitive, the practice of adding value through data and hence pursuing a DDBM also poses a threat to consumers (Wu et al. 2013). One example is digital profiling: Organizations remotely collect significant amounts of personal information that can be stored unlimitedly (Adomavicius and Tuzhilin 2005). A second threat is identity theft (Greenaway and Chan 2013).

3.2.2 Privacy Concerns

Privacy has multiple definitions and it is sector specific (Schoeman 1992; Solove 2006; Warren and Brandeis 1890). In this paper, we take information privacy as a basis (Bélanger and Crossler 2011; Skinner et al. 2006). The most appropriate definition of privacy for this paper is "the ability of individuals to control the terms under which their personal information is acquired and used" (Culnan and Bies 2003, p. 326). Privacy gains an increasing importance for individuals in a time when data is constantly reproduced and shared with different parties (Acquisti et al. 2016; Tene and Polonetsky 2012). For reasons of simplicity, we use the term privacy instead of information privacy.

The rising economic interest of the collection and processing of personal data leads to growing concerns of users about the protection of their privacy (Culnan and Armstrong 1999; Pavlou 2011; Smith et al. 1996). Privacy concerns are "consumers' concerns about possible loss of privacy as a result of information disclosure to a specific external agent (e.g., a specific website)" (Xu et al. 2011, p. 800). Individuals are concerned about their personal information when they disclose it online (Dinev and Hart 2006), especially if it is indicative of their daily routines and physical location (Brush et al. 2010). Moreover, individuals are concerned about how businesses handle their personal data (Smith et al. 1996), and even about a fair relationship between data disclosure and usage on one side and control over the personal information on the other side (Malhotra et al. 2004).

There are mainly three reasons why privacy concerns emerge among users. First, privacy concerns arise from organizations' practice of constantly recording personal information and storing them without the individual's consent (Cha et al. 2019; Majeed et al. 2016). Second, privacy concerns can occur if the reason for collecting and storing personal

information is unknown or not transparent to the involved people (Guilloteau and Mauree 2012). Third, privacy concerns can arise if personal data is shared with third parties without the knowledge or consent of users (Gopal et al. 2018).

The reason why privacy concerns should be of interest to organizations is privacy concerns have a negative influence on the consumers' willingness to disclose their personal data (Culnan and Armstrong 1999; Dinev and Hart 2006; Li 2011; Malhotra et al. 2004; Xu et al. 2011). The reaction of customers can lead to difficulties for organizations to run DDBMs, as customers either refuse to provide personal data (Dinev and Hart 2006) or provide incorrect personal data (Xie et al. 2006).

Simultaneously, disclosure of personal information is at the core of the success of many DDBMs. For this reason, it is necessary for organizations to consider privacy concerns of customers as early as possible, i.e., at best in the design phase of DDBMs. In fact, organizations that consider privacy concerns well in their business-models can gain a competitive advantage (Lee et al. 2011). Organizations have an incentive to address privacy concerns due to their need to attract and keep customers for their DDBM. With this regard, Xu (2007) identified a positive correlation between PETs and the consumer's perceived control over their personal information. To date, there are few papers showing that PETs can reduce privacy concerns and data breaches. However, Brecht et al. (2012) investigated the acceptance factors of anonymized services, providing first insights into this context. They find a positive influence between privacy concerns and the intention to use an anonymized service (Brecht et al. 2011). In connection with the finding that after gaining more control over personal information, consumer trust and thus usage of the service increases (Xu 2009), usage of PETs is a worthwhile research direction to mitigate the contradicting interests (Acquisti et al. 2016).

The decentralized technology environment intensified organizational privacy problems (Culnan et al. 2008). Problems arising from the lack of protection of personal information can ultimately endanger the relationship with customers, either through customer defections (Culnan and Williams 2009; Engelbrecht et al. 2016) or through the loss of reputation (Gerlach et al. 2019). So far, organizations have difficulties balancing the two interests privacy and value creation (Gerlach et al. 2019). They favor the latter and regulatory use of personal information for pursuing DDBMs and rarely mitigate customer concerns. Thus, striving for a solution to overcome this trade-off should be a research focus.

3.2.3 Privacy-Enhancing Technologies

From a technical perspective, Privacy-Enhancing Technologies (PETs) promise to enable organizations to unite their controversial interests. We define PETs as "information and communication technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary or undesired processing of personal data; all without losing the functionality of the data system," (Borking and Raab 2001, p. 1). PETs are a collective term for technologies that aim to increase levels of privacy. Therefore, the adoption of such technologies would first and foremost reduce the reasons due to which privacy concerns regularly arise. Second, the economic advantages that organizations gain by becoming data-driven remain intact. Hence, these technologies are a steppingstone to reduce the need for a trade-off between data-driven value creation and maintaining information privacy.

Given the issues and sensitivities of processing data, there is a whole range of PETs and approaches, either used by consumers or by data collectors, to help managing concerns. Examples for consumer PETs are the Virtual Private Network (VPN) technology or the anonymized communication network TOR. We do not discuss such technologies in this paper. Instead, we focus on PETs for data controllers. In the literature, a number of papers have been published that categorize the complex PETs landscape (van Blarkom et al. 2003; Burkert 1997; Deswarte and Aguilar Melchor 2006; Goldberg 2003, 2008; Goldberg et al. 1997; Oppliger 2005; Seničar et al. 2003; Tavani 2000).

In addition, there is another example of PETs which could be used in DDBMs. Synthetic data is algorithmically generated data that reflects the properties of a real dataset. It could therefore be used as a substitute for the training of algorithms. The advantage of synthetic data is the protection of the nature of the data itself (Patki et al. 2016).

However, PETs are not widely employed by organizations in data-driven applications (Danezis et al. 2005; Harborth and Pape 2020; Rossnagel et al. 2010). The existing literature is at the beginning in terms of how privacy concerns can be addressed with PETs (Majeed et al. 2016). Only a few studies describe which sorts of privacy can be enhanced by PETs (Wang and Kobsa 2008).

In a preliminary literature search, we identified several reasons for the low adoption. Albeit, broader environment of inhibiting forces has not yet been presented in a consolidated overview in the IS literature with the aim of defining a research agenda.

3.3 Methodology

A representative and structured analysis of the literature is necessary to understand why the adoption of PETs by organizations is limited in DDBMs, although PETs are understood as promising solutions to balance the two diametrical objectives of privacy protection and value creation. In order to ensure the rigor of our analysis and to enhance replicability of our findings, we adhere to well established IS guidelines (vom Brocke et al. 2015).

The Structured Literature Review (SLR) analyzing the challenges of PETs in DDBMs is based on the steps by vom Brocke et al. (2015). We started the SLR by studying a variety of different sources (e.g., magazines, journals, conference papers) to get a better understanding of the topic.

Cooper (1988) provides a taxonomy to organize the SLR process. We designed a conceptual SRL process, emphasizes a neutral position, and the predominant target groups are scientists and practitioners. Besides, we use selected quotations for reporting (Cooper 1988). Furthermore, the overall approach structures by the following dimensions: process, source, coverage, and techniques. The process is sequential. The SLR draws from databases and publications, and the literature search aims at a comprehensive coverage. Thus, an extensive set of searching techniques is used to provide the foundation for the analysis and conceptualization: keyword search, backward search, and forward search. We conducted backward and forward searches iteratively based on the search query.

We defined the review scope according to vom Brocke et al. (2015). Hence, we performed an initial explorative literature search using Business Source Premier in order to gain a full understanding of synonyms and the existing related literature. As for the aspect of PETs, we found related terms such as e.g., “privacy preserving technology”. In the same vein, we form the organizational perspective of our SLR by adding the context of “business”, or “organizational”. Even though the study’s focus lies on organizations pursuing DDBMs, we renounced this component, since the organizational literature in the area of PETs should be examined as comprehensively as possible. The resulting search string is:

(“privacy enhancing technologies” OR “privacy enhancing technology” OR “Privacy Enhancing Technologies” OR “Privacy Enhancing Technology” OR “privacy-enhancing technologies” OR “privacy-enhancing technology” OR “Privacy-Enhancing Technologies” OR “Privacy-Enhancing Technology” OR privacy-preserving OR “privacy preserving”) AND (company OR organisation OR organization OR firm OR provider OR

merchant OR economics OR economy OR "online service" OR "online services" OR business OR enterprise OR venture OR institution)

We queried the following databases: AIS Electronic Library, informs PubsOnLine, EBSCOhost Business Source Premier, ACM Digital Library, Web Of Science, and IEEE Xplore Digital Library. We did not limit ourselves to only highly rated journals or conference proceedings to ensure a retrieval of an exhaustive result list of this research stream. The search process resulted in 3945 publications excluding the duplications.

Before beginning the screening process, we developed the following three inclusion and four exclusion criteria to ensure that we adhere to our search scope (Levy and Ellis 2006; Webster and Watson 2002). The inclusion criteria are as follows: 1) The focus is on the use and influence of PETs in the business context, 2) the publication contains the organizational perspective, or 3) potential research direction in the field of PETs is identified from a business perspective. Next, we defined the exclusion criteria: 1) The study investigates the technical design of PET, 2) the study generally relates to privacy without connection to PETs, 3) the study has been published before 2000, or 4) the paper is in progress.

By screening the titles and abstracts of all publications we could reduce the number of papers drastically down to 118. After conducting a full-text analysis, the screening process resulted in 24 publications. Finally, we executed a backward and a forward search and identified 9 further publications (Webster and Watson 2002). Thus, the resulting final set comprises 33 publications. To answer RQ, we have analyzed and coded the paper with the aim to identify different barriers of PET adoption. As foundation for the coding process serve the factors described in the TOE framework. During the process, we follow the coding guidelines of Ryan and Bernard (2000). As a result, we have conceptualized the PETs barriers for data-driven business models based on the TOE framework. An overview of the results is presented in Figure 2 and it is comprehensively explained in chapter 4. As a final step, we developed a research agenda taken the different barriers into account (Webster and Watson 2002).

3.4 Analysis and Results

During this research, it turned out that even though many studies on PETs are already available and new PETs have been developed over the last couple of years, organizations use them rarely in practice. In this chapter we discuss barriers of PET adoption, thereby

answering the RQ. Based on the identified barriers, we develop a framework for conceptualizing the barriers of PETs visualized in Figure 2.

The TOE framework describes how the adoption process of technologies is influenced by the technical, organizational and environmental contexts (DePietro et al. 1990). This framework is widely used in several contexts, in the IS community [e.g., Artificial Intelligence (Pumplun et al. 2019), ERP (Xu et al. 2017)], in interorganizational business processes (Venkatesh and Bala 2012), and notably it is also used to present inhibitors and challenges of innovations (e.g., Karunagaran et al. 2016; Stieglitz et al. 2018). Since the adoption of a technology is a challenging and multi-layered process for organizations, the TOE framework offers a great way to structure the main barriers of PETs on an organizational level (Oliveira and Fraga 2011). Therefore, we use this foundation to encapsulate the main barriers of PETs into three groups.

The **technological context** describes the features of a technology internally available and new technologies which are important for organizations (DePietro et al. 1990). It comprises the complexity, the relative advantage and the compatibility of a technology. The *complexity* of a technology is the degree to which a technology is perceived as relatively difficult to understand and use (Rogers and Shoemaker 1971, p. 154). The *relative advantage* of a technology is the degree to which a technology is perceived as being better than the previous ways of solving the problem (Rogers and Shoemaker 1971, p. 138). *Compatibility* is the degree to which a technology fits the needs of an organization and the past experiences (DePietro et al. 1990).

The **organizational context** refers to the characteristics and available resources of an organization including the profitability, the financial resources and the technology readiness (Baker 2011; DePietro et al. 1990). *Profitability* is the amount of profit which an organization yields from the adoption of the technology (Tornatzky and Klein 1982). The technology *costs* are mentioned as one component of the financial resources (Tornatzky and Klein 1982; Zhu et al. 2004). It refers to the costs incurred in the adoption of technology (e.g., investment in software and hardware, system integration, etc.). The t*echnology readiness* is the propensity to embrace a new technology for accomplishing goals (Gutierrez et al. 2015). We define technology readiness as the extent to which PETs are established in business processes of an organization (maturity of PETs) and the extent to which the organization is able to maintain the technology (e.g., update the cryptographic algorithm, infrastructure, user training).

The **environmental context** represents the external conditions under which an organization can conduct its business (DePietro et al. 1990), which includes consumer readiness and the regulatory environment. *Consumer readiness* is usually described as the volume that can potentially be generated on the market (Zhu et al. 2003). This study defines consumer readiness as a collective term for the demand of the consumers, the awareness of consumers towards PETs, and the willingness to pay for them. Consumer demand reflects the actual disposition to buy PETs. Awareness represents the consumers' interests in PETs. The willingness-to-pay shows how much the consumer is willing to pay for PETs. The combination of the three factors represents consumer readiness for PETs. Finally, *regulations* by the government have been identified as a critical factor influencing technology adoption. Regulation can either help providers implementing a trustworthy environment or establishing supportive business laws to encourage the use of PETs (Zhu et al. 2004).

				Author(s)	Ackerman 2004	Acquisti 2002	Acquisti et al. 2016	Bachlechner et al. 2018	Bélanger and Crossler 2011	Benenson et al. 2015	Boehme and Koble 2007	Boritz and No 2011	Borking 2011	Cha et al. 2019	D'Acquisto et al. 2015	Funke et al. 2017	Gan et al. 2019	Harborth and Pape 2018	Harborth and Pape 2019	Hendrik et al. 2013	Hochheiser 2002	Hoffman 2018	Kantarcioglu et al. 2010	Kantarcioglu et al. 2011	Kosta et al. 2008	Krontiris et al. 2016	Lee et al. 2017	London Economics 2010	Pelkola 2012	Reay et al. 2007	Reay et al. 2009	Rossnagel 2010	Rubinstein 2011	Schreiner et al. 2013	Thiesse et al. 2007	Turner and Dasgupta 2003	Vemou and Karyda 2015
Barriers based on TOE framework	Techno-logical barriers	Complexity issues (e.g., lack of usability)			●		●	●			●			●		●						●				●				●				●			●
		No relative advantage								●			●	●							●						●				●						
		Compatibility issue														●										●											
	Organi-zational barriers	Profitability	Unclear economic risks			●	●			●						●						●					●						●				
		Costs	High adoption fees			●								●								●		●		●						●				
		Technology readiness	Low maturity					●	●					●	●							●							●								
			Lack of maintenance															●												●	●						
	Envirn-mental barriers	Consumer readiness	Low demand			●		●										●													●	●		●	●	
			Lack of awareness				●							●				●														●	●				
			Low willingness to pay			●						●		●						●												●			●		
		Lack of regulatory enforcement																				●															
Theories and others	Theories	Technology Acceptance Model							×									×								×						×				
		Unified Theory of Acceptance and Use of T.																								×										
		Diffusion of Innovations											×																			×				
		Economic Theory of Privacy			×	×		×															×	×												
		Game Theory																					×	×												
		Signaling Theory																												×						
	Tax. & Fram.	PETs Taxonomies													×																	×				
		Privacy Research Framework									×		×							×		×													×		
	Others				×			×			×				×		×		×					×		×	×	×	×				×			×

Figure 2. Overview of SLR results: Barriers of PET adoption

Before explaining the barriers in detail, we highlight the different theories and frameworks shown in the lower part of Figure 2. In most cases, frameworks were used to investigate different PETs. For instance, the "E-Commerce Privacy Research Framework" used by Boritz and No (2011) or the "Information Technology Privacy Cycle" used by Turner and Dasgupta (2003). Just a few paper applied common IS theories, e.g., Technology Acceptance Model (Benenson et al. 2015), the Unified Theory of Acceptance and Use of Technology (UTAT) (Krontiris et al. 2016) or Diffusion of Innovation Theory (Borking 2011; Rossnagel et al. 2010).

3.4.1 Technology barriers

Complexity. PETs are perceived as complex innovations and due to the complex domain-specific building blocks, PET adoption is slow (Borking 2011; Funke et al. 2017). For instance, from a technical perspective, fully-homomorphic encryption (FHE) and differential privacy are constructed with complex cryptographic building blocks (Acquisti et al. 2016; Bachlechner et al. 2018) and multi-party computation (MPC) has hurdles in its practical implementation. The complexity of these PETs might hamper their integration into DDBMs. Another example is mentioned by Thiesse et al. (2007). They illustrate how PET mechanisms increase the complexity of protocols and tag design in RFID chips. Some PETs (e.g., access control) also require significant engineering effort to integrate them into organizations (Bachlechner et al. 2018). From the user's perspective, various studies emphasize the complexity of PETs hamper internet users from applying PETs. For instance, Benenson et al. (2015) show that users assess the additional privacy function on electronical IDs for authentication as too complex. Moreover, Rossnagel (2010) states that the correct installation and related browser configuration is often difficult for users. Implementing PETs does not only require technical knowledge but also legal expertise (Borking 2011). Organizations often do not understand which privacy laws they need to obey. Therefore, they often use the wrong set of protective measures (Borking 2011).

Low usability is another factor for low user demand (e.g., Ackerman 2004; Bachlechner et al. 2018; Lee et al. 2017; Reay et al. 2007; Vemou and Karyda 2015) and thus PET adoption (Benenson et al. 2015; Krontiris et al. 2016). Other factors have been identified as even more important, e.g., perceived usefulness of PETs for privacy protection on the intention to use PETs ($\tau = 0.420$, $p < 0.01$) (Krontiris et al. 2016). Usefulness seems to be a central construct in the perception of (Benenson et al. 2015) and should be adequately addressed (D'Acquisto et al. 2015; Bachlechner et al. 2018). Another aspect is the specific cryptographic vocabulary used in PETs (e.g., P3P). Technical and complex cryptographic terms are hard to understand for naïve users (Ackerman 2004; Hochheiser 2002; Lee et al. 2017).

No relative advantage. PETs aim to improve the privacy protection of organizations and individuals. However, the relative advantage of PETs is not perceived by users and SMEs. Measuring the relative advantage seems difficult compared to other protective measures (Borking 2011). The paper explains that the relative advantage of PETs is perceived to be zero by SMEs. Several studies emphasize that users cannot see a relative advantage in

PETs. They often do not understand how PETs make their life easier (Benenson et al. 2015). Additionally, users do not recognize security benefits from PETs and do not understand how PETs enhance their online security (Benenson et al. 2015). The fact that the relative advantage is not recognized may also be due to the fact that positive effects of PETs are not observable (Rossnagel et al. 2010). Observability is the degree to which the results of an innovation are visible to others. For instance, anonymous communications cannot be observed directly, which makes it difficult for the user to understand the relative advantage. Hendrik et al. (2013) developed a framework to evaluate the effectiveness of various PETs. In particular, it can be used to understand if PETs provide the benefits they promise. Nevertheless, there is little evidence that PETs are more effective and efficient than other privacy protection alternatives (e.g., government regulation) (Boritz and No 2011). In general, data protection agencies, business and consumer associations are optimistic regarding the effectiveness of PET deployment. They perceive PETs as instruments which mitigate the risks associated with online activity (London Economics 2010). However, the overall studies have evidence that the unclear relative advantage will be a significant barrier in PET adoption (Rossnagel et al. 2010).

Compatibility issues. In most cases, PETs are often integral parts of information systems. PET integration means to rethink and redesign the business processes and systems, implying much effort. PETs must be compatible with data-processing systems and cannot be viewed as independent. In case of DDBMs, massively collected data from multiple sources are involved. It is questionable if PETs can be integrated without interrupting the data flow processes. In particular, it has not been clarified yet how anonymisation techniques can be integrated into DDBMs. It must also be clarified to which extent the use of PETs is compatible with the massive collection from different sources and the presented data-driven business processes (D'Acquisto et al. 2015; Kosta et al. 2008).

3.4.2 Organizational barriers

Unclear economic risks. The two seemingly opposing goals of sharing and protecting personal data can both be beneficial for organizations and data subjects depending on the concrete technology or applications (Acquisti et al. 2016; Benenson et al. 2015). On the one hand, the increasing use of certain online personal information might produce an increasing revenue for organizations. Data subjects profit through personalized services or target offers. On the other hand, privacy protection can prevent the misuse of personal information (identity theft, price discrimination) (e.g., Acquisti et al. 2016; Feri et al.

2016). It also protects organizations from hazardous and potentially costly situations such as image damage (Acquisti et al. 2016).

PETs strive to dissolve the fundamental trade-off between sharing and protecting personal data, allowing organizations and data subjects to benefit from both. In particular, PETs can allow the protection of sensitive data without entirely disrupting commercially valuable flows of consumer information (Acquisti et al. 2016). Moreover, users assess the benefits of using anonymous credentials larger than the effort to use them (Benenson et al. 2015).

There are, however, hints that PETs may have a negative influence on DDBMs. For instance, privacy protection could lead to a significant loss of accuracy in analyses (D'Acquisto et al. 2015). In particular, Dwork (2006) assesses PETs as computationally intensive, and highlights that the reduction of granularity of individual information may diminish their economic value (e.g., differential privacy). Thiesse et al. (2007) assess the economic impact of PETs on RFID systems in the retail industry. Side-effects of PETs include an increased energy demand caused by complex cryptographic protocols within the RFID tag. As a consequence, the number of items that can be identified per time unit decreases, resulting in insufficient data quality. Furthermore, using PETs can lead to the situation that personal data can no longer be collected in an extensive way as organizations wish to do. For instance, applying an anonymization technique called 'cube generalization' can increase information loss. In some cases, the effectiveness of PETs themselves is put into question. Cube generalization, for example, may not be a viable way to anonymize large amounts of data because it takes much computational effort (Hoffman 2018; Jain et al. 2016). Thus, the usage of PETs could reduce the benefit of data analysis and might only ensure data protection partially (London Economics 2010). Different aggregating techniques in big data solutions can even circumvent various PETs, which makes their usage obsolete (Fang et al. 2017; Hoffman 2018). These examples show that PETs involve unquantifiable economic risks, hindering the adoption of PETs by organizations and data subjects.

High adoption fees. A monetary barrier is given by adoption fees, i.e., costs connected with the implementation of PETs. These costs can be subdivided into technology costs for deployment, data costs for preparation, costs for education and training, and opportunity costs (London Economics 2010; Rubinstein 2011). Moreover, organizations need to consider costs for the integration of PETs into their applications and business processes, e.g., the integration of PETs into the IT landscape or necessary configurations (Kosta et al.

2008). Even though the usage costs of PETs are low, the switching costs of PETs are an essential factor. The direct costs of deployment are the most immediate type of costs (London Economics 2010). Kantarcioglu et al. (2010, 2011) developed an explicit formula for the threshold of organization's investment costs into PETs which explains these costs based on consumer's level of privacy, and the level of privacy PETs promise. Kosta et al. (2008) investigate a negative effect of implementing costs on the adoption of PETs. The high costs of PETs are a limiting factor for their deployment in large organizations (Borking 2011). Investing in PETs also means costs that are un-recoverable. For instance, the configuration of PETs for the specific use cases of an organization is costly as is the training of employees to use these PETs (London Economics 2010). All in all, the adoption fees were identified as a significant entry barrier (Acquisti 2002).

Technology readiness - low maturity. Several papers indicate a low maturity of PETs in organizations many of which are still in an early stage of privacy program development. In fact, some organizations have not established a design processes for adequate privacy protection yet, a prerequisite for PET adaption (Bachlechner et al. 2018; Solove 2018). Furthermore, the focus of decision makers generally lies on key business processes, and privacy standards and PETs play a secondary role (Borking 2011). The situation is made even more difficult by a lack of clear organizational accountability for PETs (Pelkola 2012).Cha et al. (2019) show that PETs in the field of the Internet of Things are not mature enough, which indicates organizations do not put much effort into PETs. Additionally, Bélanger and Crossler (2011) suggest expanding the studies on organizational level regarding implementable and available PETs. In sum, the results present a lack of motivation to adopt PETs in a rigorous way by organizations.

Technology readiness - lack of maintenance. The work of Gan et al. (2019) analyzes the effects of PET implementation on work processes and employee perception. They raise concerns regarding the sustainability of PETs. After the initial implementation, PETs require several updates, monitoring activities, controlling mechanisms for maintenance and employees need trainings (Gan et al. 2019). However, a lack of PET feature updates, lack of monitoring, and lack of tracking was identified. It was not clear which kinds of updates are necessary for PETs. Early on, Reay et al. (2007) identified also a lack of corrective maintenance for P3P. Maintenance effort may thus be a reason why organizations have little incentive to adopt PETs (Reay et al. 2009, 2007).

3.4.3 Environmental barriers

Consumer readiness - low user demand - lack of awareness – willingness-to-pay. The adoption of PETs in organizations depends mainly on user demand (Acquisti et al. 2016). However, several papers indicate that PETs are in general used by relatively few users and demand continues to be low (e.g., Bachlechner et al. 2018; Harborth and Pape 2018; Rubinstein 2011; Turner and Dasgupta 2003). Reasons are manifold. First of all, consumers are generally unaware of the existence of PETs (Rubinstein 2011; Turner and Dasgupta 2003). The results of Acquisti and Grossklags (2005) suggest that even technologically highly educated people are not familiar with such technologies. This may be due to the fact that PETs do not receive much social recognition (Borking 2011). Another reason for low demand is that PETs often pass the organizational effort for privacy protection on to consumers (Thiesse et al. 2007), making them less attractive. They also do not have an effective signalling mechanism to indicate that privacy protection is active and works appropriately (Lee et al. 2017; Rubinstein 2011). Moreover, users are often in the position of information asymmetry (Acquisti 2002; Feigenbaum Freedman M. Sander T. Shostack A. 2002; Rossnagel et al. 2010; Rubinstein 2011). That is, it remains unclear to users how exactly their data will be used and which risks result from sharing personal data (Rubinstein 2011).

A particularly important factor for low demand is that most users are not concerned enough about their privacy (Rubinstein 2011; Turner and Dasgupta 2003). Users' awareness towards privacy risks in the use of online personal information has increased, but it is still at a relatively low level (London Economics 2010). Often, users assume negative events are less likely to happen to them than to other people. This underestimation of privacy risks leads to a limited demand for PETs and consequently a limited adoption in organizations (Acquisti et al. 2016; London Economics 2010; Rossnagel et al. 2010). The lack of privacy awareness could also explain why some of most promising PETs are little known among users (London Economics 2010).

The degree to which users are privacy-aware strongly affects their willingness to pay for PETs (Böhme and Koble 2007). Indeed, the market of privacy-conscious individuals willing to pay for PETs is small (Acquisti 2002; Spiekermann et al. 2001). Offering PETs can, however, be an alternative for both service provider and their users. Realizing an additional value of PETs is possible by implementing privacy-control functionalities in the form of a Freemium model, in which consumers can activate a premium version with

privacy protection functionalities, and estimate their prices (Schreiner et al. 2013). It might be profitable for service providers to leverage privacy protection (e.g., using PETs) as a value-added service in order to elaborate the optimal pricing points (Schreiner et al. 2013). Only few papers investigate the attitude of users towards spending money for PETs. Harborth et al. (2019) show that trust in PETs is the strongest driver for the willingness-to-pay or to donate for PETs. Nevertheless, there are many examples which illustrate users are not willing to pay for PETs. For instance, the pseudonymity service ”The Freedom Network” had to be shut down (London Economics 2010).

Lack of regulatory enforcement. In general, the studies identify the lack of regulatory enforcement of PETs as an inhibitor. Privacy laws could motivate the adoption independently of respective costs. A lack of enforcement of existing privacy rules, inadequate sanctions for infringements or a generous interpretation of existing data protection rules might depress PET deployment (London Economics 2010; Reay et al. 2007). In such a situation, businesses can freely choose between deploying and not deploying PETs. Fang et al. (2017) analyze different PETs in the big data context. They conclude that privacy-preserving methods are still immature. In particular, they identify a need for legal constraints, encouraging the development of big data privacy-preserving solutions (Fang et al. 2017; Hoffman 2018).

3.5 Discussion: A path to overcome the barriers of PET adoption

We contribute to research in mainly two directions. First, we have conceptualized the barriers of PETs and have embeded them into the TOE framework. Second, we pave future avenues in order to advance privacy-sensitive value creation by employing PETs in DDBMs. During the SLR, we found a broad consensus that PETs bear the potential to balance the interests between data-driven value creation and privacy.

To mitigate the threat of privacy concerns, studies from various disciplines (e.g., computer science, economics, information systems, etc.) call for privacy protection solutions (Acquisti et al. 2016; Bélanger and Crossler 2011; Pavlou 2011; Smith et al. 2011). Boritz and No (2011) extended this call for research by explaining that PETs need to be considered in the design of e-commerce systems. Additionally, Conger et al. (2013) support this view by stating that there is a “need for privacy-preserving technologies to be embedded in new digital artefacts” (Conger et al. 2013, p. 414). However, only few studies in IS research are PET-related with the aim to balance the diametral direction of value

creation and privacy protection. Therefore, we propose research directions to deepen the understanding of PET adoption and especially, to overcome the barriers adopting PETs.

First, reflecting our results, we have identified that most of the papers ascertain the complexity issue of PETs. On the one hand, this refers to technology itself and on the other hand it refers to the usability for employees or end users. Therefore, we propose to investigate how PETs can be integrated directly into DDBM or at the end users' devices. Moreover, future research should be referred to and critically examine the usability of PETs. We encourage researchers to answer questions such as "Does high usability influence the perceived usefulness of PETs?" (Krontiris et al. 2016) or "Does the acceptance of PETs increase if PETs have an integrated suitable function for the user's control?" (Ackerman 2004). More research is needed to give the user the possibility to understand PETs and their functionality.

Second, the most prominent research gap seems to be regarding the economic value and impact of PETs on DDBMs or how adoption of various PETs may affect DDBMs. The performance of PETs is still insufficiently investigated (Acquisti et al. 2016). DDBMs require large amounts of collected data which have to be processed. This already raises the performance question by construction. In the SLR, we identified the barrier that PETs influence the accuracy in data analytics which entails the risk of useless results (D'Acquisto et al. 2015). Simultaneously, several new advanced technologies (e.g., artificial intelligence) constantly emerge, which need huge amounts of data. In addition, degradation of data quality can lead to poor service, which in turn could lead to financial loss (D'Acquisto et al. 2015). Thus, it is a promising research direction to evaluate how PETs can be integrated into DDBM without data quality issues. Thus, future research should clarify the question "Which technologies or practices can counteract data quality degradation when PETs are introduced?"

Third, we have identified a gap in research regarding how PETs are compatible with DDBMs. It is unclear how business processes are changed by PETs. Consequently, we propose to quantify how PETs influence the effectiveness of value-creation. This would allow organizations to identify PETs as a value-adding investment. A related question is how the definition of "return on invest" (ROI) can be further developed so that privacy provided by PETs is considered. These two areas, effectiveness and investment, combined, lead to the question "To which extent do an organization's data protection practices change when the issue of data protection is included in a strategic objectives?" (Boritz and No

2011). Compatibility was the least mentioned barrier in the literature. For further exploration it would be very interesting to statistically analyse the barriers of PET adoption in order to analyse if some barriers are proven stronger than others.

Fourth, one result of the SLR is the low maturity level of PETs in organizations. Therefore, it is essential to investigate what preparatory work needs to be done to enable organizations establishing PETs in their DDBM. Thus, questions need to be answered such as "How costly will PETs ultimately be?", "Will their implementation costs, as well as the opportunity costs they may cause, be offset by gains in privacy protection?", and especially "Who will bear those costs?" (Acquisti et al. 2016). Moreover, it could be helpful for organizations to know if the use of PETs can be a unique selling point (USP). Therefore, the question raises if PETs can be a true competitive differentiator (Harborth et al. 2019). Additionally, it has not been conclusively clarified what effects the usage of PETs has on the reputation of organizations with DDBMs. Thus, a ground-breaking study for corporate practice could be the analysis of the influence of PETs on the organization's reputation (Acquisti et al. 2016; Boritz and No 2011). As already presented in the SLR, there are a few studies that relate to the topic of how the establishment of PETs changes business processes. This is particularly relevant when assessing the long-term benefits in comparison to the short-term costs of implementing PETs. Simultaneously, two question arises, "What maintenance activities are needed for PETs?" and "How can these activities be managed while using as few resources as possible?".

Fifth, closely related to the previous question, we found initial evidence that organizational usage of PETs might change price strategies based on customer-segmentation. As PETs reduce the ability to differentiate customers into price-segments, organizations face the challenge to develop new pricing strategies while implementing PETs in DDBMs. Since we found evidence that privacy-aware users are willing to pay for PETs, the RQs "Which pricing strategies can be established in DDBMs while using PETs?" and "How much can organizations charge for the usage of PETs?" arise.

Sixth, based on the SLR, we notice that PET providers receive a high degree of trust. As already mentioned, most organizations do not have the complete know-how to integrate PETs into their business processes. Service providers are engaged to incorporate PETs. In this case, PET providers have extensive access to customer data of the contracted organization during the integration of PET. Therefore, a future research direction may be to investigate the role of PET service providers and the risks associated with this

relationship (Gan et al. 2019). By investigating the role of PETs providers, researchers could generate relevant findings for practitioners.

Seventh, it could be investigated to which extent PETs could be used in regulated markets. Especially, to what extent PETs enable the usage of DDBMs in highly regulated markets. For example, how GDPR requirements can be met using PETs. For instance, anonymous data must fulfil less GDPR requirements than personal data. Furthermore, organizations operating in regulated markets (e.g., finance, insurance) would be able to expand their DDBMs and to increase data analysis by adopting PETs while simultaneously protecting their customers' personal data.

Eighth and finally, the SLR shows that only few studies explore PETs using common IS theories (e.g., Technology Acceptance Model, UTAT and Diffusion of Innovation). We have identified more research developing taxonomies and frameworks than using common IS theories. In combination with the emerging technologies, more types of PETs (e.g., differential privacy, anonymous credentials) could be investigated with those theories. Additionally, we encourage to expand the application of more theories (e.g., resource-based view (Barney 1991), resource dependency model (Pfeffer 1981; Pfeffer and Salancik 1978), which could help deepening the understanding of PETs, generalizing and empirically validating the results.

3.6 Limitations and Outlook

This study is one of the first that particularly investigates the current state of research on the barriers of PET adoption for organizations pursuing DDBMs. Conducting a holistic SLR, we identified central barriers of why PET adoption hampers in general, and in particular in DDBMs. Following this structure, our work aids researchers in this field with a comprehensive and aggregated overview of various research areas considering the balance of data-driven value creation against privacy.

Note that our findings must be interpreted with caution due to some limitations. This work is subject to several restrictions using a qualitative research method. The results of the SLR depend on the search terms (Schryen 2015). The definition of the search terms is subjective through the selection of the authors, even if this was determined beforehand in a detailed preliminary search. A different selection of keywords could have led to other results. Besides, the selection of relevant publications is a process that is subjectively influenced

by the authors. The authors strictly adhered to the defined selection and exclusion criteria to exclude potential subjective distortions as much as possible.

The search query carried out in this paper concentrates primarily on two components, PETs and organizations. However, it cannot be completely ruled out that studies have been published on the topic using different synonyms. This could lead to a situation in which some relevant papers do not find their way into the analysis. The search query did not focus on "data-driven business models". The aim of this was to identify a comprehensive spectrum of literature in the area of the possibilities of how PETs used in organizations.

Nevertheless, the SLR clearly emphasizes the rare usage of PETs, which is in line with Danezis et al. (2005) and Acquisti et al. (2016). Since privacy remains to be a critical challenge for individuals and organizations gain further capabilities in analyzing data, we call for further work preparing the path for organizations adopting PETs in DDBMs. Questions occur such as "What changes do organizations need to make to their DDBMs to adopt PETs?" and "Which new data-driven services are enabled by PETs, especially in sectors which are highly regulated?". Our work can act as a step stone for such future work since we foster transparency for the need of PETs being applied to data-driven value creation by considering that PETs can reduce privacy concerns. Possible research questions are "To which extent can PETs mitigate privacy concerns?" or "To which extent does the image of organizational change by adopting PETs and which influence does the usage have on consumers?"

Our SLR makes implicit research areas explicit. For example, we uncovered that in big data environments, there are still open questions concerning the influence of PETs on the efficiency of algorithms and regarding their compatibility with other systems. One major challenge that needs to be addressed is that the protection of individuals' privacy usually goes hand in hand with a loss of accuracy in data analysis. Thus, one aim is to enable organizations to conduct privacy-sensitive data analyses that without restricting the economic value needed for DDBMs. Thus, an interesting research direction might be to identify the threshold which provides on the one hand high data quality and on the other hand privacy protection for different types of PETs which could be used in DDBM. This analysis could quantitatively provide specific and significant practical implications for organizations to understand the extent of potential impact of PETs.

Overall, advanced and new technologies are essential for practitioners and the development of our society. PETs can be one solution to balance value creation and privacy concerns.

However, it can be concluded that IS research on PET adoption is still in its infancy. Based on this insight, Bélanger and Crossler (2011) motivate the IS community to conduct research on both the design of PETs and the subsequent evaluation of these tools by expected users. In any case, PETs represent a fruitful research field, in particularfor interdisciplinary research teams considering both the design and subsequent evaluation of PETs.

ACKNOWLEDGMENTS This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

4 Paper B: Giving Users Control Over How Peers Handle Their Data: A Design Science Study

Title

Giving Users Control Over How Peers Handle Their Data: A Design Science Study

Authors

Anne Zöll, Dr. Amina Wagner, Dr. Melanie Reuter-Oppermann

Publication Outlet

International Conference on Information Systems

Abstract

In today's interconnected world, Internet users are increasingly concerned about losing control over the data they share with peers, which indicates a need for higher levels of control and notification mechanisms. We address this need by building on design science methodology and developing a socio-technical artifact, i.e., a peer-privacy-friendly online messaging service. We draw on Malhotra et al.'s (2004) Internet Users' Information Privacy Concerns framework and refine and evaluate our artifact via focus groups, interviews, and a survey among users of online messaging services. Our artifact provides senders with the ability to control how their personal information is processed by peers and allows receivers to be made aware of the sender's privacy expectations. We contribute to the growing literature on peer privacy concerns by developing and evaluating design requirements, principles, and an instantiation that can mitigate peer privacy concerns that go beyond concerns about organizational data practices

Keywords

Peer Privacy Concerns, Information Privacy, Social Media, Online Messaging Service

4.1 Introduction

Disclosure of personal information via online messaging services (OMSs) is ubiquitous in today's interconnected world with 2 billion WhatsApp, 1.26 billion WeChat, and 557 million Snapchat users (Statista 2022). Similar to the disclosure of personal information to providers in e-commerce contexts, sharing information with peers via OMSs raises privacy concerns (Zhang et al. 2022). In fact, 86% of the Americans responding to a Pew Research survey in 2019 stated that they had only limited or no control over the private information they shared with peers (Auxiert et al. 2019). Such concerns, referred to as peer privacy concerns, describe a "general feeling of being unable to maintain functional personal boundaries in online activities as a result of online peers' behavior" (Zhang et al. 2022, p. 6). "Personal boundaries" refers to users' individual needs for privacy (Petronio 2002) and in turn their privacy expectations. To make sound privacy decisions, peers (receivers) who have received personal information from another peer (the sender) have a responsibility to comply with the original sender's privacy expectations (Petronio 2002). These peers can be friends, family members, distant acquaintances, or even strangers. As an example, imagine that Sarah has just spent an enjoyable vacation at the beach. To share this experience with her friend Mark, she sends him a photo of herself at the beach through an instant message. Since she has shared her photo with Mark, he can now make decisions that affect Sarah's privacy. For instance, Mark can forward the photo to another friend. However, Sarah might not be informed of this decision and also might not have been asked for permission to forward her photo. Thus, a sender like Sarah can lose control over when, how, and to what extent their personal information is shared by peers (Malhotra et al. 2004). This may lead to privacy theft, relational conflicts, and even terminations of friendship (e.g., Morlok 2016; Stutzman and Kramer-Duffield 2010; Thomas et al. 2010). Moreover, as a receiver, Mark might not be aware of Sarah's privacy expectations. It is apparent that this gap between a sender's privacy expectations and the actual handling of the sender's personal information by a receiver requires research attention and suggestions for potential interventions.

Peer privacy concerns have been investigated from a number of angles. For instance, Thomas et al. (2010) highlighted that conflicting privacy settings between friends can reveal information that at least one user wants to keep private. Chen et al. (2015) studied the effectiveness of decision controls to mitigate peer privacy concerns in the context of online social networks. Such et al. (2017) examined privacy conflicts in the context of group photos, and found that 74% of the participants in their study complained about the

sharing of group photos that included them without their consent. Through a vignette study, Franz and Benlian (2022) analyzed the efficacy of a peer privacy nudge and found that this nudge reduced the likelihood of peers sharing personal information about others by 62%. All of those studies point to (1) the interdependency of privacy due to the fact that individuals' privacy is affected by peers' disclosure decisions (e.g., Biczók and Chia 2013) and (2) a consequent worry about losing control over peers' data handling practices with regard to personal information. Although related research has begun to investigate peer privacy concerns, these researchers do not examine mechanisms that can mitigate peer privacy concerns and do not respond to the calls of scholars to investigate how a peer-privacy-friendly artifact might be designed (Pu and Grossklags 2017). Against this background, the goal of our study is to examine how a peer-privacy-friendly online messaging service might be designed to mitigate peer privacy concerns.

In this study, we follow the Design Science Research (DSR) methodology proposed by Vaishnavi and Kuechler (2007) and Peffers et al. (Peffers et al. 2007). As our kernel theory, we lean on Malhotra et al.'s (2004) Internet Users' Information Privacy Concerns (IUIPC) framework, which emphasizes the three key dimensions of privacy concerns: collection of personal information, lack of control over personal information, and non-awareness of secondary data usage. We offer three design outputs: design requirements, design principles, and an instantiation of the peer-privacy-friendly OMS in the form of mockups. In three design cycles, we evaluated the design requirements based on focus group discussions, refined and evaluated the design principles based on interviews, and evaluated the effectiveness of our proposal with an online survey among OSM users using mockups to instantiate a peer-privacy-friendly OMS.

Our study has several implications for research as well as messaging service providers and users. First, our main theoretical contribution is the development and evaluation of a socio-technical artifact that allows OMS users to control the personal information they share with peers and to be aware of peers' actual data handling decisions. In this regard, we respond to Pu and Grossklags' (2017) call to design mechanisms for notification when individuals share their friends' data. Second, in contrast to prior DSR studies that aim to develop IT artifacts that mitigate organizational privacy concerns (Angelopoulos et al. 2021; Wang et al. 2021), we shift the focus from user-to-provider interactions to peer-to-peer communications and provide a socio-technical artifact. In this regard, we aim to mitigate peer privacy concerns and consider the interdependency of privacy decisions between

users. Third, we validate the three key dimensions of privacy concerns proposed by Malhotra et al. (2004) and contextualize them to privacy threats stemming from peers. Overall, we complement the small but growing literature on peer privacy concerns (Chen et al. 2009; Ozdemir et al. 2017; Zhang et al. 2022) by developing technical user-centered design features for an OMS that aim to mitigate peer privacy concerns.

For messaging service providers, we offer potential instantiations illustrated by mockups that show how to overcome peer privacy concerns that can inhibit data sharing. By implementing these features, providers can promote sharing with fewer peer privacy concerns and thus distinguish from the competitors. Finally, by offering a user-centered design that has been evaluated by frequent OMS users, we develop a socio-technical artifact that allows users to communicate their privacy expectations in a standardized form and leverage awareness of receivers' data practices. Specifically, we present features for a greater granularity of control for information senders as well as awareness of how the receiver handles their personal information. In addition, these features provide the receivers a higher degree of awareness of the senders' privacy expectations. In this sense, our artifact presents senders and receivers of information with the opportunity to regulate and apply rules for sound privacy decisions that align with senders' or even co-owners' privacy expectations.

In the next section, we identify the problems to be addressed, describe the scope of our study, and present important insights from previous work on privacy concerns and their implications for our approach. Following that, we describe the DSR methodology along with our three iterative cycles. Then we present the outcome of these cycles: five design principles and their instantiation in the form of mockups. Finally, we discuss the practical and theoretical contributions of our study, point out its limitations, and suggest future research directions.

4.2 Problem Identification and Motivation

4.2.1 Research Gap: A Review of the Literature

Extant research has predominantly studied privacy concerns stemming from information system providers (Bélanger and James 2020; Smith et al. 2011) and has mainly investigated the extent to which users perceive privacy concerns related to secondary data use, unwanted access, and lack of information about data practices from providers (Smith et al. 2011). Since this privacy research predominantly deals with user-to-provider

interactions, privacy threats caused by the provider, privacy-enhancing IT artifacts, and mitigation of users' organizational privacy concerns have been the focus of research attention. In this context, for example, Oetzel and Spiekermann (2012) systematically considered the privacy concerns of users in a step-by-step privacy impact assessment. Choi et al. (2020) designed personal privacy and security risk scores to minimize users' cognitive gaps in Internet-of-Things settings. Besmer et al. (2010) designed a privacy-enhancing mechanism for tagged photos. Wang et al. (2011) designed a user interface for privacy settings for third-party apps embedded in Facebook. Using a DSR approach, Paefgen et al. (2012) developed a privacy enhancement in a usage-based car insurance system design that obviates the need for location information in order to reduce privacy concerns. Gerlach et al. (2022) developed design requirements and design principles for privacy-friendly personal information processing in smart energy services to reduce organizational privacy concerns.

However, it is not only providers who put users' privacy at risk, but also peers that can store, re-share, or further process personal information (Zhang et al. 2022). Recently, a small number of studies have begun to investigate the phenomenon of peer privacy concerns (e.g., Chen et al. 2015; Franz and Benlian 2022; Humbert et al. 2019). For instance, by applying a choice-based conjoint analysis, Pu and Grossklags (2017) determined the value that users place on the privacy of their friends in the context of information disclosure on online social networks. They found that users also account for the privacy threats that occur to their friends. In addition, users tend to value their friends' data less if they believe this data is useful for the functionality of an application (Pu and Grossklags 2017). Using a quantitative survey method, Ozdemir et al. (2017) studied the antecedents and outcomes of peer privacy concerns. They confirmed that increased awareness of peer privacy leads to greater privacy concerns among peers, and they found that greater peer privacy concerns have a negative impact on the disclosure of co-owned information. Thus, they demonstrated that when individuals perceive greater peer privacy concerns, they are less willing to disclose personal information. Jia and Xu (2015) elaborated on the notion of peer privacy concerns and developed and evaluated a measuring instrument for peer privacy concerns, which resulted in a second-order factor model of peer privacy concerns. Similarly, Zhang et al. (2022) conceptualized peer privacy concerns, developed a measurement, and distinguished such concerns from organizational privacy concerns: Peer privacy concerns arise from a user's lack of control over peers' privacy behavior (Zhang et al. 2022). Specifically, such concerns arise in the absence of

functions and mechanisms that determine what peers are allowed to do with personal information that was originally shared by other users (Squicciarini et al. 2009).

Although peer privacy concerns have begun to receive research attention, socio-technical artifacts that can mitigate peer privacy concerns are missing in the literature. This is problematic for two main reasons. On the one hand, peer privacy concerns are surfacing among OMS users. In several forums such as reddit.com, for example, users complain about their photos being (re-)shared without their consent (Anonymous Reddit User 2020). One indication that these are not isolated cases is that providers have begun to set up help pages that address peer privacy concerns. For instance, Apple offers a help page for such incidents (Apple 2022), and Meta provides help pages with recommendations regarding how to deal with intellectual property coming from others (Meta 2022).

On the other hand, peer privacy decisions are less regulated than organizational data handling processes, which require technology-mediated rule settings. In contrast to the legislative rules that drive organizational privacy practices, peer-related privacy rules are more implicit in nature and dependent only on people's intuition (Tene and Polonetsky 2013). For instance, while laws such as the General Data Protection Regulation (GDPR; European Union (2022)) or the Health Insurance Portability and Accountability Act (HIPPA; U.S. Department of Health and Human Services (2022)) regulate that companies are not allowed to share personal information (e.g., photos of individuals) with third parties without their consent, it is not generally known whether peers are allowed to forward a photo that had intentionally been shared by the original sender. Thus, peers might reveal information that at least one user intended to be private (Thomas et al. 2010). Furthermore, compared to the e-commerce context in which users provide information such as name, address, and so forth, users often share sensitive information with peers (Zhang et al. 2022). This sensitive information might be private photos, information about the user's emotional states, or other private messages that are not publicly available. As a result, there is a need for novel solutions that protect the privacy of OMS users without hindering the benefits that arise from sharing personal information online. In summary, even though prior research hints at the existence of peer privacy concerns and there have been many complaints, there is a lack of research on specific design features for a peer-privacy-friendly OMS.

4.2.2 Research Scope: Online Messaging Services

The focus of our study is the design of a socio-technical artifact in the context of peer-to-peer communication in general and for OMSs in particular. In Figure 3, we illustrate how personal information (e.g., photos, texts, or voice messages) is transmitted between a sender and up to n receivers. To be more specific, an initial sender shares personal information with another person, whom we call the first receiver. The first receiver is then in turn able to make decisions about the received personal information, such as storing it on their smartphone, forwarding it, or editing it. For instance, the receiver could decide to share the sender's personal information with n receivers. Notably, the first receiver can also be a group of people, e.g., in a group chat. Given the context of common sender–receiver communications on an OMS, we identify the following problems: P1. Senders cannot trace how receivers actually process their shared messages. P2. Senders are limited to one simple option—to either share or not share personal information—without fine-grained privacy settings for each message or data type. P3. Receivers face the challenge of correctly anticipating senders' privacy expectations and in turn making sound privacy decisions. P4. Users can share personal information that is co-owned without the co-owners' awareness. Unfortunately, there is a lack of research suggesting mechanisms for managing the handling of personal information in the context of OMSs (e.g., Squicciarini et al. 2009). In this study, we develop design requirements, design principles, and an instantiation of a peer-privacy-friendly OMS in the form of mockups to enable the senders' and receivers' control and awareness of data handling processes for personal information from peers.

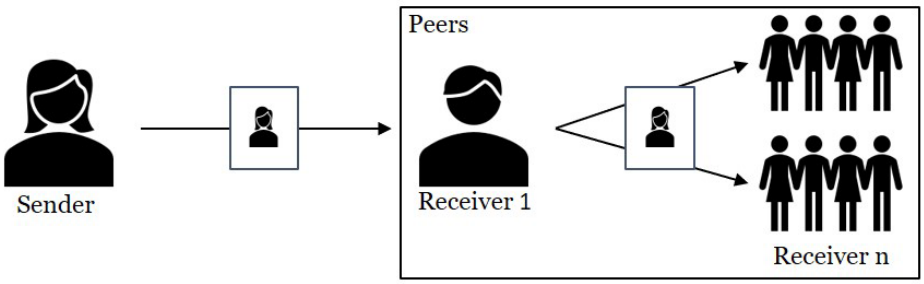

Figure 3. The process of sharing personal information

4.3 Design Science Research

To design a peer-privacy-friendly socio-technical artifact in the context of OMS, we apply the well-established DSR methodology (Gregor and Hevner 2013; Hevner et al. 2004). DSR is the most suitable method to achieve our goal due to its wide applicability for

investigating general real-world problems (Baskerville et al. 2015; Venable and Baskerville 2010) like the control and awareness gap between a sender's privacy expectations and the receivers' actual handling of the sender's personal information. Specifically, we seek to develop a socio-technical artifact that can be deployed in practice: a peer-privacy-friendly OMS that considers the interdependency of privacy decisions insofar as they are made in a social system of multiple users exchanging information that goes beyond the pure consideration of the technical aspects of our artifact. We combine the theoretical understanding of information privacy research (e.g., Malhotra et al. 2004; Zhang et al. 2022) with users' actual needs (through an evaluation from the user's perspective) in order to deepen the understanding of how to mitigate peer privacy concerns. In this regard, DSR provides an established, concise approach to developing such designs whilst allowing for multiple design cycles to iteratively improve them. The user-centered perspective is important for mitigating individuals' peer privacy concerns and providing actionable features. To ensure that we address these aims, we follow the DSR methodology proposed by Vaishnavi and Kuechler (2007) and Peffers et al. (2007).

Figure 4 visualizes our approach, which consists of three design cycles: In cycle 1, we began by identifying the real-world problem under investigation in more detail. In order to account for rigor in our design process (Hevner et al. 2004), we reviewed related literature on peer privacy concerns and used Malhotra et al.'s (2004) IUIPC framework as the kernel theory. The IUIPC framework guided the development of our design requirements and further enriched the formulation of our preliminary design principles. To ensure the relevance of the identified problems (P1 – P4) (Hevner et al. 2004) and evaluate the suitability of the design requirements, we conducted focus group discussions. In cycle 2, we reflected on the results of cycle 1, as proposed by Vaishnavi and Kuechler (2007), and we derived insights for our preliminary design principles. In addition, we analyzed existing OMSs and their peer privacy features to further refine our preliminary design principles, and we evaluated these principles based on interviews of OMS users to further extend and refine the principles. These insights served as input knowledge for the next cycle. In cycle 3, as suggested by Peffers et al. (2007), we again iterated and extended our final design principles. In this cycle, we also created mockups in line with the design principles to comprehensively instantiate the design principles and to support the evaluation and demonstration phase. Here we followed the approach of Peffers et al. (2007), who proposed demonstrating the socio-technical artifact before evaluating it. To evaluate the effectiveness of our design principles, we conducted a survey study among OMS users.

Although Vaishnavi and Kuechler (2007) term the final phase of a DSR project the "Conclusion," we communicate the results of our DSR study following the approach of Peffers et al. (2007) by writing this conference paper.

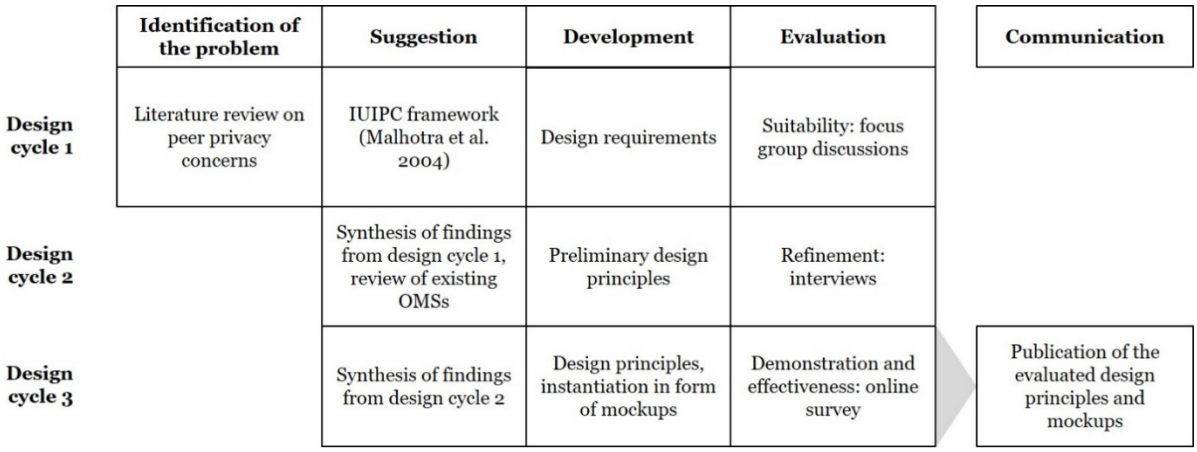

Figure 4. DSR methodology for our study

4.3.1 Design Cycle 1: Design Requirements and Suitability

Following Peffers et al. (2007), we begin the first design cycle with an extensive literature review (see section Research Gap: A Review of the Literature) to substantiate our real-world problem of peer privacy concerns. In the suggestion phase, we build on Malhotra et al.'s (2004) IUIPC framework to develop our design requirements (DRs). These requirements represent general guidelines (Hevner et al. 2004) that can be transferred to any OMS to make it peer-privacy friendly. According to the IUIPC framework, privacy concerns exhibit into three subdimensions: collection, control, and awareness. Collection refers to the extent to which a person is concerned about the amount of their personal information that is processed relative to the advantages that are received as well as the appropriateness of this concern (Malhotra et al. 2004). In the e-commerce context, this usually means that users are not exploited by privacy-intrusive data gathering mechanisms. Applying this idea to the peer privacy context, we assume that how peers handle others' personal information may raise concerns among individuals. Thus, we formulate the first design requirement as follows:

DR1. Given the amount of personal information that is collected (unintentionally) by peers, an OMS should consider users' concerns that may be triggered by peers' collection of such information.

Second, Malhotra et al. (2004) propose that an individual's privacy concerns regarding privacy originate from the feeling of losing control over one's personal information when sharing it with others. These concerns can be reduced if users can approve or modify the processing of their personal information or request the deletion of this personal information (Caudill and Murphy 2000). Thus, individuals perceive the collection of personal information to be appropriate when they can decide who, when, and how far their personal information can be processed (Zhang et al. 2022). Hence, we propose the second design requirement:

DR2. An OMS should enable users to control the personal information they share with peers.

Third, awareness refers to the extent to which a user knows how peers handle their own personal information (Culnan 1995; Malhotra et al. 2004). The concept of awareness includes the extent to which other parties are transparent about their data practices and communicate how they process personal information (Malhotra et al. 2004). Thus, we propose the third design requirement:

DR3. An OMS should inform users about how peers handle their shared personal information in order to create awareness.

Focus group discussions. To test the suitability and ensure the relevance of these design requirements, we conducted two focus group discussions. We deem focus group discussions to be appropriate at a very early stage of the DSR study due to the lack of existing knowledge regarding the interdependency of privacy decisions in the context of OMSs. By allowing direct interactions between OMS users during the focus group discussions, we can identify the specific requirements and needs of users with differing privacy attitudes. Following Tremblay et al. (2010), we used two exploratory focus groups with five and six participants and a duration of approximately 90 minutes each to achieve rapid incremental improvements in the artifact design along the social dimension. Since our goal was to evaluate the privacy expectations of OMS users, we recruited psychologists and engineers who regularly use OMSs. One author moderated the discussions with an initial introduction to the peer privacy context in OMSs, followed by general questions, and then more specific ones at the end. For instance, the researcher asked participants what they would expect from a receiver when they share a message with him or her. Applying open coding (Miles et al. 2019), we screened the transcripts for concepts related to the three subdimensions of privacy concerns explained earlier and

searched for supporting or contrasting arguments. Specifically, two researchers coded the transcripts separately, discussed, and categorized the emerging needs of the participants. Using this process, we were able to confirm all three design requirements. Regarding DR1, more than half of the participants expressed peer privacy concerns and described situations where they felt uncomfortable with co-owners' privacy decisions. Thus, DR1 was supported. Second, aligning with DR2, participants suggested the possibility of setting privacy settings for each message and/or receiver. However, they also mentioned that those features should not affect the usability of OMSs. The need to be able to communicate privacy expectations in a more fine-grained way for some messages from a sender to a receiver thus resulted in some preliminary design principles. Regarding DR3, we identified a gap between the sender's privacy expectations and the actual handling of the sender's personal information by the receiver. In particular, receivers face the challenge of anticipating others' privacy decisions or expectations. This is because peer privacy concerns differ strongly across users. For instance, some focus group participants said they had no concerns at all when sharing photos via an OMS, while such sharing was unacceptable for others. The literature confirms that privacy expectations vary widely and even change over time (Stutzman and Kramer-Duffield 2010). This diametric alignment suggests that senders and receivers need to be able to communicate and regulate the data practices for shared content. Based on the results of the literature review, our kernel theory, and the focus group discussions, we developed a preliminary set of design principles with regard to awareness and control.

4.3.2 Design Cycle 2: Refinement

Analysis of existing OMSs. After evaluating the design requirements and deriving preliminary design principles, we analyzed OMSs that are commonly used in Europe. Specifically, we analyzed messenger applications on smartphones with the highest user rate in Europe (Statista 2022): WhatsApp, Facebook Messenger, Signal, Telegram, and Snapchat. The goal was to examine which peer-privacy-friendly messaging features are already used to strengthen the users' control and awareness. As illustrated in Table 4, OMSs have begun to provide features regarding one-time views of content by receivers.

Table 4. Privacy-friendly messaging features

Privacy-friendly messaging features	WhatsApp	Facebook Messenger	Signal	Telegram	Snapchat
Prevents re-sharing messages	x	✓	x	x	x
Indicates a "forwarded" label	✓	✓	✓	✓	✓

One-time view of messages for receivers	✓	✓	✓	✓	✓
Blocks screenshots	x	x	x	x	x
Screenshot notifications for senders	x	x	x	✓	✓
Prevents storage of transmitted files in the receiver's memory	x	x	x	x	x
Fine-grained privacy setting for each message	x	x	x	x	x
Raises awareness regarding sharing personal information about others	x	x	x	x	x
Notifications of what peers are doing with others' content	x	x	x	x	x

Thus, senders can ensure that their content cannot be re-shared or stored on the receiver's device by using the one-time view function. However, receivers are able to take screenshots of the content. Apart from Telegram and Snapchat (Vaterlaus et al. 2016), this option is not promoted by OMSs and thus is rarely used by their users. Except for Facebook's Messenger, no provider prevents messages from being re-shared. For example, messages (e.g., photos) are automatically saved on the receivers' devices, and hence these messages can also be forwarded by another app (e.g., a photo app) on the device. What all of the OMSs have in common is that it is not possible to make fine-grained decisions about what the receiver can do with the content. Currently, if a content is being shared, the sender can only decide whether the receiver can see/read the shared message for a few seconds or can freely process the content. These insights further informed the formulation of the design principles and the instantiation of the peer-privacy-friendly OMS that was then evaluated based on interviews.

Interviews. We used interviews to evaluate and refine the preliminary design principles. In total, two researchers conducted ten semi-structured interviews via zoom and in person (six males, four females). We targeted frequent OMS users because of their experience with online peer-to-peer communication, potential privacy concerns, and ability to imagine design principles and features. The participants were between 21 and 32 years old, representing the largest share of OMS users (Auxiert and Anderson 2021). They included a salesperson, students, police officers, researchers, consultants, and recruiters.

The interview procedure was as follows: First, the participants were introduced to our context of peer privacy concerns in OMS. Second, each preliminary design principle was individually presented to the participants. For each preliminary design principle, the

participants were asked the following four questions: (1) Do you understand the principle? (2) Do you think the principle is useful for mitigating peer privacy concerns? (3) Would you like to see the principle introduced, and if not, why not? (4) Do you have any suggestions for improvement? Each question was asked and answered individually before presenting the next question. The first question aimed to check whether the participants could understand the preliminary design principles without any additional explanation, while the remaining three questions were related to the meaningfulness of the preliminary design principles themselves. More specifically, question (2) was related to the participants' thoughts about the preliminary design principle and its impact on their peer privacy concerns. Question (3) specifically asked the participants whether they would introduce the preliminary design principle because we assumed that OMSs have features that are considered useful but are not used due to the increased effort that is required or for other reasons. To avoid such problems and maximize the utility of the preliminary design principles, the question (4) asked participants for possible improvements.

Afterwards, each interview was transcribed and analyzed based on Ryan and Bernhard (2003). Specifically, we traced the transcripts for perceptions about peer privacy concerns and potential features that could help to mitigate these. Two authors coded the transcripts, and multiple concepts per response were allowed. We related these concepts to prior literature in the field of privacy concerns and to the preliminary design principles. Overall, the interview process led to the following refinements of the preliminary design principles. Regarding control, all participants agreed that they need a higher level of control over peers' data practices; however, it was highlighted that it is not necessary to control every message for each receiver: "I think I'd rather decide for myself whether I want to restrict the sender to further process my data. It shouldn't be a standard pop-up that might annoy me after a certain time." Instead, participants preferred setting receiver groups that differentiated between people for whom certain privacy settings would be needed for shared messages and people for whom privacy settings would not be needed because of a high level of trust, such as close ties. Regarding awareness, six participants reported that they would like to see awareness-related principles introduced. However, they also pointed out that a sender can share content that belongs to other peers, and they indicated that if they were made aware that they were sharing other people's personal information, they would reconsider whether they should actually share that information. Finally, the interviews also confirmed what we had already found in the focus group discussions, namely, that the number of notifications and the effort required to protect personal

information should not be too high and should not jeopardize the overall usability of the OMS.

4.3.3 Design Cycle 3: Demonstration and Effectiveness

In design cycle 3, we again refined our design principles. This time, we created an instantiation of our peer-privacy-friendly OMS in the form of mockups visualizing the different design principles. Our socio-technical artifact was informed by the literature review on peer privacy concerns in particular and privacy-enhancing mechanisms in general, the IUIPC framework, the focus group discussion, a review of common messaging services, and the interviews. A prerequisite for all design principles stems from users' concerns about the collection of personal information, as expressed in DR1.

Design Principles 1: Control. The design principles regarding control provide a solution for P1 and P2 and are responsive to DR2. More specifically, the principles propose that a peer-privacy-friendly OMS should enable senders to control how receivers can handle the shared data. As supported by the IUIPC framework, the focus groups, and the interviews, OMS users require features that will help them to set find-grained privacy settings for shared content. DP1a indicates that senders should be able to select privacy settings on a fine-grained level, while DP1b indicates that these fine-granular privacy settings should also be available per message:

DP1a: For a peer-privacy-friendly OMS to leverage control over personal information, the sender should be able to select receiver's access rights and the further processing of a shared message that is allowed on a fine-grained level.

DP1b: For a peer-privacy-friendly OMS to leverage control over personal information, the sender should be able to select the privacy settings for each message.

To ensure the senders' privacy settings in DP1a and DP1b, technical enforcement is required. For example, if a sender decides that a message should only be displayed briefly, it should not be technically possible for the receiver to download this message. This principle builds on the single-view feature found in existing messengers such as Signal and WhatsApp (Signal 2022; WhatsApp 2022). However, WhatsApp's documentation points out that the sender is not protected from screenshots that might be taken by receivers. Therefore, our fine-grained privacy settings in DP1a and DP1b move beyond existing technical applications, because receivers' data practices are restricted in a more comprehensive manner.

As stated by our interviewees, the setting control feature should not pop up for each message. Therefore, we included this feature (which we call "Secure Photo", displayed in Figure 5) in the settings that need to be proactively opened by the user. Here the sender can select whether the content can be re-shared, viewed for more than a few seconds, duplicated (in the form of a screenshot), or saved on the receiver's device.

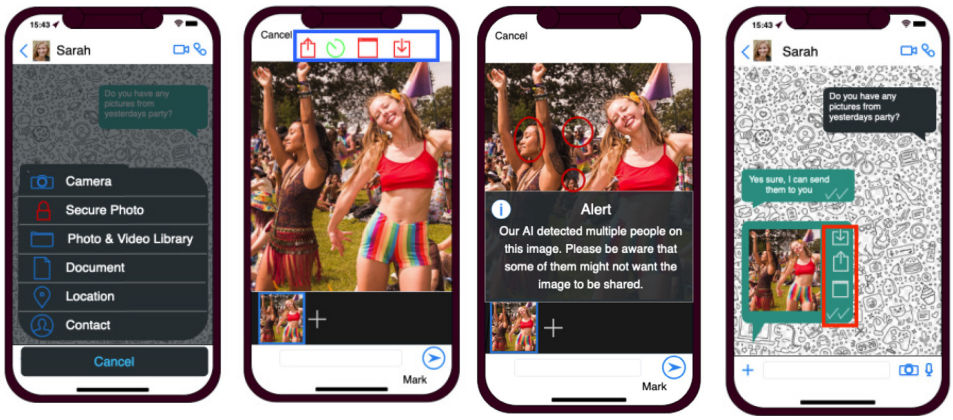

Figure 5. Demonstration of fine-grained peer privacy settings

As recommended by Wang et al. (2011) and shown in Figure 5, the icons and color themes can be inspired by familiar interfaces. For instance, green icons mean "possible," while red icons mean "restricted."

Design Principle 2: Awareness. Addressing P3 and P4 and conforming to DR3, we investigated design principles regarding awareness. As a result of the focus group discussions (our extension phase in design cycle 1), our first two design principles related to awareness (Malhotra et al. 2004) affect the sender and the receiver:

DP2a: For a peer-privacy-friendly OMS to leverage awareness of data processing, senders should be notified in a standardized way about how the receiver handles the sender's personal information.

DP2b: For a peer-privacy-friendly OMS to leverage awareness of senders' privacy expectations, receivers should be informed about senders' privacy preferences.

On the one hand, the OMS should communicate to senders in a transparent and standardized way how their data is actually processed by receivers. This can be done either actively in the form of a notification tool or passively (i.e., as information that needs to be retrieved by checking the status of a message). For instance, to inform a sender about the receiver's data processing actions, an icon can be implemented next to the message that displays various potential actions of the receiver. A similar feature can already be found in

existing OMSs, where senders can get a read receipt in the form of a check mark next to the message. In this way, the sender can be informed whether and how often his/her personal information has been forwarded, saved, or screenshotted.

On the other hand, receivers should also be made aware of senders' privacy expectations—that is, receivers should be informed about what they are allowed to do with the message that a sender has shared so that they can make sound privacy decisions. Similar to the "privacy nutrition label" proposed by Kelley et al. (2009), we propose that receivers should be notified in a unified and comprehensive way in order to avoid misunderstandings and thus potential privacy threats. In addition, technical solutions can be implemented that prevent the receiver from circumventing the privacy rules defined by the sender. For example, senders could be able to specify whether their messages may be forwarded, screen-shotted, or saved on others' devices. As another example, to prevent a message from being stored on the receiver's device, the message could be loaded into the cache, and when the messaging application is closed, the cache can be deleted (Chen and Hahn 2020).

The interviews also revealed that awareness means that senders should be informed about their responsibility to make privacy decisions that are in line with all co-owners' privacy expectations. For example, if someone takes a group photo and then shares it via a direct message, this person is disclosing personal information about the whole group. The third awareness design principle ensures that senders will be made aware when they are about to share personal information about others:

DP2c: For a peer-privacy-friendly OMS to leverage awareness of different privacy expectations, senders should be made aware of co-ownership of personal information when they are sharing that information.

To increase users' awareness of the different privacy expectations of other users, alerts can be used. For example, machine learning could be used to detect whether a photo depicts several people. If the machine learning algorithm detects several persons in a photo, an alert in the form of a pop-up window could indicate that permission from all persons is required for disclosing this photo. Similar mechanisms could be implemented in the case of voice messages or any other type of shared information that is co-owned.

Survey. The goal of the third evaluation cycle was to evaluate the effectiveness of our socio-technical artifact in mitigating peer privacy concerns. In this regard, we empirically evaluated our design principles among OMS users with the help of instantiations in the form of mockups. We examined whether these users had fewer peer privacy concerns

when the additional instantiations were introduced. To demonstrate our artifact, we created four different mockups representing our suggestions for instantiations. These included one mockup that did not reflect any of our design principles and thus served as the control scenario for testing whether our artifact would have an impact on privacy concerns. Since some of the design principles could not be implemented separately, they were illustrated in a single mockup. We developed a scenario-based survey in order to be able to present our socio-technical artifact in a realistic manner and to compare different groups (for a review see Brakemeier et al. (2017)). Since one of the focus groups had discussed the situation of a photo from a party being forwarded without the consent of the original sender, we decided to use this scenario for our final evaluation. The scenario was the following:

"Yesterday, Sarah attended a party, where many photos were taken. Since Mark missed the party, he asks Sarah for photos over a messenger. Sarah answers that she will send a photo to him. Afterwards, Sarah chooses one of the photos where she is dancing and sends it to Mark."

All of the participants were asked to imagine being Sarah in the described scenario. In developing the mockups, we leaned on the interface design of well-known OMSs such as iMessage, WhatsApp, and Signal. This helped us to present mockups that were easy to understand and did not deviate in major ways from existing approaches. The mockups represented the instantiation of the peer-privacy-friendly OMS. To avoid biases in the results, a fictitious messaging service was used to ensure that no user had positive or negative experiences with the service in the context of peers (Ozdemir et al. 2017). All features were built in accordance with this mockup design and differed only in the objective of the specific instantiation under investigation. In Table 5, we describe the mockups in detail. Additionally, we have presented exemplary mockups in Figure 5 for groups 2, 3, and 4.

Table 5. Description of mockups

Mockup description	DP
Group 1 (G1): The first mockup represented the control group. The mockup demonstrates a basic photo sharing process that is similar to those in existing OMSs. The representation was not enhanced by any peer privacy feature. The mockup illustrates a chat history between Sarah and Mark. This view was deliberately chosen because the design principles were intended to evaluate the control and awareness of the sender as well as the receiver. The mockup illustrated the following scenario: Mark asks Sarah if she has a photo of the yesterday's party. Sarah sends him the photo.	Control Group

Group 2 (G2): The second mockup demonstrated a peer-privacy-friendly extension that consists of fine-grained privacy settings for each message, called the "Secure Photo Feature". What makes this feature peer-privacy-friendly is that it allows the sender to make fine-grained settings for sharing messages (i.e., a photo). These include whether the receiver is allowed to i) forward the message, ii) take a screenshot, or iii) download the message, and iv) how long the receiver is able to view the content of the message. Since it is up to the sender to decide what the receiver is allowed to do with the received message, DP1a and DP1b are evaluated using this mockup. In addition, the fine-grained setting informs the receiver about the senders' privacy preferences, which means that DP2b can also be evaluated.	DP1a DP1b DP2b
Group 3 (G3): The third mockup illustrated a feature that increases the sender's awareness of the co-ownership of personal information. Specifically, when a sender shares content that also contains personal information about others, the sender is made aware of this through a pop-up window indicating that s/he is sharing the personal information of others. In our scenario, when Sarah creates the message to Mark including the photo of yesterday's party, a pop-up window informs Sarah that she is sharing other people's information. As the sender is made aware of sharing the personal information of others, we evaluate DP2c with this mockup.	DP2c
Group 4 (G4): The fourth mockup illustrated a peer-privacy-friendly extension that informs the sender about what the receiver has actually done with the sender's message (in this case, a photo). In more detail, Sarah shared with Mark a photo of herself that included others from yesterdays' party. Additional icons were added to the photo to notify the sender (Sarah) that the photo has been i) forwarded, ii) screenshotted, or iii) downloaded by the receiver (Mark). This icon was inspired by the blue ticks on common messaging services that indicate whether the receiver has read a message. For the mockup, a gray share icon means that the action was not performed, while a blue share icon indicates that the action was performed. Therefore, this feature increases the sender's awareness by informing the sender about what happened to their information after it was shared. Thus, we can evaluate DP2a using this 4th mockup.	DP2a

We used an online survey to collect the data. The average completion time was about 6 minutes. The link was distributed through social media, and two 10-euro amazon vouchers were raffled. We randomly assigned the respondents to either the control group or one of the three treatment groups. The described scenario did not vary. We measured demographics and controls as well as peer-shared information privacy concerns (PCIPC) and self-shared information privacy concerns (SSIPC) as developed by Zhang et al. (2022) (see Table 6). Using these scales, we measured respondents' worries about losing control over their personal information that is shared with peers. To control whether respondents had imagined the described scenario and understood the new features, an attention check was employed. Respondents had to select one of four statements that best described the presented mockup, for instance, "Before sending, Sarah defined what Mark can do with the photo (download, share, ...)." After screening out respondents who i) failed the attention

check, ii) completed the survey unrealistically quickly (less than 3 minutes), or iii) clicked Likert scale in a straight line (Zhang and Conrad 2014), the final data sample consisted of n = 138 participants. The sample consisted of 68 males and 70 females, and the age distribution was 59 participants between 18 and 24, 62 participants between 25 and 30, 14 participants between 31 and 40 years old, and 3 participants older than 40 years. The mean value for all participants' OMS experience was 6.18 measured on a 7-point Likert scale, with 7=strongly agree.

To test whether our design principles significantly decreased peer privacy concerns, we run t-tests. Specifically, we used the t-statistics to identify significant differences between the control group (G1) and the other groups (G2–G4). A significant difference between the mean value of the control group and that of the treatment group in question would indicate that the design principles and associated messenger function had a significant impact on users' PSIPC and SSIPC.

Table 6. Constructs based on Zhang et al. (2022)

Item Description (7-point Likert scale, 1=Strongly disagree, 7=Strongly agree)	
Peer-Shared Information Privacy Concerns (PSIPC)	**Self-Shared Information Privacy Concerns (SSIPC)**
1) I am concerned that my friends can share embarrassing information about me on the messenger. 2) I am worried that I may not have full control over who can share information about me on the messenger. 3) I am concerned that my messenger friends may share information about me on the messenger that are not correct. 4) I am concerned that my messenger friends may share inaccurate information about me on the messenger.	1) It bothers me that I do not have control over how the personal information I share on the messenger is used by my messenger friends. 2) I am concerned that my messenger friends can use the personal information that I share on the messenger for other purposes. 3) I am concerned that my messenger peers can unintentionally (through their "sharing" activities) expose photos I shared to people who were originally not intended receivers by me. 4) I am concerned that my messenger friends can unintentionally (through their "sharing" activities) expose my messages to people who were originally not intended receivers by me.

Results. In group 1 (n = 36), the mean for PSIPC was 4.63 and for SSIPC was 4.57. In group 2 (n = 36), the mean for PSIPC was 3.19 and for SSIPC was 3.24. In group 3 (n = 30), the mean for PSIPC was 3.31 and for PSIPC was 3.53. In group 4 (n = 36), the mean for PSIP was 3.99 and for SSIPC was 4.37. To provide empirical support for the mean comparison results, we conducted three t-tests for each of the PSIPC and SSIPC constructs. First, we tested for each construct PSIP and SSIPC and for each group if it holds the

assumption of normal distribution by conducting the Shaprio-Wilk test. This test assumes that the sample is normally distributed (null hypothesis). All p-values for each construct (PSIP and SSIPC) and in each group is greater than the significance level of 5% which is evidence that the data are normally distributed. Second, we tested whether the assumption of the homogeneity of variances was fulfilled in order to apply the t-test based on the Levene test (Levene 1960). The test assumes the null hypothesis of the equality of variances between groups. The Levene test revealed that both the PSIPC ($p < 0.54$) and the SSIPC ($p < 0.42$) rejected the null hypothesis at the 5% significance level (Lim and Loh 1996). Accordingly, we confirmed the statistically significant homogeneity of the variances. After Shaprio-Wilk test confirmed normal distribution and Levene's test indicated that the variances for the PSIPC and SSIPC constructs were statistically equal, we performed a t-test to determine the equality of the means among the variables. The results are presented in Table 7.

Table 7. Results of t-statistics

Groups	**G1&G2**		**G1&G3**		**G1&G4**	
Constructs	**PSIPC**	**SSIPC**	**PSIPC**	**SSIPC**	**PSIPC**	**SSIPC**
t-values	4.84***	4.49***	4.56***	3.64***	2.16*	0.68

Note. ***p<0.001, **p<0.01, *p<0.05.

For **G1 & G2**, the results of the t-test confirmed that the mean values of the PSIPC construct for groups G1 (mean=4.63) and G2 (mean=3.19) are significantly different at the 5% significance level ($p<0.001$). Thus, the mean value for the control group is significantly higher than the mean value for G2, indicating that the design principles DP1a, DP1b, and DP2b lead to less PSIPC. Furthermore, the t-test results also confirmed that the mean values of the SSIPC for groups G1 (mean=4.57) and G2 (mean=3.24) are significantly different at the 5% significance level ($p<0.001$). Since the mean value for the control group is significantly higher than the mean value for G2, the design principles DP1a, DP1b, and DP2b lead to less SSIPC.

For **G1 & G3**, the results of the t-test confirmed that the mean values of the construct PSIPC for groups G1 (mean=4.63) and G3 (mean=3.31) are significantly different at the 5% significance level ($p<0.001$). Thus, the mean value for the control group is significantly higher than the mean value for G3, indicating that the design principle DP2c leads to less PSIPC. Furthermore, the t-test results confirmed that the mean values of the construct SSIPC for groups G1 (mean=4.57) and G3 (mean=3.53) are significantly different at the

5% significance level ($p<0.05$). Since the mean value for the control group is significantly higher than the mean value for G3, the design principle DP2c leads to less SSIPC.

For **G1 & G4**, the t-test results confirmed that the mean values of the PSIPC construct for groups G1 (mean=4.63) and G4 (mean=3.99) are significantly different at the 5% significance level ($p>0.05$). Since the mean value for the control group is significantly higher than the mean value for G4, the design principle DP2a leads to less PSIPC. The t-test results did not confirm that the mean values of the SSIPC construct for groups G1 (mean=4.58) and G4 (mean=4.37) are significantly different at the 5% significance level ($p>0.05$). Since the mean value of the control group is not significantly higher than the mean value of G4, the design principle DP2a does not lead to less SSIPC.

For robustness analysis, we observed to what extent the results of the t-test and the p-values changed with alternative analytical choices for each of the constructs. First, we changed the confidence interval from 95% to 97.5% when performing the t-test. This revealed that the t-statistic and the p-values did not change. Second, we excluded the last two observations in the data sample set. This showed that the t-statistic changed slightly, but the p-values did not change expect for the construct PSIPC when comparing G1 & G4. The significance level changed from $p = 0.035$ to $p = 0.067$. Third, we included the preciously removed outliers. We found that the t-statistic changed slightly, but the p-values did not change except for the construct PSIPC when comparing G1 & G4. The significance level changed from $p = 0.035$ to $p = 0.232$. We critically discuss this observation in the following chapter.

4.4 Discussion, Limitations, and Future Research

In this paper, we aim to develop a socio-technical artifact—a peer-privacy-friendly OMS—including design requirements, design principles, and an instantiation in the form of mockups to mitigate peer privacy concerns. Currently, when using OMSs, users cannot control how peers handle their shared data; instead, they are trapped by the imposed features, facing binary share/not share decisions without fine-grained privacy settings for each message and/or receiver. In addition, they lack awareness regarding how their data is stored, processed, or reshared by peers and what peers are allowed to do with the data they receive. Using DSR methodology, we propose five design principles that were refined and evaluated in three design cycles, following the DSR process developed by Vaishnavi and Kuechler (2007) and Peffers et al. (2007). Malhotra et al.'s (2004) IUIPC framework

guides our designs as kernel theory with a special focus on increasing users' control over the data they share and their awareness regarding peers' data handling procedures. Additionally, we created mockups to demonstrate and thus evaluate our principles among frequent OMS users. Our evaluation of the design principles shows that our socio-technical artifact significantly decreases peer privacy concerns in the context of OMS compared to a baseline scenario.

The design principles DP1a and DP1b aim to increase senders' control over how their personal information is used. These principles emphasize the need for OMS users to be able to control who can process their shared information, and when and how it can be processed. These design principles are also supported by our evaluation showing that higher control along with fine-grained privacy settings do indeed mitigate peer privacy concerns. Design principles DP2a to DP2c are concerned with senders' and receivers' awareness of privacy practices and expectations. DP2a and DP2c address senders' need to be informed about receivers' data handling practices. While design principle DP2c was supported, design principle DP2a (by which senders are notified about the receiver's data handling processes) was able to partially decrease PSIPC, but not SSIPC. Potential reasons might be that higher awareness regarding data practices can lead to two contrasting outcomes: On the one hand, a higher level of awareness is associated with lower peer privacy concerns due to the fact that data handling procedures become transparent and thus more trustworthy (Malhotra et al. 2004). On the other hand, greater awareness might lead to a higher focus on potential privacy threats and thus raise concerns (Gerlach et al. 2015). Since privacy practices become more transparent, this leads to a more substantiated justification and thus evaluability of concerns (Brakemeier et al. 2017). Principle DP2b takes the perspective of the receiver. It highlights the need for the receiver to be informed about senders' privacy expectations in order to be able to make sound privacy decisions in line with senders' preferences. Overall, all of the evaluated design principles except for design principle DP2a resulted in a significant decrease of peer privacy concerns.

We provide the following theoretical contributions: First, as peer privacy concerns have been identified as a major inhibitor of online self-disclosure (Ozdemir et al. 2017; Zhang et al. 2022), we are among the first to extend prior literature by proposing how these concerns can be mitigated. Prior literature investigating the concept of peer privacy concerns is primarily concerned with its measurement (Zhang et al. 2022), its impact on disclosure decisions (Ozdemir et al. 2017), and other behavioral outcomes (Such et al. 2017). By

applying the DSR methodology, we contribute to prior literature by developing a socio-technical artifact consisting of design requirements, actionable design principles, and an instantiation of a peer-privacy-friendly OMS in the form of mockups to mitigate peer privacy concerns. In this respect, we respond to Pu and Grossklags's) call for research to provide privacy-friendly mechanisms for senders to communicate their privacy expectations in a standardized and convenient way.

Second, we contribute to privacy-related DSR studies that have developed and evaluated IT artifacts by going beyond the concept of organizational privacy concerns (e.g., Gerlach et al. 2022; Paefgen et al. 2012; Sjöström et al. 2022). We shift the focus from user-to-provider interactions to peer-to-peer communication. Our socio-technical artifact bears similarities to and differences from IT artifacts that mitigate organizational privacy concerns, such as privacy-friendly social media sites (Angelopoulos et al. 2021). Our design principles are similar to prior work in terms of a higher level of control through fine-grained privacy settings (Wang et al. 2011) or a higher level of privacy stewardship (Angelopoulos et al. 2021). Nevertheless, our work differs with regard to the conceptualization of privacy as being embedded in an interconnected system with multiple interaction partners and shared ownership of data. While prior privacy studies have been concerned with dyadic user-to-provider interactions, our socio-technical artifact takes into account the interdependence of privacy decisions (Bélanger and James 2020) in settings where a number of users exchange information. Overall, our artifact extends the still limited knowledge about the prescriptive design of peer-privacy-friendly artifacts in IS.

Third, by focusing on peer privacy concerns, our socio-technical artifact also validates Malhotra et al.'s (2004) IUIPC framework, which was primarily tested in the organizational context, for the peer privacy context as well. We reconsider the three key dimensions of privacy concerns proposed by Malhotra et al.ualize them to privacy threats stemming from peers. On the one hand, we provide design principles for enabling senders to increase their control over their own personal information. On the other hand, we offer design principles to raise receivers' awareness of the privacy preferences of peers, i.e., how sensitive others consider their personal information and what activities are in accordance with senders' expectations. All of these principles are underpinned by technical solutions and mockups for a potential user interface. The creation of mockups constitutes a level-one artifact, according to Gregor and Hevner (2013), who provide recommendations for implementation that include user interface elements as a first step towards instantiation of a

peer-privacy-friendly OMS. To conclude, our artifact is effective in reducing peer privacy concerns as compared to common OMSs.

Beyond theoretical contributions, we provide several practical implications: First, we provide guidance regarding how to design and implement effective privacy-enhancing mechanisms for online messaging providers. Our mockups offer evaluated and specific features that can be implemented, such as a fine-grained selection option that enable senders to decide what the receivers are allowed to do with shared messages. By implementing these privacy-friendly design principles, providers can mitigate peer privacy concerns and thus improve their competitive advantage. Second, we have developed design principles that empower senders to communicate their privacy expectations in a standardized form; here we offer a user-centered design evaluated by frequent messaging service users. We present features for greater granularity of senders' control over their personal information and for leveraging awareness of the receivers' data practices. Hence, we provide a higher degree of awareness for both senders and receivers, and senders and receivers are both provided with an opportunity to regulate and apply the rules for sound privacy decisions that align with senders' expectations. Finally, our design requirements and principles may also be transferrable to privacy-enhancing technologies other than OMSs, where our design principles can also reduce potential privacy threats when very sensitive information is transferred between communication partners. As an example, if a doctor makes patient information available to another doctor in order to exchange opinions or to evaluate risky therapies, the doctor who sends the information could benefit from our DP1a and DP1b. In this respect, the patient's privacy would be preserved since secondary data use is excluded.

Finally, although we conducted this DSR study with great care, our study comes with several limitations that pave the way for further research. First, the scope of this study was to evaluate design principles and some instantiations in the form of mockups, but not a prototype. By developing a prototype, future research can test the usability of our design principles and test different variations. In this regard, future work can also consider the development and evaluation of different types of technical enforcement and user interfaces. We recommend consulting experts with technical expertise for the final evaluation. Second, we used photos as an exemplary type of personal information to evaluate our socio-technical artifact. However, we deem our design principles and instantiation of the peer-privacy-friendly OMS to be transferrable to other types of personal information, such

as voice messages, text, or videos. For instance, receivers can also be informed about a sender's privacy expectations regarding a voice message. Therefore, we suggest that future research focus on other types of data in the peer privacy context. Third, for DP2a we implemented a notification tool that overtly informs the sender about a receiver's actual data practices. Although both the focus groups and the interviews indicated that DP2a would be useful for messaging service users, the survey results do not confirm that this feature reduces SSIPC. Therefore, for future research, we suggest either testing this design principle in combination with other principles or creating it as a covert notification tool that allows the sender to retrieve information about peers' data practices if interested.

Acknowledgements

This research work was funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts through their joint support of the National Research Center for Applied Cybersecurity, ATHENE.

5 Paper C: The Power of Trust: Designing Trustworthy Machine Learning Systems in Healthcare

Title

The Power of Trust: Designing Trustworthy Machine Learning Systems in Healthcare

Authors

Mariska Fecho, Anne Zöll

Publication Outlet

International Conference on Information Systems

Abstract

Machine Learning (ML) systems have an enormous potential to improve medical care, but skepticism about their use persists. Their inscrutability is a major concern which can lead to negative attitudes reducing end users trust and resulting in rejection. Consequently, many ML systems in healthcare suffer from a lack of user-centricity. To overcome these challenges, we designed a user-centered, trustworthy ML system by applying design science research. The design includes meta-requirements and design principles instantiated by mockups. The design is grounded on our kernel theory, the Trustworthy Artificial Intelligence principles. In three design cycles, we refined the design through focus group discussions (N1=8), evaluation of existing applications, and an online survey (N2=40). Finally, an effectiveness test was conducted with end users (N3=80) to assess the perceived trustworthiness of our design. The results demonstrated that the end users did indeed perceive our design as more trustworthy.

Keywords

Trust, Machine Learning, Healthcare, Design Science Research, Trustworthy AI, Artificial Intelligence

5.1 Introduction

Over the recent years, and particularly during the COVID-19 pandemic, the healthcare sector has been subject to unprecedented strains and challenges, repeatedly testing its limits worldwide (Tong et al. 2022). One outstanding challenge is that physicians are overworked, and patients often have to wait months for appointments. Beyond that, an increasingly aging society demands additional medical care, underlining the need for scalable and accessible solutions that can alleviate the burden on the healthcare sector while improving patient outcomes. The growing prevalence of Information Systems (IS) in healthcare, specifically Machine Learning (ML) systems designed to aid in medical diagnoses, is anticipated to transform the provision of medical services, potentially serving as the primary point of contact for patient care (Siau and Wang 2018). ML systems are able to identify diseases like cancer and strokes from medical images or assist physicians during surgeries (Esteva et al. 2017; Taylor et al. 2016). The evolution of digitization and the proliferation of big data have caused a shift in the paradigm of decision-making from being solely reliant on human expertise and intuition to an approach that is predominantly data-driven (Berg 1997; Lebovitz et al. 2021). Especially for data-intensive and repetitive processes like image recognition in radiology or dermatology, ML systems can help to reduce physicians' workload and analysis costs (Buck et al. 2021). In addition, ML systems have shown great potential for facilitating self-examinations towards diseases for end users with various conditions without the need for physicians to be involved in the diagnosis process from the beginning (Takiddin et al. 2021). For example, ML systems enable end users to submit data such as skin images, health metrics, and descriptions of symptoms, which are then evaluated using ML algorithms for a health assessment (e.g., Baldauf et al. 2020). Such ML systems hold immense promise for end users, as they provide a convenient and accessible means of assessing health, improving the availability of medical care, and potentially reducing the burden on the healthcare sector.

However, ML systems supporting end users in diagnosing diseases are met with skepticism (Baldauf et al. 2020). Reasons include insufficient performance and privacy concerns. The non-use of ML systems by end users is exacerbated by algorithmic aversion, a phenomenon where individuals tend to prefer human support over ML algorithmic support, even if the latter performs better (Dietvorst et al. 2015). For instance, a study found that when physicians were unable to comprehend the reasoning behind a diagnostic algorithm's conclusion, they chose to rely on their own expertise and experience instead (Lebovitz et al. 2021). This suggests that in high-risk environments such as healthcare, end users are

more likely to trust human expertise than ML systems - especially when the decision-making process is opaque. Further factors such as inscrutability, biases and discrimination, and prediction inaccuracy could also hinder end users from building trust in ML systems (Berente et al. 2021; Gillath et al. 2021). Glikson and Woolley (2020) highlight the critical role that the notion of trust plays in shaping end users' perceptions of accepting ML advice (Dietvorst et al. 2015). In this sense, trust is paramount, as it helps overcome end users' skepticism and contributes to better adoption of ML systems.

Previous research has focused on the technical implementation of ML systems (Liu et al. 2020; Takiddin et al. 2021), particular factors influencing end users' trust in ML systems (Glikson and Woolley 2020; Li and Hahn 2022; Yang and Wibowo 2022), exploring the influence of trust on the adoption of ML systems (Handrich 2021; Lohoff and Rühr 2021), and identifying characteristics determining trustworthy ML (Kaur et al. 2022; Thiebes et al. 2020). There is, however, still a lack of research on how to design user-centered ML systems that reinforce trust in these technologies (Li and Hahn 2022; Riedl 2022). Thus, recent studies have called for concrete design recommendations for trust in user-centered ML systems (e.g., Riedl 2022). In addition, research studies on ML systems in the healthcare context have mostly focused on physicians as end users, often neglecting the perspective of end users without particular medical expertise (e.g., Jussupow et al. 2022; Lebovitz et al. 2021; Pumplun et al. 2019). Therefore, in this study, we refer to ML systems that support end users without requiring domain expertise. Our study aims to investigate the research question:

What design principles should be adopted to create trustworthy ML systems in healthcare for end users?

In this study, we present a socio-technical artifact, in our case, design principles (DP), for developing trustworthy ML systems to support end users. We employed a design science research (DSR) approach consisting of five phases: Awareness of the problem, suggestion, development, evaluation, and conclusion (Kuechler and Vaishnavi 2008) . These phases were iterated in three design cycles. In this vein, we derived 13 DPs for the design of trustworthy ML systems. This paper contributes to IS research by, first, responding to recent calls of research for the development of trustworthy ML systems (e.g., Riedl 2022). Second, we extend the existing trust literature by applying the trustworthy artificial intelligence (TAI) principles (Thiebes et al. 2020) to the context of ML systems and developing DPs that increase trust in these systems. Third, we present a unique approach to

designing ML systems, involving end users in all three design cycles and creating a social-technical artifact that meets the needs of its intended audience.

5.2 Theoretical Background

5.2.1 Trust in Machine Learning Systems

Trust has been widely researched in the IS domain (Glikson and Woolley 2020; McKnight et al. 2011; Thiebes et al. 2020). It's defined as the "willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. 1995). This definition has been used previously in the interpersonal domain (McKnight et al. 2011). It emphasizes that trust presupposes the vulnerability of the trustor, and it implies that the trustor is dependent on the actions of the trustee and cannot force the trustee to fulfill his expectations. Researchers argue that the trust definition applies beyond interpersonal relationships to the technology domain (Glikson and Woolley 2020; McKnight et al. 2011). Trust in technologies comprises three dimensions: Functionality, reliability, and helpfulness (McKnight et al. 2011). Functionality refers to the belief that a technology can successfully perform its intended task (i.e., provide necessary features to complete a task). A technology that works well and fulfills its intended purpose is considered functional. This property can help build trust in its ability to perform. Reliability describes the belief that a technology consistently functions properly. A technology that operates as expected and performs predictably in different situations is deemed reliable and can contribute to developing trust in its performance. Helpfulness refers to the belief that a technology offers sufficient assistance to end users, meaning that help and support functions provide necessary guidance. A technology that provides benefits to end users and supports them in achieving their goals is considered helpful, which can help build trust in its overall value. The technology trust constructs are used to evaluate the trustworthiness of a technology and can help end users decide whether they are comfortable using it. In addition, research has introduced technical concepts related to autonomous systems alongside trust in technologies (Lee and See 2004; Thiebes et al. 2020). Lee and See (2004) refer to the following three trusting beliefs to conceptualize trust in autonomous systems: Performance, purpose, and process. Performance refers to the ability demonstrated by autonomous systems to achieve their intended goal. Thus, performance is closely related to functionality. Purpose describes to

what extent the autonomous system is used in the developer's intent. This concept corresponds to helpfulness by reflecting that an autonomous system has a positive orientation towards end users. Process refers to how appropriate the autonomous system is for a given task and how well it can achieve the operator's goals. Consequently, process relates to the concepts of reliability (Thiebes et al. 2020).

Previous research on ML and trust mainly refers to the organizational context and present literature reviews (Kaur et al. 2022; Li and Hahn 2022), develop DPs to manage customer processes (Emamjome and Rosemann 2021), or frameworks to explore how ML systems impact trust (e.g., FEAS framework (Toreini et al. 2020), TAI Principles (Thiebes et al. 2020). Empirical studies explore how trust can be transferred from known technologies and providers to ML systems (Renner et al. 2021) or investigate the influence of trust on ML adoption (Handrich 2021; Lohoff and Rühr 2021). Trust-related studies on the individual level were conducted conceptually by developing frameworks that either distinguish user personality and trust in ML systems (Riedl 2022) or identify factors that affect trust in ML systems (Glikson and Woolley 2020; Yang and Wibowo 2022). Kim et al. (2021) explored the relationship between explainable AI and user behavior mediated by trust. The study revealed that trust effectively influences the interaction between humans and ML systems. The uniqueness of the role of trust within the context of ML systems is multifaceted. First, ML algorithms embedded in IT systems lack a physical presence. This lack of embodiment poses challenges to the development of trust between humans and ML. Human trust relies on physical cues, absent in ML systems. This absence of a visible identity makes the establishment of trust more complex and nuanced (Glikson and Woolley 2020; Li 2015). Second, ML systems possess a higher level of autonomy, enabling them to perform complex actions without direct human intervention (Berente et al. 2021). However, end users might not always be aware of the actual extent of ML's technological sophistication. This variability in perceived autonomy contributes to uncertainties in trusting ML systems. End-users may not be able to accurately assess when the ML is fully capable or when it may reach its limits (Glikson and Woolley 2020). Third, the non-deterministic nature of ML systems introduces perceived risks in human-ML relationships (Chao et al. 2016). Due to the algorithmic nature of ML systems, these risks arise from the potential for them to make unexpected or incorrect decisions. Finally, ML system's invisible nature, coupled with its potential for erroneous functions, contributes to a unique trajectory of trust, which means that trust in ML systems changes based on the feedback regarding its accuracy (Glikson and Woolley 2020). Initially, high levels of trust can be

quickly eroded when users encounter errors in ML systems, and rebuilding trust takes considerable time.

Previous literature on ML systems in healthcare has focused mainly on technical implementation. In particular, the literature has dealt with ML performance indicators for the diagnostic processes of diseases (Tofangchi et al. 2017), automated classification of patient data such as skin lesions using a convolutional neural network, the implementation of health telematics infrastructure (Schweiger et al. 2007), the development of collaboration platforms aiming in reinforcing the clinician–biostatistician relationship (Raptis et al. 2012), or the general implementation or design of mobile healthcare applications using ML (Greve et al. 2020; Ngassam et al. 2021). For instance, Greve et al. (2020) undertook the challenge of delivering non-communicable disease care for developing countries, a task demanding specialized medical equipment and expertise. To address this issue, the study set out to develop a mobile application to support community health workers in their routine care and counseling on non-communicable diseases. In addition, a critical task in cancer treatment strategy is to identify and establish links between key patient characteristics while streamlining redundant data and inefficiencies. This optimization enables cancer centers to deliver faster and more successful patient-centered treatment plans. Tofangchi et al. (2017) successfully used its ML system to identify a set of essential characteristics for treatment advice, such as the inflammatory response of the tissue surrounding a tumor. A few studies have also emphasized the implementation of user-centered mobile healthcare applications based on ML and investigated the end users' overall willingness-to-use (Baldauf et al., 2020). In addition, previous research explores how ML conversational agents and chatbots could be designed to interact with patients (Nguyen et al. 2021). However, most of the identified studies are related to the organizational level and clinical decision support systems (Braun et al. 2022; Pumplun et al. 2023). The ongoing research conducted by Braun et al. (2022) focuses on the development of design principles tailored to the development of ML systems specifically intended for use in clinical and healthcare settings. Thus, they were conducted in clinics where ML systems interact with or are assessed by physicians for diagnosis (Lebovitz et al. 2021). For instance, scholars explore how radiologists utilize diagnostic ML systems in clinical practice (Jussupow et al. 2022).

Table 8. Overview literature review

	Dimensions / Authors	Emamjome and Rosemann 2021	Glikson and Woolley 2020	Handrich 2021	Kaur et al. 2023	Kim et al. 2021	Li and Hahn 2022	Renner et al. 2021	Riedl 2022	Thiebes et al. 2020	Toreini et al. 2020	Yang and Wibowo 2022	Baldauf et al. 2020	Braun et al. 2022	Esteva et al. 2017	Greve et al. 2020	Jussupow et al. 2022	Lebovitz et al. 2021	Lohoff and Rühr 2021	Ngassam et al. 2021	Nguyen et al. 2021	Pumplun et al. 2023	Raptis et al. 2012	Rudin and Ustun 2018	Schweiger et al. 2007	Tofangchi et al. 2017
	Dimension	**Trust and ML**											**Healthcare and ML**													
Dimensions	Trust	x	x	x	x	x	x	x	x	x	x	x	x					x	x					x		
	Healthcare												x	x	x	x	x	x	x	x	x	x	x	x	x	x
	User-centered												x		x						x					
	Conversational Agents			x																	x					
	Physicians													x	x	x	x	x	x	x	x	x	x	x	x	x
	Patients												x							x					x	x
	Organizational	x	x	x	x		x	x		x	x			x	x	x	x	x	x	x	x	x	x	x	x	x
	Individual					x			x			x	x													
Methodology	Framework				x				x	x	x	x														
	Literature review		x		x		x																		x	
	Quantitative			x		x		x					x													
	Qualitative (Interviews)																	x		x						
	DSR	x												x		x					x	x				
	Techn. implementation												x		x	x				x	x		x	x	x	x
	Experiment																		x							
	Case Study																x									

Prior research has shown that interpreting the output of ML systems is challenging due to inscrutability (Berente et al. 2021), often likened to ML algorithms operating as black boxes with unexplainable inner logic (Adadi and Berrada 2018; Lebovitz et al. 2021; Rudin and Ustun 2018). Therefore, scholars have investigated how explainable ML systems could be designed to address the physician's needs (Pumplun et al. 2023) (see Table 8). Their findings suggest that ML systems should provide model and global explanations in clinical decision support systems when required. All in all, we identified a research gap in the design of user-centered trustworthy ML systems in healthcare, particularly within the individualized context. While the notion of trust is a widely explored concept in research, its practical application still presents challenges that have yet to be fully addressed (Emamjome and Rosemann 2021a, 2021b). Thus, we found that IS research lacks an in-depth exploration of how to design ML systems to earn end users' trust (Riedl 2022). Addressing this gap is important because patient safety, improved healthcare efficiency, and stakeholder acceptance depend on user-centered DPs that ensure trust in ML systems.

5.2.2 Systems Problem Awareness: Challenges in Fostering End Users' Trust in ML Systems

ML is not widely deployed in the healthcare sector for end users' (Baldauf et al. 2020), but there is a tremendous need since ML techniques assist in detecting early indicators for diseases and improve overall efficiency while lowering the cost of care (Buck et al. 2021). As ML represents a highly intricate technology, the literature inevitably engenders a host of issues, such as inscrutability, bias and discrimination, prediction inaccuracy, and privacy issues (Berente et al. 2021; Gillath et al. 2021; Rai 2020). Our efforts have centered on mitigating these issues, closely aligned with our research goals.

P1-Inscrutability: Inscrutability refers to the difficulty of understanding and interpreting the ML systems' output (Berente et al. 2021). It can be attributed to the probabilistic nature of ML, which makes its output variable difficult for end users to interpret and understand (i.e., how the model generates its predictions) (Adadi and Berrada 2018; Berente et al. 2021). This inscrutability has multiple facets, including opacity, transparency, explainability, and interpretability (Berente et al. 2021). Recently, a senior scholar has suggested that "inscrutability can hamper end users' trust in the system, especially in contexts where the consequences are significant, and lead to the rejection of the systems." (Rai 2020, p. 1). In healthcare ML system development, addressing inscrutability is paramount, as its implications can directly affect users' health and personal lives. Thus, the opacity inherent in ML systems may foster a sense of distrust, prompting end users to terminate their utilization of such systems. P2-Bias and discrimination: The issue of biases in ML algorithms is a major factor that contributes to the erosion of trust in these systems. Biases in ML refer to the existence of systematic errors or prejudices in the data, algorithms, or decision-making processes employed by ML systems (Berente et al. 2021; Rai 2020). Bias and discrimination in ML systems occur when the training data used to build the model contains inherent biases, leading the model to replicate and even amplify those biases in its predictions. This problem arises when the training data is not representative of the real world diversity it is intended to reflect. Biased ML systems can lead to inaccurate or unreliable predictions or recommendations, which could potentially result in harm or negative impacts on end users. For instance, ML-based image recognition systems that have been trained on biased datasets may wrongly identify or exclude certain racial or ethnic groups, resulting in discriminatory surveillance practices. Inscrutability (P1) could exacerbate the biases, making it difficult to detect and correct any issues that may impact the system's performance (Lebovitz et al. 2021). When end users perceive ML

systems as biased or discriminatory, they are likely to have less trust in the outputs. This can result in increased skepticism or even complete rejection (Lebovitz et al. 2021). This is particularly pertinent in healthcare ML systems, where biases can lead to discrimination against specific demographics, potentially resulting in unequal healthcare access and compromised health outcomes. P3-Prediction inaccuracy: Prediction accuracy refers to an ML system's ability to produce precise outputs or forecasts, closely tied to achieving high performance (Lebovitz et al. 2021; Thiebes et al. 2020). Prediction inaccuracy occurs when ML systems fail to make accurate predictions on new or unseen data. This problem arises from various factors such as inadequate training data, insufficient feature representation, model overfitting, or inappropriate model selection (Rai 2020). Prediction accuracy is one reliable factor of ML systems (Baskerville et al. 2015). If ML systems are not reliable or accurate, end users may question the effectiveness or usefulness of the ML system. Prediction accuracy in healthcare is critical since inaccuracies can profoundly impact lives. For instance, erroneous medical diagnoses by healthcare ML systems can lead to harm, fatalities, and a substantial erosion of trust in such systems (Davenport et al. 2019). P4-Privacy: Privacy refers to the protection of personal and sensitive information from unauthorized access, use, or disclosure (Malhotra et al. 2004). ML systems in healthcare gather, process, and store vast amounts of sensitive user data (e.g., health conditions). Failure to protect end users' privacy can cause privacy concerns (Rai 2020). Privacy concerns and lack of end users' control could result in mistrust, discontinuing use, and stopping the usage of the ML system in healthcare.

5.3 Overview of Design Science Research Process

Designing user-centered, trustworthy ML systems in healthcare requires a holistic approach that considers the social dimensions. It involves working with potential end users to ensure that ML systems meet their needs and expectations. DSR approach is most suitable since it involves the end user's perspective and allows for literately improving the socio-technical artifact. The DSR approach is also well-suited to addressing real-world challenges, such as those faced by the burdened healthcare sector (Gregor and Hevner 2013). Following the guidelines proposed by Kuechler and Vaishnavi (2008), we apply an iterative DSR approach, which comprises five sub-phases: Awareness of the problems, suggestion, development, evaluation, and conclusion (see Figure 6). In sum, we have conducted three design cycles to develop 13 DPs.

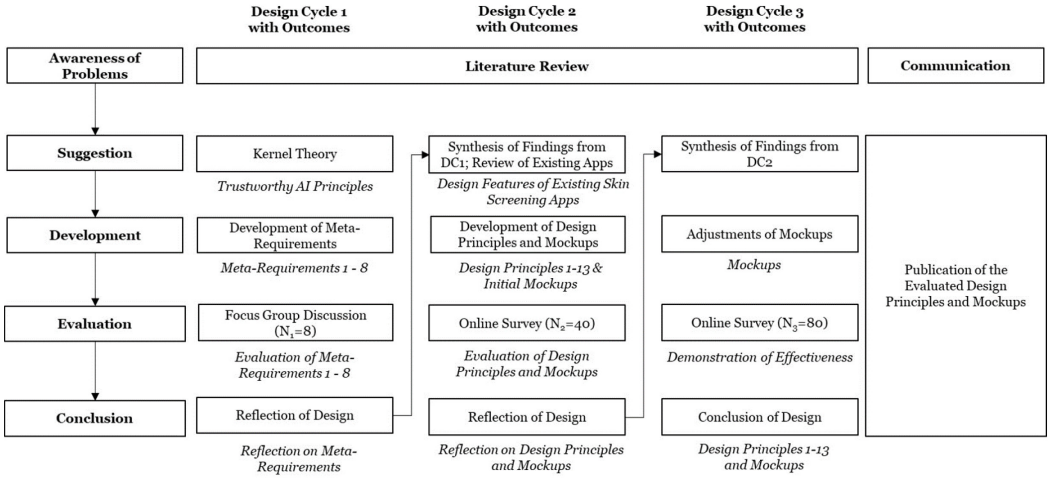

Figure 6. Design science research process according to Kuechler & Vaishnavi (2008)

Based on a literature review, we have identified certain problems of ML systems that lead to lower end user trust and derive relevant meta-requirements (MRs) for designing trustworthy ML systems in healthcare. The literature review helps us to gather knowledge relevant to our problem, identify the research gap, and derive our kernel theory (Gregor and Hevner 2013). The concept of ML trustworthiness remains debated in research and practice. To address this, TAI frameworks and guidelines have emerged to advance ML technology (Thiebes et al. 2020). However, there is a significant gap in fully exploring the core TAI principles, namely beneficence, non-maleficence, autonomy, justice, and explicability (H. Liu et al. 2022; Thiebes et al. 2020). Applying these frameworks to end users is uncertain. Thus, our study is based on the TAI framework (Thiebes et al. 2020), which introduces TAI as an emerging goal. Thus, we decided to utilize the TAI principles as our kernel theory for several reasons: 1) It drew on a data-driven perspective, 2) it is based on the idea of building trust in automation technologies, and 3) the framework based on established trust theories (Mayer et al. 1995; McKnight et al. 2002, 2011).

In the first design cycle, we developed the MRs for a trustworthy ML system based on the TAI principles. We conducted two video conferencing focus groups with a total of 8 potential app end users, lasting approximately 55 minutes each, to assess the MRs' suitability and relevance. The participants were 26 years old on average and were 50% male and female. As our objective was to assess MRs with end users, we selected participants who were already engaged with healthcare applications and had experience with ML systems. As there was limited existing knowledge regarding the design of such ML systems, focus group discussions were deemed appropriate at an early stage of the DSR study (Tremblay et al. 2010). These discussions allowed for direct interactions

between end users, leading to the identification of specific MRs and needs. One author moderated the discussions with an initial introduction to the context of self-examination apps. We asked the participants about their expectations for the design of trustworthy ML systems and which features are important to them. Then, each MR was discussed. Following the open coding guidelines of Miles et al. (2019), two researchers separately coded the transcripts, categorized the emerging needs of the end users, and searched for supporting or contrasting arguments. All in all, the participants confirmed the MR1 - MR8 as important for the design of a trustworthy ML system. Generally, the focus group provided insights into what is important to them and how to promote trust, such as ensuring that they receive information about what the recommendation-for-action is. We took these comments into account when developing the DPs. In the second design cycle, we developed the socio-technical artifact, the DPs for ML systems, and an instantiation in the form of mockups. Based on the kernel theory and MRs, we formulate the DPs according to the recommendation of Gregor et al. (2020). We then identified a suitable use case in the healthcare domain. The objective was to enable the end user to independently use the ML system, enabling patients to regularly monitor their own health conditions. A second criterion for selecting the use case involved choosing an ML system that uses image recognition and employs a classification algorithm for disease identification. The third criterion was the identification of a disease whose early detection is crucial for effective treatment. Consequently, we opted for the recognition of skin diseases. To design the mockups, we first analyzed existing ML systems for self-examined skin screening to develop a fundamental understanding of their functionality. We examined the skin screening applications and their design features listed in Table 9.

Table 9. ML systems for self-examined skin screening

Apps / Features	Instructions	Information: Purpose	States limitations	Data privacy; Limitation of data	Deletion of data	Verification by a physician	Appointment with physicians	Transfer results to physicians	Information about ML decision-	Error communication	Information about accuracy	Explainability of results	Recommendation for action
SkinScreener	✓	✓	✓	-	-	-	-	-	-	-	-	✓	✓
SkinVision	✓	✓	-	-	-	-	-	-	✓	-	-	✓	✓
AIDermatologist	✓	✓	-	-	-	-	-	-	✓	-	-	-	✓
Scanoma	✓	-	-	✓	-	-	-	✓	-	-	✓	-	✓

For the design of the mockups, we utilized the interface design tool Figma to create a realistic representation of a skin screening application (Figma 2023). The final step in this second cycle was the evaluation of the instantiation of the DPs in the form of mockups. We used an anonymous online survey to evaluate the DPs with N2=40 end users. We inquired

about the participant's perception of the helpfulness of the DPs and mockups (McKnight et al. 2002) as well as their assessment of the ease of use of these components (Davis 1989). One approach involved requesting the participants to evaluate the variables using a 7-point Likert scale, while the other method involved soliciting their subjective opinions through a text input field. The participants of the survey were potential end users of ML systems, on average 32 years old and 50% male and female. All of the DPs were considered essential (mean values >=4.80 on a scale from 1="not at all" to 7="extremely"), and none of the participants expressed concerns about the development of a particular DP. Furthermore, we also adjusted the mockups based on the online survey feedback for the effectiveness test. In general, the initial DPs that were derived from the MRs based on the focus group discussions could be confirmed by the survey as our final set of 13 DPs. In the third design cycle, we tested the effectiveness of our DPs and of the instantiation in the form of mockups in an online survey with N3=80 end users. Thereby, we referred to measures derived from the identified justificatory knowledge measure to what extent the trust changes in the designed ML system.

5.4 Results: Deriving Meta-Requirements and Design Principles

In the following, we present the MRs based on the related literature and kernel theory (TAI principles). Then, we present the derived DPs. (Thiebes et al. 2020) introduced the concept of TAI by arguing that the full potential of AI will only be realized if trust can be established in its development, deployment, and use. We deem the TAI principles appropriate in our study since ML is a subcategory of AI (Berente et al. 2021). The TAI principles are characterized by: 1) Beneficence, 2) non-maleficence, 3) autonomy, 4) justice, and 5) explicability. These five principles are related to the trust in technology and automation beliefs mentioned in the theoretical background. The imperative for trustworthy ML systems becomes undeniable when they are applied in the context of human health. Based on the related literature and the TAI principles, we derived eight MRs for trustworthy ML systems in healthcare that frame our design theory (Gregor and Hevner 2013). In addition, by formulating the MRs into concrete design recommendations, we derived 13 DPs (see Table 10) that ensure the development of a trustworthy ML system for end users.

Beneficence refers to the development, deployment, and use of ML that is beneficial to humanity by acting in the end user's best interest, trying to help or achieve certain benefits (McKnight et al. 2002; Thiebes et al. 2020). This principle refers to the two trusting

beliefs, helpfulness, and purpose (Thiebes et al. 2020). Extant research shows that these trusting beliefs are essential indicators for measuring trust in technologies (McKnight et al. 2011; Renner et al. 2021). The content provided by ML systems influences end users' perceived information quality. In particular, end user's trust in ML systems relies on the systems' ability to provide precise, up-to-date, comprehensive, and relevant information that aids the end user's objectives and supports its task (Kim et al. 2021; Yen and Chiang 2021). Consequently, ML systems in healthcare should provide adequate and responsive help to end users (MR1). In summary, to meet MR1, we derived our first DP (DP1) (see Table 10, summarizing the final set of derived DPs), which refers to leveraging trust in the ML system in healthcare by providing guidance and appropriate help to end users. This principle may be instantiated by the provision of short explanations in the form of instructions and advice to the end user. In line with the trusting belief purpose, trust in ML systems can be increased by providing the user information about its purpose, i.e., the goals it was designed to achieve (Lee and See 2004). Therefore, it is important to clearly communicate the purpose of ML systems in healthcare (MR2) (Amershi et al. 2019). According to Yen and Chiang (2021), end users interacting with ML systems expect informative conversations while minimizing the occurrence of irrelevant information. Conclusively, we derived the DP2a and DP2b. These two principles aim to increase trust in the ML system by providing information about the functionalities and limitations of the system. DP2a and DP2b may be instantiated by giving examples of how to use the ML system and how not to use it. Non-maleficence refers to the development, deployment, and use of ML in a way that avoids bringing harm to people by particularly protecting people's privacy (Thiebes et al. 2020). It relates to the trusting beliefs reliability and process. Advances in digitization have shifted the emphasis from the intuition-based expertise of a human expert to a more data-driven approach to decision-making (Berg 1997; Lebovitz et al. 2021). A large amount of data is essential for ML systems to derive patterns and make predictions about a certain problem (Duan et al. 2019). An ML system should aim to transmit data confidentially, integrally, and authentically to reduce concerns and comply with privacy protection regulations. If the ML system has mechanisms in place to protect personal information such as identity, location, and device data and ensure only authorized end users have access, it is more likely to be trusted (Robinson 2020). Thus, ML developers should enable end users to have control over their data in ML systems (Sheridan 2019). In summary, our third MR for ML systems in healthcare is to address end users' privacy concerns by implementing suitable measures for safeguarding their personal

data (MR3). This results in DP3a and DP3b, which aim to protect the privacy of users. According to DP3a, the collection of data from the end user is kept to a minimum by collecting only the data that is actually needed for the health analysis. In addition, technical measures ensure that no information is disclosed to unauthorized parties. DP3b refers to leveraging trust in the ML system in healthcare by giving users control over their data (e.g., allowing them to permanently delete their data). Autonomy advocates for the promotion of human autonomy, agency, and control, which may include limiting the autonomy of ML systems when necessary (Thiebes et al. 2020). Due to ethical and legal aspects, ML systems are currently developed to support end users rather than to replace human experts (Roshanov et al. 2013; Takiddin et al. 2021). In contexts where tasks are primarily performed by human experts, end users usually expect humans to be in the decision loop (Yang and Wibowo 2022). This expectation stems from the direct impact these tasks may have on high-risk domains. Because ML systems lack physical appearance and have a high level of autonomy without human intervention, end user trust may be diminished. The inclusion of a human expert provides a critical layer of oversight, which helps to ensure that the decisions supported by ML systems are accurate and reliable (Faraj et al. 2018). Thus, ML systems in high-risk domains that include proper oversight mechanisms, such as involving a human expert in the final decision-making process (i.e., keeping "human-in-the-loop"), are generally considered more reliable and trustworthy than those that do not. In addition, the involvement of a human expert can help to address questions that end users may have regarding. Therefore, it should be possible for a human expert to intervene in the decision-making process of ML systems in healthcare, if necessary (MR4). To satisfy the fourth MR, the DP4a, DP4b, and DP4c should be followed. According to these DPs, a human expert (i.e., a physician) should be involved in the health analysis. In particular, DP4a aims to enhance trust by incorporating a human expert to review and, if necessary, rectify the results of the ML system. Furthermore, DP4b enables the user to directly schedule a consultation with a human expert. DP4c aims to enable the ML system's results to be promptly conveyed to a human expert. Justice describes the utilization of ML to amend past inequities, the creation of shareable and subsequent distribution of benefits through ML, and thwarting the creation of new harms and inequities by ML. It relates to the trusting beliefs reliability and process (Thiebes et al. 2020). Biases in the data used for training ML systems can cause algorithms to have disparate impacts on the results for disadvantaged groups (Teodorescu et al. 2021). Thus, it is essential that trustworthy ML systems in healthcare avoid providing biased or

discriminating information by enhancing the diversity of the data sets and including multiple groups and conditions in algorithmic development (MR5). Therefore, we have derived our fifth DP. DP5 mandates the provision of information regarding the operation of the ML system's algorithm to end users. System reliability, accessibility, and timeliness of functional features are crucial factors for assessing the quality of an ML system (Bedué and Fritzsche 2022; Yang and Wibowo 2022). Thus, an ML system is perceived as trustworthy when it is easily accessible and free from errors such as miscalculations, inaccuracies, misinterpretations, over- or underestimations (Kim and Peterson 2017). Consequently, ML systems in healthcare should be able to detect and correct system errors and inaccuracies (MR6). This results in the sixth DP. DP6 aims to increase trust by automatically notifying end users of system errors. DP6 also relates to DP1. Thus, an ML system's trustworthiness is determined by its reliability (i.e., the ML systems exhibit the same and expected behavior over time) (Hoff and Bashir 2015) and accuracy. Thus, MR7 aims to maximize the reliability of ML systems in healthcare by achieving a high level of accuracy in performing specific tasks or functions. To meet our seventh MR, we derived the DP7. According to DP7, system errors will be sent directly to the support service to ensure and improve functionality. Explicability refers to the development, deployment, and use of explainable ML by producing interpretable ML models whilst maintaining high levels of performance and accuracy (Thiebes et al. 2020). This principle relates to the trusting beliefs functionality and performance. With the increasing complexity and non-deterministic nature of ML models and the potential impact of their decision process, the necessity for transparent and explainable models has grown increasingly important. Transparency in ML algorithms and the capacity to offer clear explanations for ML-generated results are pivotal factors affecting end user trust in ML predictions (Glikson and Woolley 2020). In particular, increased transparency and explainability can positively influence end user's trust in adhering to the advice provided by the ML system (Ebrahimi and Hassanein 2019; Glikson and Woolley 2020; Strich et al. 2021) because it enables end users to reliably judge process characteristics of the ML system (Lee et al. 2019). Finally, our eighth MR refers to maximize the transparency and explainability of ML systems in healthcare (MR8). Thus, we have derived our DP8a and DP8b. By providing users with information that helps them understand the results of the ML system, DP8a aims to increase the transparency of the results and trust in the ML system. According to DP8b, users should receive appropriate recommendations for action.

Table 10. Description of DP

TAI		Description of DP
To increase trust in ML systems in healthcare, developers need to implement measures to ensure that...		
Beneficence	MR1	…the ML system provides end users with brief explanations that can be easily understood without prior domain and technical knowledge in the form of instructions and advice on how to use the ML system correctly. (DP1)
	MR2	…the purpose of use is clearly stated, and end users are informed about how and for what the results of the ML system can be used. (DP2a)
		…the limitations of the ML system are presented to the end users. (DP2b)
Non-maleficence	MR3	…only the necessary end user data is collected in compliance with relevant data protection regulations, and such data is safeguarded by robust technical measures. (DP3a)
		…end users are given control over their data, for example, by allowing them to permanently delete their data. (DP3b)
Autonomy	MR4	…the result of the ML system is verified by a human expert and corrected if necessary. (DP4a)
		…for critical results, it is possible to arrange a prompt appointment with a human expert directly via the system. (DP4b)
		…the ML system's result can (optionally) be sent to a human expert for documentation and potential follow-up actions. (DP4c)
Justice	MR5	…the proposed system aims to provide end users with information about how the ML algorithms work and the data on which the algorithm is based. (DP5)
	MR6	... if there is a system error that causes improper functioning of the ML system, an automatic notification is sent to the end user, and the corresponding error code will be automatically transmitted to the support service. (DP6)
	MR7	…if there is a system error that causes the ML system not to work properly, provide the end user with a notification, and the corresponding error code is relayed to the support service. (DP7)
Explicability	MR8	…the result of the ML system and its interpretation are provided in an appropriate information density and quality so that they are comprehensible for end users without prior domain and technical knowledge. (DP8a)
		…end users receive appropriate and understandable recommendations for action in the case of both negative and positive results, considering factual communication of the results. (DP8b)

5.5 Principles Effectiveness of the Trustworthy Machine Learning System

We conducted a scenario-based online survey to evaluate our socio-technical artifact, comprising the DPs for ML systems, by utilizing instantiated mockups. The objective of this survey was to investigate the efficacy of our DPs in fostering trust in ML systems. We followed established guidelines in IS to design our online survey (Lowry et al. 2016).

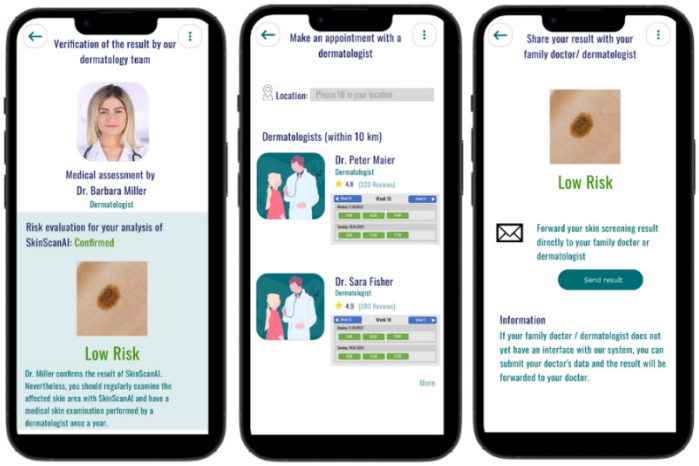

Figure 7. Examples of mockups (DP4a-4c)

Design of Effectiveness Test: We tested the same scenario in two different groups, the control and the treatment group. We adhered to the procedures outlined by Mettler et al. (2014) for carrying out controlled experiments aimed at assessing designs. We then juxtaposed SkinScanAI, which was constructed based on DPs aligned with the TAI principles (see Table 10), with a variant of the mockups devoid of any trust elements. The stimulus (i.e., the new and improved design) is presented exclusively to the treatment group, while the control group remains unexposed. Therefore, we developed mockups for an ML system, applying our context of the skin screening process identified in the second design cycle. We present a basic skin screening process representing the control group. For the treatment group, we designed mockups based on the DPs. To prevent the priming of participants, we chose a between-subject study design in which participants were randomly assigned to one of the two groups (i.e., control or treatment group). Specifically, the goal is to scan a skin lesion with a mobile phone camera using the fictional ML system, namely SkinScanAI. In Table 11, we present the descriptions of the mockups for the control group and the treatment group. In addition, we present in Figure 7 examples of the mockups representing DP4a-DP4c.

Table 11. Descriptions of mockups

Control Group	Treatment Group
MU1: The end user must first register to create their own profile. To do so, he/she must enter his/her name, gender, and email address.	DP3a, DP3b: Specifies that SkinScanAI collects the end user's age and gender. Optionally, the end user can also add information about their family doctor. In addition, the app provides information about its privacy mechanisms, which are compliant with current data privacy regulations. To give end users control, SkinScanAI also includes a feature to permanently delete their data.

MU2: Presents the necessary requirements for the use of SkinScanAI.	DP2a, DP2b: Presents the purpose, necessary requirements, and limitations for use.
MU3: Demonstrates the skin scan process by taking a photo of the lesion. Provides the end user with information on how to focus on the lesion.	DP1: Demonstrates the photo-taking process with clear instructions on how to take a photo of the lesion. SkinScanAI automatically provides feedback to the end user on whether the lesion is in focus, recognizable, and whether the lesion has been successfully detected.
MU4: The end user receives an exemplary result that includes an image of the lesion and the risk assessment (i.e., "Our algorithm did not detect a problematic skin lesion").	DP7, DP8a, DP8b: The end user receives a result that illustrates three risk assessment scenarios (i.e., low, medium, and high risk) and includes an image with the framed lesion. For each risk assessment, the end user is provided with an easy-to-understand explanation of how to interpret the result and the recommended course of action.
-	DP4a, DP4b, DP4c: Three mockups provide (1) additional verification of the risk assessment by physicians, (2) the option to share the result directly with the family doctor or dermatologist, and (3) the feature to schedule an appointment with a local dermatologist (i.e., online booking).
-	DP5: Provides information about how the SkinScanAI algorithm works, its average accuracy, and the database used to train the algorithm.
MU5: Provides information that if a system error occurs while using SkinScanAI, the end user can email the information to the support team.	DP6: Displays a message informing the end user that in the event of a system error, a message containing information about the error will be automatically sent to the SkinScanAI provider and that they should restart the skin screening process.

Questionnaire: The online survey includes a scenario, demographic questions, and a representative scale for the target variable, trust in technology, that was slightly adapted to fit the context. Furthermore, an attention check was implemented in the survey to detect inattentive participants. Before presenting the mockups and questions to the participants, we asked them to imagine that they would like to examine a specific skin lesion (e.g., moles) using the ML system SkinScanAI. Then, the participants were guided through each step of the skin screening process by showing them mockups and particular functions. Afterwards, the participants were asked to assess trust in SkinScanAI consisting of the three dimensions: functionality, reliability, and helpfulness. To measure trust, we refer to our kernel theory from the literature (Iivari 2020) and lean on the established scale by McKnight et al. (2011) (see Table 12).

Table 12. Constructs and items

Constructs	**Items** (7-point Likert scale, 1=strongly disagree, 7=strongly agree)
Functionality	SkinScanAI has the functionality I need; SkinScanAI has the features required for my tasks; SkinScanAI has the ability to do what I want it to do.

Reliability	SkinScanAI is a very reliable piece of software; SkinScanAI does not fail me; SkinScanAI is extremely dependable; SkinScanAI does not malfunction for me.
Helpfulness	SkinScanAI supplies my need for help through a help function; SkinScanAI provides competent guidance through a help function; SkinScanAI provides whatever help I need; SkinScanAI provides very sensible and effective advice if needed.

Data Analysis: Overall, we collected N3=80 participants by using the established online platform Prolific (Palan and Schitter 2018), of which 40 participants were assigned to each of the two groups. The participants were evenly distributed between males (50%) and females (50%). On average, the participants were 31.5 years old, while most of them (68.8%) were between 18-33 years old. The gathered data was analyzed by using the statistical software SPSS 27. As our data for trust, including functionality, reliability, and helpfulness, was not distributed normally (Shaphiro and Wilk 1965), we applied the two-step approach for transforming the trust variables to normal distribution. First, we calculated the fractional rank of the variables, resulting in uniformly distributed probabilities, and applied an inverse-normal transformation to form a variable of normally distributed z-scores (Templeton 2011). After applying these two-steps approach, the Shapiro-Wilk test revealed that the trust variables, including functionality, reliability, and helpfulness, are normally distributed since the significances were higher than 0.05 ($p > 0.05$). In addition, the Levene's test indicated that the variances for the constructs were statistically equal, which confirms variance homogeneity. Then, we applied a t-test and could indeed confirm that the mean values in the treatment group were significantly different at the 1% significance level ($p<0.001$) (see Table 13). Thus, end users perceive the trustworthy DPs higher compared to the control group. In addition, the effect sizes were measured by using Cohen's d, and the results confirmed large effect sizes (Cohen 1988). In conclusion, the results of our evaluation showed that the ML system based on the derived DPs received higher trust than the one based on a basic ML skin screening process.

Table 13. Results of t-test

	Control Group		**Treatment Group**		**Results t-test**		
Trust Dimensions	Mean	Stddev	Mean	Stddev	t-statistics	p-value	Cohens's d
Functionality	4.613	1.458	5.775	0.824	-4.560	0.000	-1.020
Reliability	4.144	1.329	5.112	0.749	-4.322	0.000	-0.973
Helpfulness	4.525	1.435	5.775	0.711	-4.818	0.000	-1.067

5.6 Discussion

We developed 13 DPs with the goal of ensuring a user-centered and trustworthy design for ML systems through three design cycles. Prior to the initiation of the design process, we

conducted a literature review to identify problems of trusting ML systems. By using the TAI principles as the kernel theory, we derived MRs for trustworthy ML systems. The DPs were refined through focus group discussions and an online survey. The final effectiveness test confirmed that established DPs indeed increase trust in ML systems.

DP1: Delivering precise and succinct instructions is fundamental to guarantee that end users acquire a thorough understanding of the appropriate utilization of ML systems. In healthcare, the incorrect use of these systems can lead to false diagnoses or other adverse outcomes for end users that may impact individuals' lives. Hence, it is crucial to ensure that end users understand how to use these systems correctly. DP2a and DP2b acknowledge the limitations and purpose of ML systems, aiding end users in avoiding excessive reliance on the system's outcomes, which can lead to incorrect decisions and misguided conclusions. In this way, end users can avoid making incorrect usage decisions and drawing false conclusions. These DPs are in line with previous literature, which stated that it should be clear what the system can do (Amershi et al. 2019). DP3a, protecting end users' data and ensuring regulatory compliance is essential in healthcare due to the sensitive nature of patient data. Establishing trust by preserving the privacy of end users is pivotal for the widespread adoption and continuous use of ML systems. In addition, DP3b is about giving end users control over their data by allowing them to choose whether or not to share their personal information with the healthcare provider. More importantly, end users request a technical feature to delete their data. Thus, these DPs increase trust and are designed to mitigate problem P4. In addition, previous research has shown that the implementation of privacy-preserving mechanisms can increase end user trust in technology (Bansal et al. 2015). DP4a, DP4b, and DP4c involve human experts in the decision-making process due to the complexity and non-deterministic nature of ML systems, as this is important to end users due to the barriers to ML adoption, namely inscrutability (P1) and inaccurate predictions (P2). Especially in high-risk domains such as healthcare, providing an additional source of trust for ML systems is crucial, as inaccurate results could have negative consequences for end users. Therefore, ML systems in healthcare are currently developed primarily to support medical diagnosis and cannot replace human experts (Takiddin et al. 2021). Our findings align with earlier studies, which have demonstrated that collaborative work between humans and machines can yield superior outcomes (e.g., Sturm et al. 2021). Thus, these DPs could mitigate the problems P1 and P2. DP5, raising awareness among end users about the functioning of ML algorithms is crucial to increase transparency, as it is key to building trust in ML systems

and thus mitigating problem P1 (Adadi and Berrada 2018). End users can make more informed decisions regarding the suitability of an ML system for their needs, as well as whether to depend on its outputs when they possess a thorough understanding of the system's inner workings and the underlying data. For example, if an ML system is developed using training data from middle-aged people, it may not be suitable for analyzing health conditions of senior citizens. DP6 informs end users of system errors and provides support services. This information helps to build trust and ensure that end users can rely on the ML system. Especially in the healthcare context, providing direct support to end users when needed is important to avoid negative attitudes about system performance (e.g., Emamjome and Rosemann 2021b). DP7 informs end users about the interpretation of the accuracy because the trajectory of trust in ML systems has mostly focused on the way trust in ML changes based on the feedback regarding its accuracy (Glikson and Woolley 2020). In addition, it is more important than informing end users about isolated metrics (Lebovitz et al. 2021; Pumplun et al. 2023). In healthcare, providing information on how to interpret the accuracy helps end users understand and interpret the output of the ML system, thereby mitigating P3 and increasing trust. DP8a and DP8b ensure that end users can understand and respond to the output of the ML system without the need for domain knowledge (i.e., medical expertise). This holds significance due to the elevated autonomy of ML systems. Incorporating these DPs can effectively mitigate uncertainties, thereby fostering enhanced end user confidence in adhering to the advice provided by ML systems (e.g., scheduling a medical appointment) (Ebrahimi and Hassanein 2019; Strich et al. 2021). These DPs aim to mitigate P1. Ensuring that end users understand the output accordingly can help prevent incorrect conclusions that may have harmful effects on end users. Due to this issue, Pumplun et al. (2023) designed an ML clinical decision support system with additional explanation features for physicians. In summary, adherence to all these principles can ensure a user-centered development of ML systems guided by TAI principles, ultimately leading to increased end users' trust in ML systems.

5.6.1 Theoretical Contributions

Our theoretical contribution is threefold. First, we respond to the recent calls for research (e.g., Riedl 2022) to examine and develop trustworthy ML systems. Many studies focus on the technical implementation of ML systems, for instance, developing performance measures (e.g., accuracy, robustness) (e.g., Tofangchi et al. 2017). However, factors increasing trust in ML systems go beyond these algorithmic model characteristics because

trust in the ML context is of great importance (see chapter, ”Trust in Machine Learning Systems”). In addition, previous research on trust in ML systems mainly employed empirical methods to describe end user behavior (Renner et al. 2021). Thus, current studies still lack a deep understanding of trust in ML systems, particularly on how to design these systems to increase trust (Li and Hahn 2022; Riedl 2022). By deriving and evaluating concrete DPs for trustworthy ML systems, we contribute to the theory of how end users' trust in ML systems can be achieved by design. This is particularly important to expand current trust research on trust antecedences (e.g., Glikson and Woolley 2020). The DPs provide appropriate rationales for the underlying mechanisms, helping researchers to understand the development of end users' trust in ML systems. Thus, our results deepen and expand the understanding of trust in ML systems by particularly providing guidelines on how to derive trust in ML systems. Second, our research expands the trust literature stream by developing DPs for ML systems. By developing these DPs, we were able to specify the overarching TAI principles, thus guiding future research. It is worth highlighting that the end user placed significant emphasis on acknowledging the decisive role of human experts during the design process due to the uniqueness of trust in ML systems. Consequently, the design incorporates a human-in-the-loop approach to ensure effective decision-making and optimize outcomes. This is an important finding for IS research to understand whether or under what conditions ML systems will fully automate or augment human work processes. Third, previous research has mostly focused on ML systems in an organizational context (e.g., Lebovitz et al. 2021; Pumplun et al. 2023) rather than from the individual perspective of non-specialist end users (i.e., users without medical expertise). Our research is unique due to the design of a user-centered ML system. In doing so, we involved potential end users in all three design cycles, which means that we considered the perspective and needs of end users. This is important because end users are the target group for these systems and will be interacting with the ML system. Thus, we create a social-technical artifact in the form of DPs and an instantiation in the form of mockups that meet the needs of its intended audience.

5.6.2 Practical Contributions

We contribute to practice by, first, providing a social-technical artifact in the form of DPs, which can serve as practical guidance for developers and researchers to develop trustworthy ML systems. We instantiate the DPs by mockups not only to illustrate the crucial DPs for end users but also to demonstrate how these principles can be put into

practice. By doing so, we are addressing key challenges in the development of ML systems, such as the lack of transparency, the involvement of humans in the decision-making process, and the infrequent use of ML systems by end users. As a result, the potential of ML in the healthcare domain can be better leveraged. This contribution is highly relevant to society and could help to increase ML system adoption. Second, the increasing pressure on the healthcare sector can be relieved by involving end users in the diagnostic process and supporting them with self-examination tools as the first point of medical contact. Even if these systems cannot replace human physicians due to legal, ethical, and validation reasons (Roshanov et al. 2013), physicians' workload can be reduced by providing end users with the availability of self-examination tools at home. By involving end users in the diagnostic process, ML systems in healthcare have the potential to reduce the number of physicians' appointments, which in turn can help to ease the burden on the healthcare sector. Moreover, ML systems can also empower end users to take control of their health and well-being, as they can monitor their symptoms and keep track of their health data in a convenient and accessible manner. Finally, we can assist healthcare providers by demonstrating DPs to increase trust in ML systems that can promote continuous use. End users are more likely to use ML systems continuously if they perceive them as trustworthy and effective (Glikson and Woolley 2020). Through the promotion of user-centered design, healthcare providers can improve the end user's experience and create a sense of trust in the ML systems. In addition, the continued use of ML systems can lead to the collection of more accurate and comprehensive health data, consequently resulting in improved diagnosis and treatment outcomes. Thus, the results of our study can ultimately benefit both end users and healthcare providers by improving health outcomes and promoting more efficient and trustworthy ML systems.

5.7 Limitations, Future Research, and Conclusion

Overall, our research aims to address the problem of an overburdened healthcare sector by developing an ML system that prioritizes the needs and preferences and engages the end user in the diagnosis process of diseases. We recognized that end users may not trust these systems due to issues such as inscrutability, biases and discrimination, prediction inaccuracy, and privacy concerns. To address these challenges, we focused on designing a trustworthy ML system that increases trust. We applied a DSR approach and used the TAI principles as our kernel theory to develop a socio-technical artifact consisting of DPs and instantiation mockups in three design cycles. Our final evaluation test demonstrated the

effectiveness of our DPs in increasing end user trust in ML systems. Our research provides important insights into the design of trustworthy ML systems and contributes to the growing body of knowledge on the development of systems in high-risk domains such as healthcare.

Our study also has limitations. First, the proposed DPs have not been technically implemented in a prototype. While the mockups provide a visualization of the DPs, the implementation feasibility remains unclear. Future research could focus on developing a prototype based on the proposed DPs, the instantiation in the form of mockups, and evaluating the technical feasibility. This would involve the ability to provide transparent explanations of their decision-making processes. It would also require addressing any technical challenges that arise during the implementation process, such as issues related to data privacy, system integration, and end user experience. By conducting such research, we could gain a better understanding of the implications of implementing ML systems and other high-risk domains. Future research could concentrate on empirical research of end user acceptance of the DPs using a prototype of the ML system. Thus, it could lead to valuable insight into the differences between DPs, for instance, related to autonomy or transparency. In addition, further research could explore the impact of individual differences and integrate personality traits (e.g., Big Five) and user characteristics, as these may impact the end user acceptance of ML systems (Riedl 2022). Second, the DPs are based on a broader range of literature and are not limited to healthcare. They encompass general concepts for building trustworthy technologies, which can be applied to the design of ML systems in other high-risk domains. For example, the principles may be useful in other diagnostic or treatment settings in healthcare, as well as in other high-risk environments like finance. Nonetheless, it's important to replicate this research in other contexts to provide empirical evidence of the principles' transferability to other high-risk domains or to identify any specific needs for each domain. Third, the effectiveness of the final set of DPs was evaluated in the specific context of a skin screening process. Future research could assess these DPs in varied scenarios for broader result generalizability. While our study aimed to evaluate DPs' impact on enhancing end user trust, we must acknowledge a limitation in our approach. We opted to use McKnight et al.'s (2011) established trust measurement scale due to its wide applicability. However, this choice led to the challenge of not being able to individually evaluate the impact of each DP on trust. To address this limitation and offer a more nuanced understanding, future research endeavors should focus on conducting separate evaluations for each DP. This could entail a

variety of methodologies, including online surveys to gauge user perceptions, as well as interactive sessions involving end users, such as focus group discussions or interviews.

Acknowledgments

Funded by the German Research Foundation – 251805230/GRK 2050.

6 Paper D: Machine Learning Adoption based on the TOE Framework: A Quantitative Study

Title

Machine Learning Adoption based on the TOE Framework: A Quantitative Study

Authors

Anne Zöll, Verena Eitle, Peter Buxmann

Publication Outlet

Pacific Asia Conference on Information Systems

Abstract

The increasing use of machine learning (ML) in businesses is ubiquitous in research and in practice. Even though ML has become one of the key technologies in recent years, organizations have difficulties adopting ML applications. Implementing ML is a challenging task for organizations due to its new programming paradigm and the significant organizational changes. In order to increase the adoption rate of ML, our study seeks to examine which generic and specific factors of the technological-organizational-environmental (TOE) framework leverage ML adoption. We validate the impact of these factors on ML adoption through a quantitative research design. Our study contributes to research by extending the TOE framework by adding ML specifications and demonstrating a moderator effect of firm size on the relationship between technology competence and ML adoption.

Keywords

Adoption, Machine Learning, TOE Framework

6.1 Introduction

Machine learning (ML) has been considered a megatrend for the past several years (Goasduff 2020) as its alternative programming paradigm allows information systems (IS) to derive their functionality from data rather than requiring humans to explicitly translate their solution into code (Samuel 1959). Through this paradigm shift, organizations experience a major change in the way algorithms are developed. In addition, the increasing prediction performance also contributes to ML being perceived as a megatrend. Besides the enormous improvements in computer power and low storage costs, organizations are constantly collecting more data through applications and sensors. As these growing data sets serve as training sets, ML algorithms can achieve higher prediction accuracy (Bean 2018). As the volume and velocity of data available through cloud services enable ML algorithms to outperform manual decision-making (Brynjolfsson et al. 2017), ML can be used to drive timely data-driven business decisions.

The emergence of ML algorithms has an immediate impact on IS in organizations and their business processes. In general, it is estimated that the global GDP will increase by 14% until 2030 through the use of ML (PWC 2017a). By implementing ML, organizations have the opportunity to generate new business values and disrupt their business models (Kruse et al. 2019). For instance, organizations can leverage ML to turn their data into value (Jöhnk et al. 2021), develop new products and services (Davenport 2018; Ransbotham et al. 2019), improve their organizational efficiency through data-driven decision-making (Brynjolfsson et al. 2011) and analyze data from sensors (Brynjolfsson et al. 2017). All in all, ML is one of the most promising innovations in the digital age which helps organizations to stay competitive (Dremel et al. 2020; May et al. 2020; Seddon et al. 2017).

Despite the wide-ranging benefits of ML, the overarching adoption rate in organizations is relatively low (Alsheiabni et al. 2019) as many ML initiatives fail (Ransbotham et al. 2019). The US Census Bureau states that only 2.8 percent of organizations have adopted ML (Zolas et al. 2020, p. 47). Since the low adoption rate is an indicator that the ML adoption is challenging for organizations (Afiouni 2019; Kruse et al. 2019; Zhang et al. 2020), we seek to examine which generic and specific factors influence ML adoption at the organizational level by using the technological-organizational-environmental (TOE) framework by Tornatzky and Fleischer (1990). According to the findings of previous studies on innovation adoption, organizations could leverage the known generic factors

such as relative advantage, complexity, and top management involvement to increase the adoption rate of ML (e.g., Chong and Chan 2012; Gutierrez et al. 2015; Xu et al. 2017). Since so far it remains unclear which of these generic factors primarily promote ML adoption at the organizational level, our study seeks to provide insights into these generic components. Since ML implementations differ from other technologies in terms of the new programming paradigm (Samuel 1959), specific factors need to be considered in addition to the generic factors. For instance, transparency is an intensively discussed topic in the context of ML as the decision-making process changes significantly due to the incorporation of ML applications (Rzepka and Berger 2018). In addition, successful ML implementations may also depend on compliance regulations such as data protection which allows organizations to avoid any a kind of misuse of personal data (Pumplun et al. 2019). Given the importance of transparency and data protection in the context of ML, we seek to expand the TOE framework by adding these two ML specifications. Previous research, however, lacks insights into the impact of transparency and data protection on ML adoption. Since so far only qualitative studies set the theoretical foundation of ML adoption (Eitle and Buxmann 2020; Jöhnk et al. 2021; Kruse et al. 2019; Pumplun et al. 2019), we believe there is an urgent need to follow the suggestions of Pumplun et al. (2019) and Jöhnk et al. (2021) to validate these influencing factors on ML adoption using a quantitatively research design. Hence, we seek to answer the following research question:

RQ: Which generic and specific factors of the technological-organizational-environmental framework leverage ML adoption?

Based on the TOE framework by Tornatzky and Fleischer (1990), we recruited 250 data scientists to analyze the influencing factors of ML adoption. We contribute to research by shedding light into the generic technological, organizational, and environmental factors that have an impact on ML adoption. Due to the intense discussions regarding ML specifications, our study expands the TOE framework by the specific factors of transparency and data protection. In addition, we provide valuable insights into the inconsistent results on the influence of firm size by adding a moderator effect. By following a quantitative research design, we validate the findings of qualitative studies on ML adoption and provide quantitative evidence.

6.1.1 ML Specifications

A common definition of ML states that "a computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E" (Mitchell 1997, p. 2). In other words, ML algorithms generalize their own experiences in a way that allows them to increase their performance with respect to a particular task. Experience is represented by historical data instead of explicit rules (McCarthy 2007) which enable ML algorithms to learn (Harfouche et al. 2017). Due to the capability of self-learning, the way of programming is undergoing a massive change, fueled by continuous performance improvements of ML algorithms.

ML has penetrated several business areas including healthcare (Bjarnadóttir and Anderson 2020; Hofmann et al. 2020), finance (Kruse et al. 2019), automotive (Demlehner and Laumer 2020), and software defect prediction (Rana et al. 2014). This widespread use indicates that ML can be considered a general-purpose technology (Brynjolfsson et al. 2017). While organizations seek to leverage ML to address complex decision-making processes (Knight 2015; Meyer et al. 2014) and to enhance customer experience (Bakis et al. 2017; Davenport 2018), adopting ML across an organization is challenging. Besides technological barriers (e.g., limited technological capabilities) (Jöhnk et al. 2021), organizations also face challenges related to internal organizational structures (e.g., changes in business processes, lack of leadership support, lack of funding) (Alsheiabni et al. 2019). For example, transparency is a heavily discussed topic as the underlying reasoning process of a complex ML application can be difficult to understand and to reconstruct (Rzepka and Berger 2018). Since ML is considered a black box that impedes the understanding and interpretability in decision-making processes (Peters et al. 2020; Rudin 2019), providing transparency could increase the adoption rate of ML (Jöhnk et al. 2021; Kruse et al. 2019; Sidorova and Rafiee 2019). To better understand the challenges of organizations, previous studies have proposed research frameworks to examine ML adoption (Rana et al. 2014), to identify barriers of ML adoption (Alsheiabni et al. 2019), to explore readiness factors for ML applications (Jöhnk et al. 2021; Pumplun et al. 2019), and to investigate the impact of ML on specific industries and business areas(e.g., Kruse et al. 2019; Rana et al. 2014). However, as all these ML adoption studies are based on a qualitative research design, current research lacks quantitative evidence on the influencing factors on ML adoption. Up until now, research remains vague which generic and specific

technological, organizational, environmental factors influence ML adoption and what implications they have on the continued use.

6.2 Theoretical Background

6.2.1 Innovation Adoption and TOE Framework

In IS research, there are several well-established theories that are applied in the study of innovation adoption at the individual or organizational level. In order to examine individual factors that influence innovation adoption decisions, the theory of planned behavior model (TPB) (Ajzen 1985, 1991), the technology acceptance model (TAM) (Davis 1986, 1989; Davis et al. 1989), and the unified theory of acceptance and use of technology model (UTAUT) (Venkatesh et al. 2003) are well known in the IS literature. The most widely used frameworks in the context of innovation adoption at the organizational level refer to the diffusion of innovation framework (DOI) by Rogers (1995) and the TOE framework by Tornatzky and Fleischer (1990). Considering the DOI framework, researchers seek to analyze the impact of technological factors such as relative advantage, compatibility, complexity, trialability, and observability on the diffusion of innovations over time (Rogers 1995). While the technology focus is highly valued, it is argued that despite the high complexity of innovation decisions within organizations, the DOI framework does not include any further factors that might influence the adoption of innovations (Rogers 1995). To overcome this shortcoming, the TOE framework by Tornatzky and Fleischer (1990) takes the technological, organizational, and environmental context into account when examining factors that encourage or hinder organizations in adopting innovations.

Table 14. Innovation adoption studies based on the TOE framework

Literature	Innovation	RA	PC	CM	TR	TM	TC	CP	DP	FS
(Zhu et al. 2003)	E-business						X	X		X
(Zhu et al. 2006)	E-business		X				X	X		X
(Liang et al. 2007)	ERP					X				
(Rai et al. 2009)	Procurement					X				
(Chong and Chan 2012)	RFID	X	X			X	X			X
(Venkatesh and Bala 2012)	Business Process	X	X							
(Borgman et al. 2013)	Cloud Computing	X				X		X		X
(Gutierrez et al. 2015)	Cloud Computing	X	X					X		X
(Martins et al. 2016)	SaaS	X		X		X	X			
(Xu et al. 2017)	ERP	X	X	X				X		
(Pumplun et al. 2019)	AI/ML*	X			X		X	X	X	
(Kruse et al. 2019)	AI/ML*				X		X		X	
(Eitle and Buxmann 2020)	ML	X			X		X	X	X	
(Jöhnk et al. 2021)	AI/ML*				X	X	X		X	

Note: RA – Relative Advantage, PC – Process Compatibility, CM – Complexity, TR – Transparency, TM – Top Management Involvement, TC – Technology Competence, CP – Competitive Pressure, DP – Data Protection, FS – Firm Size

* AI is associated with an "intelligent agent", which "is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through actuators" (Russell 2021, p. 54). ML is a subset of AI and provides systems with the capability of self-learning.

Since innovation adoption is considered an important research field in IS, many studies are devoted to investigating the factors that influence the adoption of innovations. As shown in Table 14, the TOE framework has been widely used in innovation adoption studies in fields such as enterprise-resource planning (ERP) (Junior et al. 2019; Xu et al. 2017), radio frequency identification (RFID) (Chong and Chan 2012), CRM (Cruz-Jesus et al. 2019), e-business (Chandra and Kumar 2018; Zhu et al. 2006), and cloud computing (Borgman et al. 2013; Martins et al. 2016), The study by Zhu et al. (2003) was among the first that applied the TOE framework on innovation adoption. Several other studies have followed using the TOE framework and have analyzed different factors on innovation adoption (Chong and Chan 2012; Fichman 2000; Junior et al. 2019; Martins et al. 2016). Drawing on the TOE framework, the studies listed in Table 14 have examined the impact of technological components such as relative advantage, compatibility and complexity, organizational components such as top management involvement, technology competence, and firm size as well as environmental components such as competitive pressure on adoption rates. With respect to ML adoption, recent qualitative studies by Eitle and Buxmann (2020), Jöhnk et al. (2021), Kruse et al. (2019), and Pumplun et al. (2019) have revealed that the TOE framework should be extended by the specific factors of transparency and data protection.

6.3 Hypotheses

Drawing on the TOE framework by Tornatzky and Fleischer (1990), we present the conceptual research model in Figure 8 and derive the hypotheses for the technological, organizational, and environmental contexts in the following section.

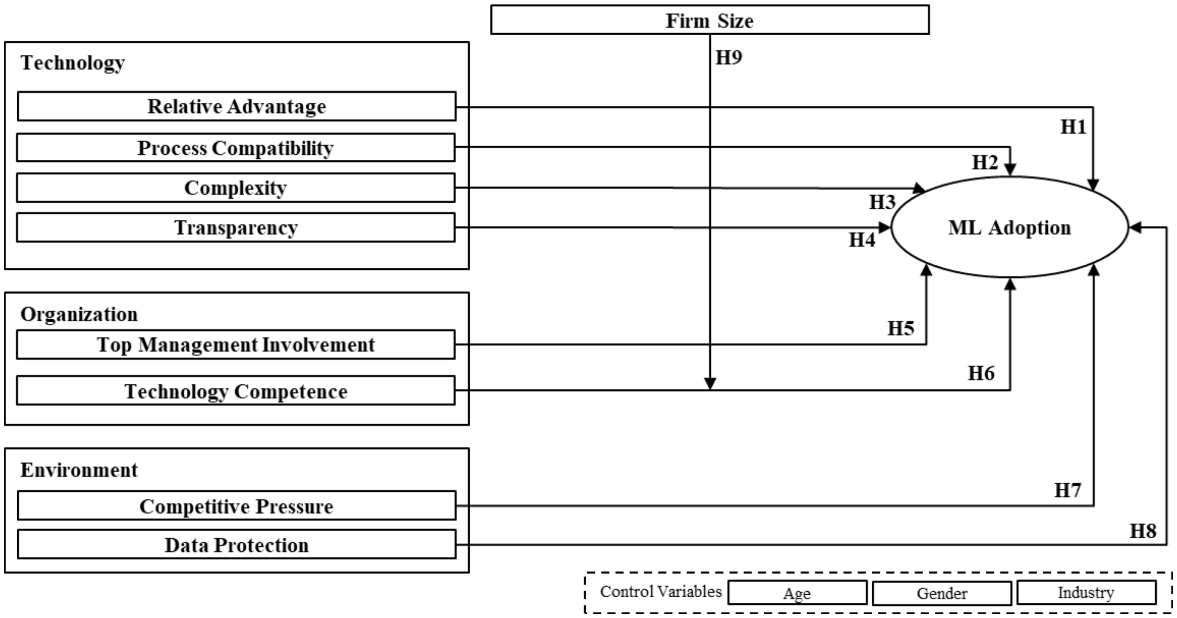

Figure 8. Conceptual research model

The **technological context** of the TOE framework addresses both internal technologies already owned by the organization and external technologies that might be considered for innovation adoption decisions (Tornatzky and Fleischer 1990). Relative advantage is considered an important technological component of innovation adoption as it relates to the perceived benefits of a technology. According to Rogers (1995), relative advantage determines the extent to which an innovation is perceived to be more beneficial to organizations than other technologies. Previous literature on innovation adoption showed that strategic and operational benefits can have a positive impact on the adoption rate of innovation (Borgman et al. 2013; Chong and Chan 2012; Gutierrez et al. 2015; Martins et al. 2016; Venkatesh and Bala 2012; Xu et al. 2017). Furthermore, the qualitative findings of Pumplun et al. (2019) and Eitle and Buxmann (2020) suggested that benefits also need to be emphasized in the context of ML. Implementing ML applications, for example, enables organizations to facilitate decision-making processes (Meyer et al. 2014), improve customer experience (Bakis et al. 2017; Davenport 2018), and gain competitive advantage (Eitle and Buxmann 2020). Considering these findings, we propose the following hypothesis:

Hypothesis 1: Relative advantage is positively related to ML adoption.

According to Rogers (1995), the component of compatibility reflects the perception to which an innovation is in line with the rooted values and prior experiences of users. Previous studies on innovation adoption such as ERP (Xu et al. 2017), RFID (Chong and Chan 2012), and e-business (Zhu et al. 2006) showed that the component of compatibility

has a positive impact on adoption. In general, compatibility refers to the extent to which an innovation can be connected to IT systems and software components (Gutierrez et al. 2015; Xu et al. 2017). Integrating innovations into existing IT landscapes can also alter existing business processes and work routines. Since these business process changes can have enterprise-wide implications, redesigning business processes is considered a major challenge for organizations (Venkatesh and Bala 2012). However, ensuring *process compatibility* can also enable organizations to leverage the full business value of ML by increasing organizational efficiency and productivity (Brynjolfsson and Mitchell 2017). In order to manage these significant changes, Kruse et al. (2019) suggest organizations to acquire ML-specific business process competencies. Since the qualitative studies by Pumplun et al. (2019) and Eitle and Buxmann (2020) revealed that organizations consider process compatibility as crucial, we believe that integrating ML applications into business processes can increase the adoption rate. Thus, we suggest the following hypothesis:

Hypothesis 2: Process compatibility is positively related to ML adoption.

The technological component of *complexity* describes the extent to which an innovation is perceived as difficult to understand and use (Rogers 1995). In case that a higher level of technological complexity increases the overall uncertainty and requires employees to learn new skills and competencies, organizations tend to reject the evaluation of initiatives and use cases (Junior et al. 2019; Martins et al. 2016). According to Xu et al. (2017), the level of complexity may also reduce the likelihood of innovation adoption among users as they are more likely to resist using a technology that is difficult to operate and may even require additional skills. Since ML is considered a complex technology due to the high efforts required to develop, train, and implement ML models (Jöhnk et al. 2021), the assumption that decision-makers and users might hesitate if the barriers are too high can also be applied to the context of ML. Due to this reason, we pose the following hypothesis:

Hypothesis 3: Complexity is negatively related to ML adoption.

Taking ML specifications into account, the qualitative studies by Eitle and Buxmann (2020), Jöhnk et al. (2021), Kruse et al. (2019), and Pumplun et al. (2019) propose the extension of the technological context by adding the component of *transparency*. According to their results, the adoption decision of ML applications can be influenced by the extent to which a decision-making process is transparent and comprehensible. Due to the fact that ML models learn and derive rules based on large historical data sets rather than being explicitly programmed (Samuel 1959), users have difficulties in understanding

and interpreting the outputs. In particular, advanced ML algorithms such as neural networks often represent black boxes that lack the ability to explain how a prediction was reached (Rudin 2019). According to previous studies, a higher level of transparency could have a positive impact on the adoption rate of ML applications since explanatory features could increase trust and thus the likelihood of adoption (Rzepka and Berger 2018; Sidorova and Rafiee 2019; Sturm and Peters 2020; Xu et al. 2014). Taking these findings into account, we suggest the following hypothesis:

Hypothesis 4: Transparency is positively related to ML adoption.

The **organizational context** of the TOE framework refers to a company's internal attributes, such as resources, structures, and processes which might have an impact on innovation adoption (Tornatzky and Fleischer 1990). Previous literature on innovation adoption has indicated that a high degree of *top management involvement* in the decision-making process can promote innovation adoption (Borgman et al. 2013; Chong and Chan 2012; Martins et al. 2016). Particularly in the allocation of technological, human, and financial resources, top management can have a considerable influence due to its decision-making authority. By supporting facilitating mechanisms, top management can contribute to creating an environment that encourages innovation and long-term visions. In addition, top management can reinforce the legitimacy of ML through performance indicators which are primarily required as the work routines of users may change as a result of ML implementations (Liang et al. 2007; Rai et al. 2009). Considering the impact of top management, we propose the following hypothesis:

Hypothesis 5: Top management involvement is positively related to ML adoption.

Technology competence refers to resources needed to drive innovations. According to previous literature on innovation adoption, technology competence consists of the two components of technological infrastructure and human resources (Chong and Chan 2012; Martins et al. 2016; Zhu et al. 2003, 2006). According to Zhu et al. (2006), technological infrastructure which comprises physical assets for developing innovation is complemented by human knowledge and skills. While the findings of previous studies showed that technology competence has a positive impact on innovation adoption (Chong and Chan 2012; Martins et al. 2016; Zhu et al. 2003, 2006), we anticipate the same effect in the context of ML. The fundamental prerequisite for a successful ML implementation is the provisioning of hardware and software for the development and deployment of ML applications (Jöhnk et al. 2021; Kruse et al. 2019). As the nature of programming changes

due to the self-learning capability of ML applications, organizations should employ highly skilled and experienced ML experts and data scientists (Eitle and Buxmann 2020; Jöhnk et al. 2021; Pumplun et al. 2019). By providing technology competence, the likelihood for a successful ML adoption increases. Thus, we pose the following hypothesis:

Hypothesis 6: Technology competence is positively related to ML adoption.

The **environmental context** of the TOE framework describes the external conditions under which an organization conducts its business (Tornatzky and Fleischer 1990). It includes factors such as the related industry, competitors, and regulations. With respect to competition, previous literature on innovation adoption emphasized that the competitive pressure which organizations feel from their rivals can also positively affect the adoption rate of innovation. When organizations face strong competitive pressure, they are able to change the rule of competition, alter the industry structure, and ultimately gain competitive advantage (Borgman et al. 2013; Gutierrez et al. 2015; Xu et al. 2017; Zhu et al. 2003, 2006). Particularly in the context of ML, competition is fierce as the implementation of ML applications enables organizations to improve decision-making processes and customer experiences. By leveraging this potential, we believe that competitive pressure can increase the adoption rate of ML and therefore suggest the following hypothesis:

Hypothesis 7: Competitive pressure is positively related to ML adoption.

As far as regulations related to ML are concerned, organizations must primarily ensure compliance with *data protection* regulations in their country. For example, the General Data Protection Regulation (GDPR), which was passed in 2018 within the European Union, prohibits the disclosure and misuse of personal data (Commission 2016). While organizations tend to take the compliance with data protection regulations seriously when implementing ML applications (Eitle and Buxmann 2020), the qualitative findings by Kruse et al. (2019) and Pumplun et al. (2019) indicate that the resulting requirement to eliminate or anonymize personal data in the training data set could also have a negative impact on ML adoption. The main reason for this assumption is that the functionality of the ML model is limited and results may not be conclusive if the training data set is reduced or anonymized by data protection regulations (Pumplun et al. 2019). However, we believe that users are more encouraged to incorporate ML applications into their work routines if they are convinced that the organization is committed to comply with data protection regulations. Thus, we propose the following hypothesis:

Hypothesis 8: Data protection is positively related to ML adoption.

Furthermore, *firm size* is also considered an organizational component which might influence the adoption rate of innovation. In this context, however, literature on innovation adoption provides inconsistent findings across different types of technologies. While Zhu et al. (2003) found a positive influence of firm size on the adoption stage of e-business technologies, the findings of Gutierrez et al. (2015) and Borgman et al. (2013) revealed that the influence was not significant for cloud computing technologies. Taking into account Rogers' (1995) statement that firm size could be a driver for the allocation of more resources, we believe that firm size could act as a moderator between technology competence and ML adoption. To be more precise, we assume that the larger an organization is, the more technology competence it has in terms of technological infrastructure and human resources. Therefore, we suggest the following hypothesis:

Hypothesis 9: Firm size positively moderates the relationship between technology competence and ML adoption.

6.4 Research Design

In this study, we conduct quantitative analysis based on the TOE framework to examine the influencing factors of ML adoption (Kim and Garrison 2010; Wu and Chuang 2010; Zhu et al. 2006). For the data analysis of the measurement and structural model, we used SmartPLS v. 3.3.3 (Ringle et al. 2015). To conduct the statistical analysis of the structural model, we applied the partial least squares (PLS) method (Fornell and Larcker 1981). This statistical method is appropriate for our study primarily because it is widely used in IS research (Chin 1998) and we follow an explorative research design (Gefen et al. 2011; Hair et al. 2006)

6.4.1 Measurements

To test our conceptual research model, we developed a questionnaire for an online survey. The development of the applied constructs is based on the TOE framework and literature on innovation adoption. Modifications in wordings were made to adapt the measurements to the context of ML. We controlled for age, gender, and industry. To ensure the validity and reliability of the constructs, we used multi-item measurements and applied a seven-point Likert scales, ranging from "1 strongly disagree" to "7 strongly agree". The dependent variable of ML adoption reflects the extent to which ML adoption affects an organization (Grover and Goslar 1993; Martins et al. 2016; Zhu et al. 2006). While a low impact of ML adoption refers to the assessment of ML use cases (Chong and Chan 2012;

Martins et al. 2016) the medium impact is related to the provision of resources for ML (Chong and Chan 2012; Martins et al. 2016). A high impact is reached when ML applications are incorporated into employees' work routines (Maas et al. 2018).The items of the independent variables are presented in Table 18.

6.4.2 Data Sample

To prepare the survey, we first sent the questionnaire to ML experts and academics, who reviewed the survey and provided detailed feedback on the structure of the questionnaire and comprehensibility of the items. Based on this feedback, we made refinements on the wording of the items. We were able to recruit data scientists through personal contacts, LinkedIn, and the participation on ML fairs. This target audience was explicitly selected because of their comprehensive knowledge of the technological, organizational, and environmental factors involved in ML implementations. After sending the potential participants a message explaining the research context, over 1,000 participants clicked on our survey link. Seven participants failed the attention check and we finally we have a sample size of n = 250. The distribution of the control variables age, gender, and industry is presented in Table 15. By examining the common method bias (CMB) (Podsakoff et al. 2003), our results indicate that no significant CMB is found in the data.

Table 15. Description of sample set

Industries (IND)	Automotive	Consulting	E-Commerce	Energy	Finance	IT	Logistics	Manufacturing	Marketing	Healthcare	Other	**Gender in %**		**Age (years) in %**	
												male	86.4	18-30	31.6
												female	13.2	31-40	43.2
														41-50	16.8
														51-65	8.4
in %	7.2	3.6	11.6	5.2	10.8	25.2	3.6	7.6	4.0	8.8	12.4				

6.4.3 Measurement and Structural Model

With respect to the measurement model, we assessed the convergent validity by checking that all latent variables are above the recommended thresholds of .5 for average variance extracted (AVE) and .7 for composite reliability and Cronbach's alpha. According to our results, the Cronbach's alpha value for the relative advantage construct exceeds the lower threshold of .6 which is, however, considered appropriate for exploratory research (Hair et al. 2012). In addition, we ensured that the item loadings surpass the threshold of .7 by removing, RA3, PC1 and CM3. As indicated in Table 16, the appropriate reliability and convergent validity for all constructs are fulfilled.

Table 16. Assessment of reliability and convergent validity

	Factor loadings	Composite reliability	AVE	Cronbach'α
RA	.861-.869	.856	.748	.663
PC	.905-.914	.906	.827	.792
CM	.908-.922	.911	.837	.806
TR	.713-.870	.894	.679	.842
TM	.820-.889	.921	.744	.886
TC	.704-.789	.861	.553	.806
CP	.918-.931	.922	.855	.831
DP	.926-952	.958	.884	.935

Table 17. Discriminant validity

	RA	PC	CM	TR	TM	TC	CP	DP
RA	.865							
PC	.346	.910						
CM	.027	-.110	.915					
TR	.204	.305	-.028	.824				
TM	.200	.313	-.025	.263	.863			
TC	.271	.339	-.127	.191	.254	.744		
CP	.298	.286	-.120	.111	.167	.285	.925	
DP	.127	.259	-.067	.136	.024	.192	.207	.940

By analyzing the discriminant validity, we verified that the square root of AVE is greater than the inter-construct correlations (Gefen et al. 2000). The square root of AVE is presented on the diagonal of Table 17. The results indicate sufficient discriminant validity for all constructs. Thus, the results revealed that the prerequisite for discriminant validity are met as well (Fornell and Larcker 1981).

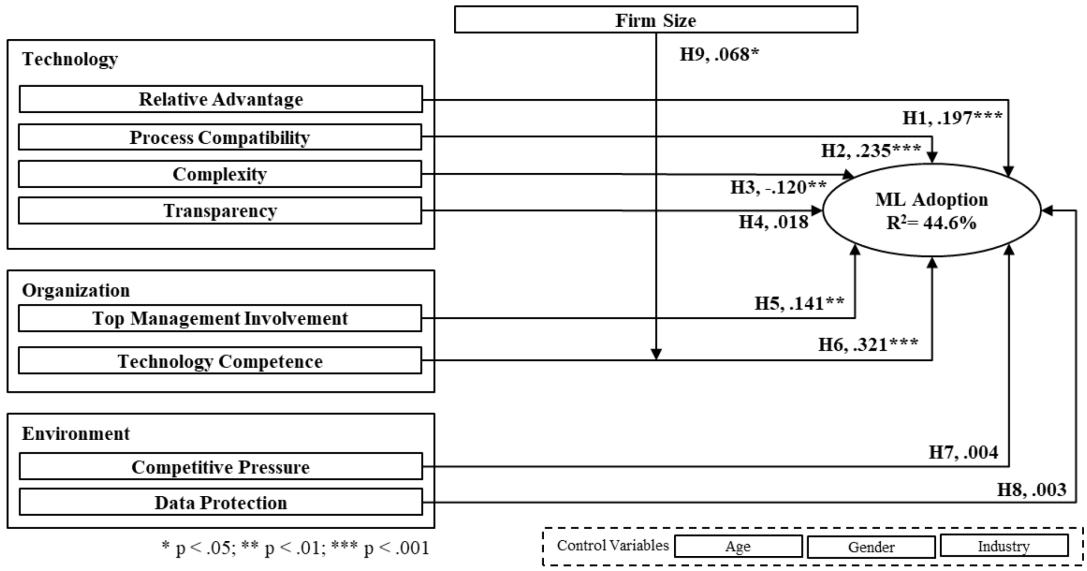

Figure 9. Results of structural model

We performed the structural model analysis based on the conceptual research model presented in Figure 9. According to our results, the R^2 value for ML adoption is predicted with 44.6 % which indicates that the independent variables explain a significant proportion of the variance in the dependent variable. In addition, we tested each individual hypothesis by examining the path coefficient and significance of its standardized path. The results are presented in Figure 9 and are explained in the following. Within the technological context, we found that relative advantage has a significant positive path to ML adoption (.197, $p < .001$). Furthermore, our results revealed that process compatibility has a significant positive path to ML adoption (.235, $p < .001$). Moreover, the influence of complexity on ML adoption is significantly negative (-.120, $p < .010$). However, transparency has no significant path to ML adoption (.018, n.s.). Within the organizational context, we found that top management involvement has a significant positive path to ML adoption (.141, $p < .010$). Moreover, our results show that technology competence has a significant positive path to ML adoption (.321, $p < .001$). Within the environmental context, competitive pressure has no significant influence on ML adoption (.004, n.s.). In addition, we found that data protection has no significant path to ML adoption (.003, n.s.). Finally, firm size positively moderates the path coefficient between technology competence and ML adoption (.068, $p < .05$). The respective simple slope analysis is plotted in Figure 10. This graph displays the impact of technology competence on ML adoption for both high and low firm sizes. The graph shows that organizations with a large firm size achieve higher ML adoption if they possess more technology competence. All in all, we provided evidence for the support of H1, H2, H3, H5, H6, and H9, while H4, H7 and H8 are not supported.

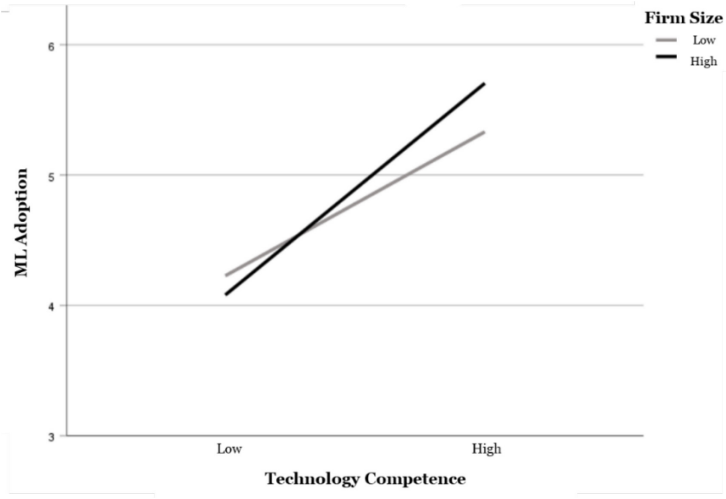

Figure 10. Simple slope analysis

6.5 Discussion

In previous qualitative research it remains unclear which factors statistically promote ML adoption (Eitle and Buxmann 2020; Jöhnk et al. 2021; Kruse et al. 2019; Pumplun et al. 2019). To understand how to overcome the challenges that organization face when adopting ML (Alsheiabni et al. 2019; Jöhnk et al. 2021), our study seeks to examine which generic and specific technological, organizational, and environmental factors can influence ML adoption. According to the descriptive results in Table 15, ML adoption is widespread in heterogeneous industries.

6.5.1 Findings

Within the **technological context**, our results revealed a significant positive influence of relative advantage on ML adoption (H1) which is consistent with previous studies (e.g., Chong and Chan 2012; Xu et al. 2017). This finding suggests that it is important for organizations to assess whether ML implementations can help them to achieve certain benefits. The advantages of using ML include better decision-making and improved customer experience. By leveraging these benefits, organizations can gain competitive advantage and use ML to better position themselves against their competitors. Additionally, the component of *process compatibility* was found to have a significant positive influence on ML adoption (H2). This finding is in line with previous research which showed that organizations tend to embrace innovation when their processes are compatible with the existing business processes landscape (Venkatesh and Bala 2012). Our findings confirm the assumption of Pumplun et al. (2019) and Eitle and Buxmann (2020) that organizations consider the process compatibility as a decision criteria for ML adoption. A seamless integration approach allows organizations to ensure that the ML application and existing business processes work cohesively and consistently. In addition, there is a significant negative influence of *complexity* on ML adoption (H3). This finding indicates that the level of uncertainty in using ML applications increases when users perceive them as complex and difficult to operate. Since high complexity reduces the likelihood of ML adoption, it is important for organizations to take appropriate measures. A possibility to reduce complexity is the focus on a user-centered perspective by involving them at the earliest point of time of the adoption process. Considering the technological component of *transparency*, our results revealed that transparency has no significant impact of ML adoption (H4). These results are not in line with our expectations and previous studies (Rzepka and Berger 2018; Sidorova and Rafiee 2019; Sturm and Peters

2020; Xu et al. 2014) which emphasized that explanatory features can help users to better understand the outcome and potentially establish trust (Bohanec et al. 2017). We suspect that our result is related to the assumption that there is a difference between users' perceived behavior of preferring transparency and their actual behavior of using ML applications that are, however, not transparent to them. Even though our study indicates a subordinate role for transparency, current research urges further investigation into the extent to which transparency is essential for trustworthy ML (e.g., John-Mathews 2021).For instance, in healthcare, such as the diagnose diseases, transparency is crucial for ML applications (Hofmann et al. 2019).

In the **organizational context**, we found a significant positive path coefficient between the component of *top management involvement* and ML adoption (H5). Our results confirmed the findings of previous innovation adoption studies (Borgman et al. 2013; Chong and Chan 2012; Martins et al. 2016) which stated that top management involvement influences the decision-making process of innovation adoption. Top management is required to emphasize the strategic impact of implementing ML applications by spreading its long-term vision throughout the organization. In addition, top management has also the decision-making power on allocating technological (e.g., training data sets), human (e.g., data scientists), and financial (e.g., budget) resources which are considered main prerequisites for a successful ML implementation. In addition, our results revealed a significant positive path coefficient between *technology competence* and ML adoption (H6). In line with previous literature (e.g., Zhu et al. 2003, 2006), technology competence is the strongest factor leveraging ML adoption. Thus, organizations are more likely to adopt ML if they have the technological infrastructure such as centralized data repositories and transfer technologies available and highly specialized ML experts and data scientists employed.

In the **environmental context**, our results did not show a significant path coefficient between competitive pressure and ML adoption (H7) which is not in line with previous studies (Gutierrez et al. 2015; Xu et al. 2017; e.g., Zhu et al. 2006). Strong competitive pressure might drive organizations to leap rapidly from one innovation to the next without sufficient time to incorporate ML throughout the entire organization. One plausible explanation for the non-significant path coefficient is that ML implementations require enough time to develop and deploy ML applications and provide the necessary technology competence. This finding indicates that too much competitive pressure does not necessarily

increase the adoption rate of ML. Furthermore, we found no significant evidence that *data protection* influences ML adoption (H8). Since the training of ML algorithm depends on data, we believe that data types might play a crucial role when examining data protection. For example, unlike sensor data, patient data used for disease diagnoses is very sensitive to individuals and therefore requires a high level of data protection. Thus, we encourage further research to analyze the role of data protection on ML adoption in more detail.

Moderation: In previous innovation adoption studies (Borgman et al. 2013; Gutierrez et al. 2015; Zhu et al. 2003), *firm size* has been controversially discussed. In order to shed more light in the context of ML, we confirm that firm size positively moderates the relationship between technology competence and ML adoption (H9). Taking this finding into account, we found evidence that larger organizations have more technology competence available which ultimately increases the likelihood for a successful ML adoption. As shown in Figure 10, the slope of the straight line of organizations with a large firm size is steeper than for organizations with a small firm size. Considering the intersection of the two straight lines for small and large organizations, our results suggest that larger firms can leverage the potential for ML adoption once they have established a certain level of technology competence. Once this intersection is reached, large organizations are more likely to adopt ML applications than small organizations.

6.5.2 Theoretical Contributions

Although ML is considered a megatrend in the current digital age (Goasduff 2020), the low ML adoption rate of 2.8 percent indicates that organizations face challenges in implementing ML applications (Zolas et al. 2020). While studies on innovation adoption in other fields such as ERP (Junior et al. 2019; Xu et al. 2017), CRM (Cruz-Jesus et al. 2019), and cloud computing (Borgman et al. 2013; Martins et al. 2016) are prevalent, research in the context of ML adoption is very scarce. Thus, by drawing on prior research on innovation adoption and using the TOE framework as a theoretical foundation, we examined which generic and specific technological, organizational, environmental factors can increase the adoption rate of ML. In the following, we present three theoretical contributions to the literature of ML adoption.

First, we theorized and empirically validated the impact of generic technological, organizational, and environmental factors on ML adoption. Following the call for research of Jöhnk et al. (2021) and Pumplun et al. (2019), we used a quantitative research design to

examine which generic factors of the TOE framework influence ML adoption. Given the limited research in this field, we provided valuable insights into the impact of the generic components of relative advantage, process compatibility, complexity, top management involvement, technology competence, and competitive pressure on ML adoption (e.g., Chong and Chan 2012; Gutierrez et al. 2015; Jöhnk et al. 2021; Xu et al. 2017). Our results revealed that the key drivers to leverage ML adoption are technology competence, process compatibility, relative advantage, and top management involvement. Second, we adjusted the widely used TOE framework by Tornatzky and Fleischer (1990) to the ML context and extended the research model with ML specifications. With respect to the specific factors, we adapted the components of transparency (Peters et al. 2020) and data protection (e.g., Pumplun et al. 2019) from previous research. We operationalized the two constructs from the perspective of data scientists. Even though our results showed that transparency and data protection have no significant influence on ML adoption, we believe that these technological and environmental components are in principle important ML specifications. Due to the self-learning capabilities of ML applications, the decision-making process is no longer the sole responsibility of humans but is augmented by ML applications. Since end users still need to interpret and process the given output in their decision-making process, the focus should still remain on transparency (Berente et al. 2021). Even though the impact of data protection was not significant in our study, we believe that data protection may be essential in others context depending on the sensitivity of the underlying data set. Third, due to inconsistent findings in previous literature on innovation adoption regarding the role of firm size, we shed light on the moderator effect of firm size on the relationship between technology competence and ML adoption. Our study revealed that larger organizations are more likely to adopt ML adoption as they have more technology competence available. To increase the likelihood for smaller organizations, they could try to establish more technology competence by providing the necessary infrastructure and hiring ML experts and data scientists. Finally, future studies could use the respective constructs and items since the requirements of the measurement model, including reliability and validity tests, were fulfilled.

6.5.3 Practical Contributions

Our study provides useful practical guidance for organizations seeking to implement ML applications. Our findings enable managers to consider relevant factors that influence ML adoption and define appropriate requirements and measures. According to our results,

process compatibility between ML applications and the existing business process landscape is crucial for unlocking the full business value of ML. Thus, we recommend that organizations should examine how ML could change their business processes and evaluate the options to carefully redesign them. Additionally, managers need to emphasize and communicate the value of ML within their organization, while also addressing the issue of complexity. Since the complexity of ML could decrease the adoption rate of ML, it becomes even more important for organizations to highlight the added value. Furthermore, managers concerned about obtaining sufficient technological, human, and financial resources to implement ML applications should ensure that top management is involved as they have the decision-making power over resource allocation.

6.6 Conclusion, Limitations, and Future Research

To overcome the challenges which organizations face when implementing ML applications and to provide guidance during ML adoption, we followed a quantitative research design to examine which generic and specific technological, organizational, environmental factors influence ML adoption. By reaching 250 participants, we were able to gain valuable insights for research on ML adoption. Our study revealed that the availability of technology competence promotes ML adoption. Further important components of ML adoption refer to process compatibility, relative advantage, and top management involvement. In addition, our study showed that firm size moderates the relationship between technology competence and ML adoption. Drawing on previous qualitative studies on ML adoption (Eitle and Buxmann 2020; Jöhnk et al. 2021; Kruse et al. 2019; Pumplun et al. 2019), we contribute to IS literature by extending the TOE framework by Tornatzky and Fleischer (1990) with ML specifications and providing quantitative evidence. Despite these contributions, our study is subject to some limitations. First, the list of variables examined in our research model does not claim to be exhaustive. Future research can build on and further extend the proposed research model of ML adoption by including other technological, organizational, and environmental factors or ML specifications. Second, the findings are by nature more general since the sample set includes a variety of industries. Future research may focus on distinct industries to examine the research model in a particular industry or compare two different industries to discover similarities or differences (service versus IT industry). Third, future research could conduct a more detailed examination of the insignificant components of our studies in different domains. Finally, by selecting data scientists as the main target audience, we limited the

sample set to a relatively small niche. Future studies could attempt to increase the sample size to gain further insights of ML adoption.

6.7 Appendix

Table 18. Measurement of independent variables

	Item	Item Description	Source
RA		To what extent are machine learning applications important for achieving the following objectives in your organization?	(Chwelos et al. 2001; Iacovou et al. 1995)
	RA1	Improved competitiveness	
	RA2	Improved service to customer	
	RA3	Improved quality of decision-making	
PC	PC1	ML applications complement the main traditional systems (e.g., legacy system).	(Venkatesh and Bala 2012; Xu et al. 2017)
	PC2	ML applications fit well with the main needs of your organization.	
	PC3	ML applications fit well with the main work processes of your organization.	
CM	CM1	The use of ML applications is difficult for employees (users) to learn.	(Xu et al. 2017)
	CM2	ML applications are difficult for employees (users) to operate compared to traditional systems.	
	CM3	ML applications are difficult for employees (data scientist) to maintain compared to traditional systems.	
TR	TR1	The feature importance functionality makes the argumentation process of the ML application clear to the employee.	(Peters et al. 2020)
	TR2	Due to the feature importance functionality, employees easily understand how the results of the ML application were generated.	
	TR3	The feature importance functionality enables the employees to understand how the ML application performs its job.	
	TR4	Due to the feature importance functionality, the ML application logic provides clear advice to the employees.	
TM	TM1	Top management attends ML project meetings.	(Grover and Goslar 1993)
	TM2	Top management is involved in information requirements analysis for ML projects.	
	TM3	Top management is involved in reviewing recommendations for ML projects.	
	TM4	Top management is involved in decision-making for ML projects.	
TC	TC1	Your organization employs highly specialized employees for machine learning applications (e.g., data scientists).	(Gangwar et al. 2015)
	TC2	Your organization has a sufficient amount of data for machine learning applications.	
	TC3	Your organization has access to data and is allowed to use data in machine learning applications due to the respective data ownership.	
	TC4	Your organization has a centralized data repository (e.g., data lake) for machine learning applications.	
	TC5	Your organization has mature data transfer technologies (e.g., cloud systems) for machine learning applications.	

CP	CP1	The competitive pressure in your industry influences your organization to adopt machine learning applications.	(Chwelos et al. 2001)
	CP2	The pressure to adopt machine learning applications from your competitors is high.	
DP		Your organization must adhere to data protection regulations in the process of...	(Tractinsky and Jarvenpaa 1995)
	DP1	… designing ML use cases.	
	DP2	… pre-processing the training set.	
	DP3	… developing ML models.	
FS		To what extent do you agree with the following statements about your firm size?	(Chong and Chan 2012)
	FS1	The number of employees of your organization is higher compared to the industry.	

Acknowledgements

This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

7 Paper E: Uncovering Cultural Differences in Organizational Readiness for Artificial Intelligence: A Comparison between Germany and the United States

Title

Uncovering Cultural Differences in Organizational Readiness for Artificial Intelligence: A Comparison between Germany and the United States

Authors

Anne Zöll, Verena Eitle, Patrick Hendriks

Publication Outlet

Hawaii International Conference on Systems Science

Abstract

Artificial Intelligence (AI) transforms the business world by enabling organizations to leverage new business opportunities through its unique capabilities of self-learning and autonomous decision-making. To unlock the disruptive potential of AI, organizations seek to implement AI applications throughout their business landscape. However, from a cross-cultural perspective, national culture can influence the way organizations implement AI applications. To better understand cross-cultural differences on AI adoption, our study combines Hofstede's national cultural framework with the organizational readiness concept for AI. We examined the moderating role of Hofstede's national cultural dimensions on the organizational readiness factors of AI-process fit, financial resources, upskilling, collaborative work, and data quality. By conducting a multi-group analysis, we aim to identify national cultural differences between Germany and the US in AI adoption.

Keywords

Cultural differences, cross–cultural study, artificial intelligence, machine learning, adoption

7.1 Introduction

The introduction of technology is profoundly influenced by diverse cultures, leading to different patterns of technological diffusion across societies. Diverse cultures shape the implementation of technologies with their unique attributes and influence the ways these technologies are integrated and used. Cross-cultural research helps organizations identify commonalities and differences in technologies need across societies, leading to more effective global technology strategies (Bharadwaj et al. 2013). This phenomenon is prominently observable in the field of Artificial Intelligence (AI), where the approaches of different countries exemplify the fusion of technology with cultural nuances. As an illustrative example, the interplay between education, workforce development, and AI deployment highlights the impact of cultural disparities: Germany (GER) is strongly committed to vocational training and skills enhancement. The country's AI education is designed to seamlessly incorporate AI applications into traditional industries. A profound effort is made to equip the workforce with AI-related proficiencies essential for sectors like manufacturing and engineering (Eitle and Buxmann 2020). The United States (US), known for its adaptable and entrepreneurial educational framework, tailors AI education towards technology and software development. The focus lies in cultivating skills that transcend various industries, including the dynamic realms of startups and technology-driven enterprises. These national cultural influences are equally evident in the sphere of manufacturing and the integration of AI. GER, renowned for its robust manufacturing sector, has embraced the principles of Industry 4.0, emphasizing the fusion of AI and automation into production processes. AI applications such as predictive maintenance and process optimization are prioritized, augmenting production efficiency. In contrast, the US' diverse industrial landscape extends beyond manufacturing. AI is, for instance, employed to optimize transportation and supply chain management (IPSOS 2022). Moreover, the US places a premium on AI-powered innovation within software and technology services (Acemoglu et al. 2022).

In academia these cultural differences become evident through an illustrative study that emphasizes different ethical preferences. Awad et al. (2018) introduced a web-based experimental platform called Moral Machine. They conducted a study that revealed variations in ethical preferences across cultures. To identify these cultural differences and nuances, conducting cultural studies becomes crucial. If AI algorithms are developed without considering cultural nuances specific to a particular country, it can result in biased or inappropriate decision-making, causing harm or misunderstanding. Thus, we aim to

answer the research question: How do national cultural differences between Germany and the United States impact AI adoption?

7.2 Theoretical Background

7.2.1 Definition of Artificial Intelligence

According to Russell (2021), the notion of AI is based on the concept of an intelligent agent which receives percepts from the environment and acts accordingly. Due to the goal of maximizing performance, intelligent agents seek to perform their actions in a way that yield the best results. To achieve this behavior, intelligent agents must be able to learn from their experiences and adapt their knowledge to new environments. Thus, the capabilities of an intelligent agent enable AI applications to perform cognitive tasks such as self-learning and autonomous decision-making. The resulting shift in tasks may lead to a greater inscrutability in the decision-making process as it is no longer the sole responsibility of humans but is complemented by AI (Berente et al. 2021). Since AI comprises technologies such as expert systems, machine learning, robotics, natural language processing, and machine vision (Collins et al. 2021), the range of application scenarios within organizations and across industries is wide. Due to this broad spectrum, technical advancements, and the development of complementary innovations, AI is considered a general-purpose technology (GPT) (Brynjolfsson et al. 2017).

7.2.2 Organizational Readiness Concept for AI

To effectively navigate the extensive organizational changes that come with adopting innovation, organizations must strive to attain a state of readiness at the organizational level. This condition reflects whether an organization is structurally and psychologically prepared for the upcoming organizational change (Weiner 2009). Rather than considering these two states separately, Nguyen et al. (2019)suggest combining both perspectives when assessing organizational readiness for innovation adoption. Since AI is considered a GPT, we decided to use the organizational readiness concept according to Jöhnk et al. (2021) as the basis for examining cultural differences in AI adoption. To provide a holistic view of the state of organizational readiness for AI, we rely on the five categories that comprise the organizational readiness concept (Jöhnk et al. 2021): strategic alignment, resources, knowledge, culture, and data.

The category strategic alignment consists of five factors: AI-business potentials, customer AI readiness, top management support, AI-process fit, and data-driven decision-making. In this study, we focus on the AI-process fit since the AI experts of our study possess specialized knowledge about the intricacies of AI technologies and their integration into organizational processes. By concentrating on AI-process fit, we tap into their domain-specific insights to understand how these experts perceive the alignment between AI technologies and existing organizational workflows.

The category resources consist of three factors: Financial budget, personnel, and IT infrastructure. We focus on financial budget because it is a critical aspect of AI adoption. We seek to understand how different cultures allocate and manage finances, revealing their priorities. Focusing on financial budgeting allows for cross-cultural comparisons regarding financial resource allocation strategies. Since different cultures may make different investment decisions in AI adoption, understanding these variations can help to develop targeted strategies for maximizing AI readiness in diverse cultural environments.

The category knowledge consists of three factors: AI awareness, upskilling, and AI ethics. We concentrate on the factor upskilling since AI experts are intimately familiar with the specific skills and competencies required to effectively integrate AI technologies. By focusing on upskilling from their perspective, the study can provide tailored insights into the areas of knowledge enhancement that are crucial for successful AI adoption.

The category culture consists of three factors: Innovativeness, collaborative work, and change management. Collaborative work is a fundamental element of organizational readiness, especially in the context of AI adoption. It involves the effective coordination of diverse skill sets and perspectives, making it essential to understand how cultural dimensions impact collaborative efforts in embracing AI technologies. It examines how AI experts perceive the collaborative dynamics within their organizations.

The category data consists of four factors: Data availability, data quality, data accessibility, and data flow. In an initial step influenced by the research discourse, we direct our attention toward data quality. Data quality is foundational to the reliability and effectiveness of AI applications. To gain meaningful insights from AI technologies, it is important to ensure that data is accurate and consistent. Focusing on data quality delves into the core of AI's functionality.

7.2.3 Hofstede's National Cultural Framework

In a cultural context, there is no one-size-fits-all strategy for adopting innovation as the diffusion of technologies is not bound by national borders and can, therefore, be influenced by cultural effects. In IS literature, the most predominate definition refers to Hofstede (2001) who defines culture as "the collective programming of the mind that distinguishes the members of one group or category of people from another" (Hofstede 2001, p. 9).

We aim to investigate the diversity of culture at the organizational level and examine cultural differences between GER and the US in the context of AI adoption. These two countries were selected primarily because they lead the ranking in AI adoption due to the high number of productive AI applications and use cases (Loucks et al. 2019). In addition, these two countries have distinct innovation ecosystems. The US, with Silicon Valley as a global technology hub, is known for its entrepreneurial spirit and tech startups. GER has a strong industrial base and is recognized for its engineering and manufacturing capabilities. We use Hofstede's (2001) main cultural dimensions of individualism, uncertainty avoidance, and long-term orientation to examine our RQ. This selection is based on the fact that these dimensions exhibit the most pronounced variations in the scores. Individualism is defined as the extent to which individuals prefer independence over inclusion in a group. In an organizational context, members of an individualist society tend to be self-reliant and show a high degree of initiative (Hofstede 2001). GER has a relatively high score: 67. In contrast, the US has a high score: 97. Uncertainty avoidance is defined as the willingness of dealing with an ambiguous and unknown situation. From an organizational perspective, the risk of unpredictable circumstances can be minimized through regulations (Hofstede 2001). GER has a relatively high score: 65. In contrast, the US has a relatively low score: 46. Long-term orientation is defined as the tendency to prioritize the future by relying on pragmatic approaches. In an organizational context, these societies promote long-term success and visions, while short-term oriented societies focus on achievements in the near future (Hofstede 2001). GER has a high score: 83. In contrast, the US has a low score: 26.

Scholarly studies using Hofstede's cultural dimensions have faced criticism from various angles (e.g., Beugelsdijk et al. 2019) . The concept of culture operates at a macro-level (Srite and Karahanna 2006), emphasizing a recurring critique of Hofstede's framework, specifically the argument of cultural homogeneity. This argument challenges the assumption that domestic populations are uniform entities, while nations actually comprise

diverse ethnic groups (Nasif et al. 1991). Conversely, countries do embody shared historical experiences that shape their national identity and prevailing cultural values (Beugelsdijk et al. 2019). Therefore, when analyzing cultures as the focus of our study, Hofstede's scores can be viewed as representing averages derived from samples of their populations. Consequently, these scores have been considered a widely accepted and frequently used approach.

7.2.4 Culture and AI Adoption

While numerous studies have explored the influence of culture on innovation adoption at the individual-level (Srite and Karahanna 2006), there is a discernible gap in research that extends this examination to the organizational context. Building on this foundation, a subset of studies has delved into the domain of organizational innovation adoption. Notably, these studies narrow their focus to specific contexts, including enterprise resource planning systems (Waarts and van Everdingen 2005), IT infrastructure (Png et al. 2001), introduction of novel products, ideas, or behaviors (Yeniyurt and Townsend 2003), and software production (Walsham 2002). In addition, prior research concentrated on frameworks at the individual level such as the common Technology Acceptance Model (TAM) that investigates the acceptance of emerging technologies (McCoy et al. 2007). Preceding studies explored the impact of culture on mobile learning adoption (Wang and Zander 2018).

There's a big gap in understanding how culture influences the link between organizational readiness and AI adoption in the field of culture and adoption research. Reevaluating AI adoption is crucial because AI's unique attributes distinguish it from earlier technologies such as rule-based systems. Notably, AI applications are often inscrutable due to their data-driven learning approach (Rudin 2019). Unlike their predecessors, these systems do not always yield predictable outcomes and may even propose erroneous strategies (Domingos 2012), making their integration into organizational landscapes distinct from other systems. Consequently, the adoption of AI applications requires substantial organizational transformation. Acknowledging this, Kane et al. (2021) emphasized the significance of exploring how organizations can proactively prepare for an AI-driven future. Due to the limited existing research, our study undertakes the task of elucidating the impact of culture on the factors of organizational readiness for AI adoption.

7.3 Hypotheses

Our research model in Figure 11 shows the impact of culture on the organizational readiness factors for AI. To define the hypotheses for cultural differences in AI adoption, we combine Hofstede's (2001) cultural framework with the organizational readiness concept for AI (Jöhnk et al. 2021).

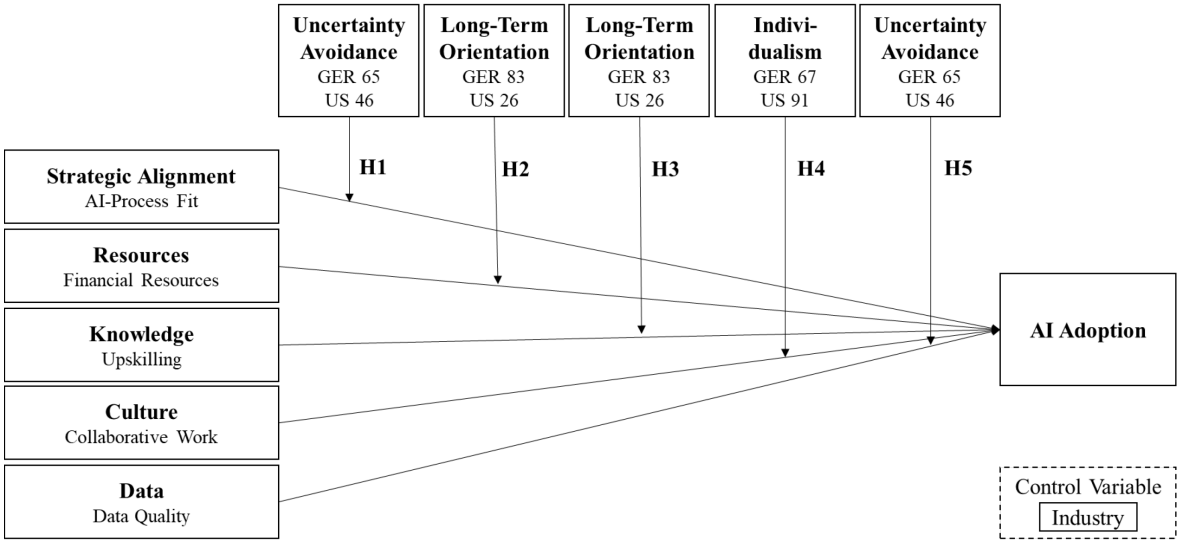

Figure 11. Research model

AI-Process Fit (PF): According to the innovation adoption literature, compatibility is a prerequisite for innovation adoption in organizations (Xu et al. 2017). Since standardization, reengineering, and implementation of new business processes facilitate AI adoption (Kruse et al. 2019), we follow the recommendation of Jöhnk et al. (2021) to consider AI-process fit as an organizational readiness factor. Generally, organizations rely on long-established business processes that have proven themselves in the past and provide them control over their innovation adoption (Xu et al. 2017). However, when these business processes need to be adjusted, organizations face major challenges (Venkatesh and Bala 2012). Even though these alterations are very likely in the field of AI (Brynjolfsson et al. 2017), the necessary adjustments related to business processes are subject to uncertainties. Even though the given AI capabilities of self-learning and autonomous decision-making increase human-machine collaboration (Berente et al. 2021), it is relatively unclear to what extent AI applications will augment decision-making processes. In this context, pertinent insights can be drawn from organizational literature, which posits that control strategies offer a strategic avenue for mitigating uncertainties (Thompson 1967). This line of thought is notably mirrored in the domain of cultural studies, exemplified by Hwang's work (2005), where processes fostering control are

consistent with the concept of uncertainty avoidance, as they demonstrate an ability to limit unforeseeable variables. The cultural dimension of uncertainty avoidance revolves around an individual's inclination toward structured as opposed to unstructured situations. Recognizing the pivotal role that uncertainty assumes as an environmental precursor to control mechanisms, we heed Hwang's advice (2005) and investigate the alignment between AI processes and the cultural aspect of uncertainty avoidance. This dimension refers to the extent to which organizations in cultures with high uncertainty avoidance scores establish rules and predefined processes to eliminate unforeseen events and to increase control in AI adoption (Javidan et al. 2006). In contrast, cultures with low uncertainty avoidance scores are more willing to take risks and do not need that much control mechanisms (Hofstede 2001). Since the uncertainty avoidance score is higher in GER (65) than in the US (46), we expect a cultural difference in the sense that the US is better at coping with uncertainties related to AI. Organizations from GER are more likely to establish standards and structured business processes when adopting AI. Considering these findings, we define the following hypothesis: H1: The positive effect of AI-process fit on AI adoption is stronger in GER than in the US.

Financial Resources (FR): The allocation of financial resources is considered a crucial organizational readiness factor when implementing innovation. Organizations need to allocate sufficient financial budget, for example, to establish the required infrastructure, ensure business process integration, and attract new candidates (Xu et al. 2017). Previous research commonly examined the moderating influence of long-term orientation and financial background. For instance,Khlif et al. (2015) investigated the moderating role of long-term orientation in the relationship between financial profitability and social and environmental disclosure. Additionally, Bahadir and Bahadir (2020) discovered that the level of long-term orientation moderates the impact of financial development on total advertising spending, a higher long-term orientation results in a more pronounced positive effect. Thus, with respect to Hofstede's (2001) cultural framework, we associated financial resources with the cultural dimension of long-term orientation (Waarts and van Everdingen 2005). Countries with a short-term orientation often seek rapid returns on financial investments. In the context of AI adoption, they may prioritize projects offering immediate efficiency gains or cost savings over longer-term endeavors requiring substantial initial investments. Instead of committing financial resources to a single AI initiative, short-term cultures tend to favor incremental investments. They allocate smaller funds to multiple projects promising quick returns, spreading risk in line with their preference for immediate

outcomes. Thus, the relatively low score of US (26) indicates that organizations tend to focus more on immediate results, regarding AI applications and are, therefore, more willing to make the necessary investments.

Countries with a high long-term score tend to see AI adoption as a gateway to sustainable growth. Countries with a high long-term orientation score, such as GER (83), are often inclined to allocate significant financial resources to building a robust AI infrastructure. They see AI as a strategic investment. At the same time, they take a cautious approach to resource allocation. They conduct careful assessments of potential AI projects to ensure alignment with the organization's long-term goals. Based on these ideas, we assume that countries with lower long-term orientation scores such as the US may regard AI adoption as an opportunity for more immediate returns and efficiencies rather than prioritizing long-term growth and strategic investments in AI infrastructure such as countries like GER. Based on the discrepancy in long-term orientation between GER (83) and the US (26), we anticipate a cultural difference in AI adoption. Thus, we propose the following hypothesis: H2: The positive effect of financial resources on AI adoption is stronger in the US than in the GER.

Upskilling (UPS): An essential organizational readiness factor for increasing the adoption rate of innovation refers to upskilling. In other words, employees require proper training on a technology to better understand and use it more effectively (Jöhnk et al. 2021; Xu et al. 2017). Since users feel more confident in using an innovation through the acquired skills and competencies, the level of anxiety and ambiguity may decrease (Schillewaert et al. 2005). Particularly in the case of AI, an appropriate skill set is required to be able to interact with the unique AI capabilities of self-learning and autonomous decision-making. Since the level of inscrutability might increase due to the distribution of decision power between humans and AI applications (Berente et al. 2021), users need to learn how to correctly interpret the outcomes of AI applications and incorporate them into the decision-making process (Jöhnk et al. 2021). With respect to Hofstede's (2001) cultural framework, the associated persistence is mainly reflected by the cultural dimension of long-term orientation (Waarts and van Everdingen 2005). According to the findings of Özbilen (2017), long-term oriented countries consider learning a work value which increases the motivation to acquire new knowledge and skills. By encouraging learning through upskilling, cultures with high long-term orientation scores are more likely to successfully implement innovation due to the acquired expertise (Özbilen 2017). Considering these

insights, we assume that GER (83) is more inclined to promote AI specific user training than the US (26). Thus, we pose the hypothesis: H3: The positive effect of upskilling on AI adoption is stronger in GER than in the US.

Collaborative Work (CW): Creating and assimilating knowledge through close collaboration among stakeholders enables organizations to better understand the requirements of innovation (Cao et al. 2010). With respect to AI adoption, a close collaboration between functional and data science teams is particularly important to assess functional problems and the technical feasibility of use cases and corresponding AI applications (Eitle and Buxmann 2020; Kruse et al. 2019). Rather than maintaining traditional siloed structures, collaborative work between these teams can accelerate innovation cycles as frequent interactions and short lines of communications drive ideation and prototyping (Pumplun et al. 2019). Drawing on Hofstede's (2001) cultural framework, the degree of collaboration is mainly determined through the cultural dimension of individualism. Since collective societies that score is low on individualism are more concerned with the needs of the group, they prefer group decisions over individualistic actions. The study by Magnusson and Peterson (2014) showed that collective cultures tend to strengthen collaboration as group goals can primarily be achieved through interpersonal ties and shared visions. By ensuring a constant information flow, cross-functional teams in collective societies are more likely to contribute to organizational-wide collaboration (Engelen et al. 2012). Since a close collaboration between functional and data science teams facilitates the implementation of AI, we anticipate a cultural difference between GER and the US in AI adoption. The lower score in GER (67) compared to the high score in the US (91) indicates that GER encourages closer collaboration between these teams than the US. Thus, we pose the hypothesis: H4: The positive effect of collaborative work on AI adoption is stronger in GER than in the US.

Data Quality (DQ): Data quality management is a major concern in organizations which becomes even more relevant as the amount and variety of data increases, analysis capabilities enhance, and business process integration matures (e.g., Glowalla and Sunyaev 2013). In the context of AI, the quality of training data is particularly important since the outcomes of AI applications are based on historical data (Sturm and Peters 2020). If data quality is not reliable, the results of AI applications might be biased or prone to ethical issues (Awad et al. 2018). In general, data quality issues are mainly caused by incomplete data in the form of missing values or incorrect data (Sturm and Peters 2020). According to

Welzer and Hölbl (2000), the different handling of data quality issues may be related to the differences in values and beliefs that arise from culture. Since reliable outcomes through the correctness and accuracy of data help to provide reliable outcomes and consequently create certainty in organizations, data quality can therefore be related to the cultural dimension of uncertainty avoidance (Hofstede 2001; Welzer and Hölbl 2000). High uncertainty avoidance cultures, such as GER, tend to favor structured and well-defined decision-making processes. They are more inclined to seek clear information before making decisions, as uncertainty is often perceived as a source of risk. In contrast, low uncertainty avoidance cultures, such as the US, may be more comfortable with ambiguity and may be willing to accept a certain degree of uncertainty in their decision-making. Overall, countries in high uncertainty avoidance cultures, such as GER (65) may be less willing to adopt AI applications if data quality is perceived as a potential source of increased uncertainty compared to countries with low uncertainty such as the US (46). Thus, we hypothesis: H5: The positive effect of data quality on AI adoption is stronger in GER than in the US.

7.4 Research Design and Data Analysis

Regarding data collection, we applied a survey-based approach and developed a questionnaire. Drawing from the established literature on organizational readiness, AI adoption, and culture, we derived the measurements for the following constructs: AI-process fit (Xu et al. 2017) (e.g., “AI applications fit well with the main work processes of your organization.”), financial resources (Chong and Chan 2012) (e.g., “Your organization has the financial resources to purchase hardware and software required for AI projects.”), upskilling (Schillewaert et al. 2005) (e.g., “The employees receive sufficient training to use the AI applications effectively.”), collaborative work (Cao et al. 2010) (e.g., “During AI projects, the data science team and the specialist departments involved have informal communication.”), and data quality (Weill and Vitale 1999) (e.g., “The training data used in AI applications are accurate.”). The items of the independent variables are measured based on a seven-point Likert scale ranging from “1 strongly disagree” to “7 strongly agree”. To determine to what extent AI applications have been implemented in organizations, our dependent variable of AI adoption encompasses three intensity levels (Chong and Chan 2012; Maas et al. 2018). While low intensity refers to the evaluation of AI use cases and appropriate AI applications, medium intensity involves the allocation of resources to implement AI applications. High intensity includes the incorporation of AI

applications into work routines. With respect to the sample set, we invited 2,153 AI experts from GER and the US to participate in our online survey on LinkedIn, of which 1,351 experts clicked on the survey. After sorting out incomplete surveys and those with a failed attention check, 232 participants completed our survey which results in a completion rate of 17%. After splitting the total sample into two groups based on the categorial variable culture by which the organization is managed, we obtained two subsamples with 155 participants for GER and 77 participants for the US. To ensure their expertise in AI, we also inquired about their years of experience (YoE) in AI. The distribution is shown in Table 19:

Table 19. Years of experience

YoE	GER (%)	US (%)
<1	4.5	3.9
1-2	25.2	22.0
3-5	33.5	26.0
>5	36.8	48.1

We also present industry distribution in Table 20.

Table 20. Distribution of industries

Industries in %	Auto-motive	E-Commerce	Energy	Finance	IT & Software	Logistics	Manu-facturing	Marketing	Health-care	Other
GER	16	8	6	8	19	9	8	5	9	12
US	3	16	3	17	27	7	5	3	9	12

The quantitative data analysis for our research model was conducted in a three-stage approach. First, we used SmartPLSv4 to analyze the measurement model in terms of validity and reliability for both countries separately. Secondly, in preparation for the multi-group analysis (MGA), we assessed the measurement invariance of composite models (MICOM) (Henseler et al. 2016). Thirdly, the MGA was conducted to determine the differences in path coefficients between GER and the US (Henseler et al. 2009). The partial least squares (PLS) method was primarily chosen because of the exploratory nature of our study and the lower sample size as the number of observations (Fornell and Larcker 1981; Gaskin and Lowry 2014).

7.4.1 Measurement Model

To ensure content validity, we followed the recommendations of McKenzie et al. (1999) to adapt the items to the context of AI. To obtain feedback on the terminology, the questionnaire was reviewed and adjusted by a panel of 12 AI researchers and practitioners. With respect to construct validity of the measurement models, we tested convergent validity and discriminant validity for each country separately (Hair et al. 2016). Convergent validity was assessed using the criteria of indicator reliability, composite reliability (CR), Cronbach's Alpha (α), and average variance extracted (AVE). To ensure indicator reliability, constructs should explain at least 50% of the variance of their respective indicators, which corresponds to a threshold of .7 for factor loadings(Hair et al. 2006). Factor loadings were higher than the threshold of .7 (Nunnally 1978). Our study also reached the threshold of .7 for composite reliability and Cronbach's Alpha (α) which indicates internal consistency of all items (Nunnally 1978). Regarding AVE, our results exceeded the threshold of .5 (Fornell and Larcker 1981). Thus, convergent validity was ensured for both measurement models. Regarding discriminant validity, our study fulfilled the heterotrait-monotrait ratio (HTMT) for both measurements. Discriminant validity was established between the constructs as the HTMT values are below .90 (Henseler et al. 2015). In summary, our data analysis shows that convergent and discriminant validity were met for both samples.

7.4.2 Measurement Invariance

To analyze the moderating effect of culture on the organizational readiness factors for AI and to examine cultural differences between GER and the US, we conducted an MGA. The PLS-MGA procedure was used to compare the path coefficients between the two countries (Henseler et al. 2009, pp. 308–309). To ensure that the same constructs are measured in both groups, we tested measurement invariance by using the MICOM procedure and followed the three-step approach of (1) configural invariance, (2) compositional invariance, and (3) equality of composite's mean values and variances (Henseler et al. 2016)). Based on our results, we were able to ensure configural and compositional invariance. With respect to step 3, we assessed the equality of the composites' mean values and variances between GER and the US. This condition holds for all constructs except for PF, UPS, and DQ which slightly fall out of the range. Thus, the measurement invariance is partially fulfilled and allows us to proceed with the MGA.

7.4.3 Results of Multi-Group Analysis

According to our results, our dependent variable explained 19% of variance in AI adoption which represents an adequate explanatory power. By examining uncertainty avoidance, we identified a significant difference between the two countries in AI-process fit. The positive effect of AI-process fit on AI adoption is stronger in GER than in the US (H1, p = .050). Thus, H1 is supported. With respect to long-term orientation, our results revealed a significant difference on the effect of financial resources on AI adoption. In this vein, the positive effect of financial resources on AI adoption is stronger in the US than in GER (H2, p = .037). Thus, H2 is supported. By further analyzing long-term orientation, we found no significant difference between the two countries regarding upskilling (H3, p = .118). Thus, we cannot confirm H3. In addition, we discovered that the positive effect of collaborative work on AI adoption is stronger in GER than in the US due to individualism (H4, p = .037). Thus, we confirm H4. Finally, we also observed a stronger effect of data quality on AI adoption in GER than in the US (H5, p = .047) due to uncertainty avoidance. Thus, H5 is supported.

7.5 Discussion

AI-Process Fit (PF): According to our results, the positive effect of AI-process fit on AI adoption is stronger in GER than in the US. This finding is in line with the cultural dimension of uncertainty avoidance since the higher score in GER (65) indicates that these organizations are not predestined in dealing with uncertain and unpredictable situations compared to the US (46). This means that in a GER (higher level of uncertainty avoidance), the alignment between AI processes and the organization's needs and practices has a more influence on AI adoption. Given their cultural inclination towards reducing uncertainty, organizations in GER are more likely to adopt AI applications when they fit well with their existing business processes. Conversely, in the US, where there is a lower level of uncertainty avoidance, the influence of AI-process fit on AI adoption is weaker. This finding indicates that organizations in the US may be more willing to adopt AI technologies even if there is not a perfect alignment with their existing processes, reflecting a greater tolerance for uncertainty. Financial Resources (FR): Given the significant discrepancy in long-term orientation scores between GER (83) and the US (26), the result suggests a notable cultural difference in AI adoption. It indicates that countries with lower long-term orientation scores, such as the US, tend to view AI adoption as an opportunity for immediate returns and efficiencies rather than prioritizing long-term

growth and strategic investments in AI infrastructure, as observed in countries like GER. These results could shape the perception of AI in diverse cultural contexts. The way AI is perceived within organizations can differ significantly across cultures. Cultures characterized by a high long-term orientation may regard AI as a strategic catalyst for long-term growth, whereas cultures with a lower long-term orientation may perceive it primarily as a tool for attaining immediate efficiency improvements. Upskilling (UPS): In contrast to our expectation, our results showed no significant difference between GER and the US in the effect of upskilling on AI adoption. A possible explanation could be rooted in the realities of today's globalized world, where the abundance of talent and expertise frequently surpasses national borders. In both GER and the US, organizations enjoy access to a vast global talent pool. Consequently, these organizations tend to adopt comparable approaches to upskilling initiatives as they strive to maintain competitiveness on a worldwide level. Collaborative Work (CW): Our results revealed that the positive effect of collaborative work on AI adoption is stronger in GER than in the US which is in line with the cultural dimension of individualism. The lower score of individualism in GER (67) compared to the US (91) implies that such cultures favor close collaboration between functional and data science teams and show a stronger inclination toward collective efforts and teamwork. Collaborative work is highly valued in such cultures, as it aligns with the collective goals and harmonious working environments that are characteristic of collectivist societies. On the contrary, the US has one of the highest scores in individualism (91) and, therefore, tends to have a high degree of independence and autonomy in decision-making. The cultural preference for individual initiatives and achievements might result in a somewhat weaker association between collaborative work and AI adoption in the US. Data Quality (DQ): The level of uncertainty avoidance in a culture can influence how organizations perceive and prioritize data quality in the context of AI adoption. High uncertainty avoidance cultures are likely to be more demanding of data quality due to their risk-averse nature, potentially moderating the impact of data quality on AI adoption.

7.6 Limitations and Implications

While previous IS research lacks empirical cross-cultural studies on AI adoption, our study seeks to combine Hofstede's (2001) cultural framework with the organizational readiness concept for AI. While examining cross-cultural dynamics on AI adoption by using Hofstede's (2001) cultural dimensions, we found cultural differences between GER and the US. Despite these valuable insights, our study is subject to several limitations which,

however, present opportunities for future research. First, even though the study was conducted in two Western countries, this selection may have influenced our findings and could have biased the role of culture. To reduce the risk of bias, researchers could select multiple countries and increase cultural diversity by including non-western countries. Second, given the relatively modest disparity in the power distance dimension score between GER and the US, we have not considered its influence in our analysis. It is important to note that while power distance could potentially impact the adoption of innovations, as suggested by researchers such as Yeniyurt and Townsend (2003), other studies, including the work of Png et al. (2001), have not consistently identified a significant influence. Consequently, we propose that future research delve into the effect of power distance on organizational readiness, as this aspect remains a valuable avenue. Third, the scope of the organizational readiness concept introduced by Jöhnk et al. (2021) is limited. While we have embarked upon an initial exploration of this framework, it is essential to acknowledge that our analysis did not encompass all 18 factors that constitute the organizational readiness concept. Our study, therefore, represents a preliminary step in this direction. We encourage researchers to undertake more extensive empirical studies to validate the full spectrum of organizational readiness factors.

The theoretical contribution of this paper is threefold. First, this study responds to the call for research to provide insights into cross-cultural dynamics on innovation adoption and the interaction of national and organizational cultural values (Leidner and Kayworth 2006; Srite and Karahanna 2006). By combining Hofstede's (2001) cultural framework with the organizational readiness concept for AI (Jöhnk et al. 2021), we were able to contribute to the discussion on how culture influences AI adoption. Rather than solely reporting country-specific discrepancies, we focused on relating these differences to Hofstede's (2001) cultural dimensions. Second, recent research on organizational readiness and AI adoption is mainly based on a qualitative research design on an individual level to set the theoretical basis (Jöhnk et al. 2021; Pumplun et al. 2019). There is a lack of quantitative studies on organizational level which evaluates the effect of cultural differences on AI adoption. We applied a quantitative research design to validate the qualitative findings and provide evidence of the moderating role of culture.

The study provides practical contributions for organizations. To ensure successful AI adoption, our study helps managers to identify appropriate organizational readiness factors relevant to the culture by which their organizations is managed. In summary, our findings

provide guidance on how to manage AI adoption in an intercultural environment and improve organizational efficiency. For instance, in cultures characterized by a high level of uncertainty avoidance, such as GER, organizations should prioritize aligning AI processes with their existing practices. Conversely, in cultures with lower uncertainty avoidance, such as the US, organizations may be more open to AI adoption even if there is not a perfect alignment with their existing processes, reflecting a greater tolerance for uncertainty. The significant difference in long-term orientation scores between GER and the US suggests that countries with lower scores, such as the US, may view AI adoption as an opportunity for immediate returns and efficiencies. In contrast, countries with higher, such as GER, prioritize long-term growth and strategic investments in AI infrastructure. Managers should align their AI strategies with the cultural orientation of their respective countries. Understanding the cultural context can help organizations determine whether to focus on short-term gains or invest in long-term AI capabilities. In cultures with lower individualism scores like GER, promote close collaboration between teams. In contrast, in highly individualistic cultures like the US, prioritize individual initiatives and autonomy in decision-making over collaboration. Collaborative work's effectiveness in driving AI adoption can vary based on cultural individualism or collectivism.

8 Dissertation Contributions and Conclusion

This dissertation examines the dilemma between privacy protection and value creation. Companies utilize ML to enhance their digital services and offer personalized services. However, effective algorithm training requires the collection of customers' personal information. Yet, such extensive data gathering raises significant privacy concerns among costumers. Increased privacy concerns, in turn, dissuade customers from sharing their personal information. As a result, this reluctance affects the quality of data-driven digital services, which rely on sufficient data for optimal performance. Companies therefore need to design their data-driven digital services in such a way that customers' personal information is also protected. This tension presents companies with a dilemma, as the competing goals of privacy protection and value creation cannot always be reconciled simultaneously.

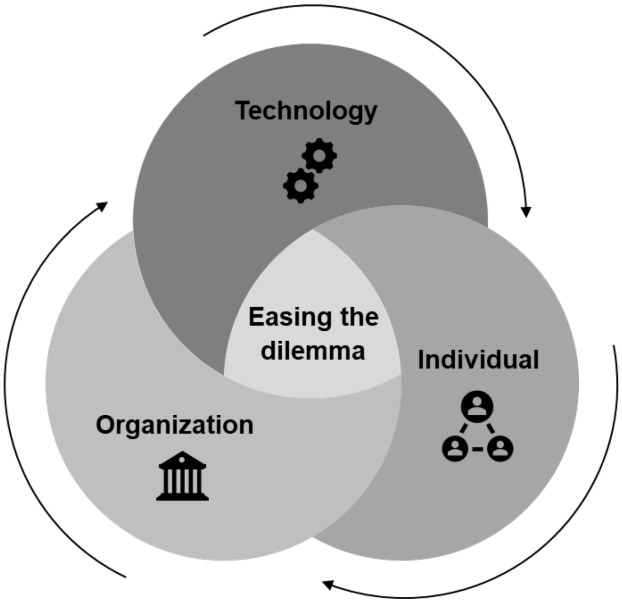

Figure 12. Easing the dilemma between privacy protection and value creation

This dissertation therefore presents three perspectives on how the dilemma can be resolved: technology, individual, and organization (see Figure 12). First, it examines

various privacy-enhancing technologies that help to minimize the collection of personal data.

It has been demonstrated that solely relying on a technological solution does not resolve the dilemma, as there are numerous barriers to implementing PETs in companies. However, the dilemma involves individuals who feel that their sense of privacy is being compromised, so it is essential to also consider the individual perspective. This perspective examines how the dilemma can be resolved by empowering individuals with greater control over their personal information. Furthermore, data-driven digital services are crafted to foster increased trust in ML-based services among individuals. In addition to addressing the individual perspective, I also explore the organizational viewpoint in designing data-driven digital services. This organizational perspective examines how companies can strategically design data-driven digital services to facilitate successful value creation processes within the context of ML adoption. It also considers that ML adoption may vary in emphasis across different cultures, prompting a cultural analysis of ML adoption. In summary, the three perspectives of technology, individual, and organization contribute to ease the dilemma between privacy protection and value creation. Based on the five included studies, I offer the following contributions to research and practice.

8.1 Theoretical Contributions

This dissertation was driven by five main RQs aimed to resolving the dilemma between privacy protection and fostering value creation processes. In this section, I discuss the theoretical contributions of this dissertation, organized around the five RQs presented in chapter 1.2. The contributions are structured around the tripartite framework that encompasses technological (PETs), individual (privacy), and organizational (value creation) perspectives.

This dissertation contributes to the literature by addressing the dilemma between privacy protection and value creation. It provides an overview of PETs (Paper A) and develops privacy-enhancing mechanisms based on theoretical concepts (e.g., Malhotra Framework and TAI Principles), aiming to enhance control over personal information (Paper B) and trust in data-driven digital services (Paper C). Consequently, this work responds to the call for research on privacy protection solutions (Acquisti et al., 2016; Bélanger & Crossler, 2011; Pavlou, 2011; Smith et al., 2011). This research shows that implementing various privacy-friendly measures can increase control and trust in data-driven digital services,

which helps reduce privacy concerns. Empirical research and theoretical analysis indicate that decreased privacy concerns are associated with a higher willingness among customers to share their personal information within digial services (Bélanger and Crossler 2011; Smith et al. 2011). Since data-driven digital services often deal with personal information, this dissertation investigates how such services should be designed to meet the needs of privacy-sensitive users. At the same time, users are in particular interested in digital services if they have a strong value proposition. ML is often the underlying technology allowing companies to create value for their users. Thus, this dissertation identifies the drivers for successfully adopting ML in digital services (Paper D). Additionally, a cross-cultural comparative study is conducted to understand which drivers of ML adoption are relevant in different cultures (Paper E). Through systematic evaluation of these drivers, this research provides novel insights into the design of strategies aimed at alleviating the dilemma between privacy protection and value creation in the digital landscape.

Technological dimension (PETs) - *RQ1: To what extent can privacy-enhancing technologies mitigate the dilemma of protecting the privacy of individuals while creating value for businesses in the context of data-driven digital services?*

In response to RQ1, this dissertation offers an examination of the current landscape concerning the utilization of PETs in negotiating the intricate balance between protecting privacy and promoting value creation (Gerlach et al. 2019; Gimpel et al. 2018; Karwatzki et al. 2022; Schneider et al. 2017). Organizations possess many of technological solutions at their disposal to address this crucial dilemma (van Blarkom et al. 2003; Burkert 1997; Deswarte and Aguilar Melchor 2006; Goldberg 2003, 2008; Goldberg et al. 1997; Oppliger 2005; Rossnagel et al. 2010; Seničar et al. 2003; Tavani 2000). However, paper A demonstrates numerous barriers that underscore the inherent complexity of achieving this balance solely through technological intervention. Notably, a significant barrier arises from the inherent dilemma between preserving individuals' privacy and upholding the accuracy of data analysis processes (D'Acquisto et al. 2015). For instance, data mining techniques are highly reliant on the accuracy of the data they analyze. One significant challenge arises when users intentionally provide incorrect information due to privacy concerns. This issue is particularly prevalent in digital services where customers are asked to share personal information. To mitigate this problem, companies typically assure users that their data will be anonymized using various techniques outlined in statistical database literature. Despite these assurances, modern users tend to be skeptical about data privacy promises made by

companies. Therefore, it is crucial to prioritize privacy protection right from the point of data collection, directly at the user's end (Agrawal et al. 2009). Consequently, this dissertation emphasizes that the deployment of technological solutions is insufficient to fully resolve the dilemma effectively. Instead, paper A uncovers the crucial need for integrating additional dimension that consider individuals' and organizations' perspectives to effectively mitigate the dilemma between privacy protection and value creation.

Individual dimension (privacy) - *RQ 2.1: How does an individual's ability to control over their personal* information *influence privacy concerns within digital services?*

RQ 2.2: To what extent does trust contribute to protect individuals' privacy and encouraging users to engage with data-driven digital services?

Previous research to protect customer data primarily concentrated on organizational strategies (cp. section 2.3) (Angelopoulos et al. 2021; Gerlach et al. 2019; Gimpel et al. 2018; Karwatzki et al. 2022; Schneider et al. 2017; Wang et al. 2021). This research goes one step further by delving into the empowerment of individuals to control and manage their personal information. Thus, papers B and C adopt an user-centered perspective to alleviate the dilemma between privacy protection and value creation. Furthermore, previous literature highlights the information asymmetry between customers and digital service providers. This means that costumers are uncertain about how companies handle their personal information (Acquisti et al. 2016). Consequently, costumers have increased privacy concerns, leading them to withhold their personal information (Acquisti et al. 2016; Bélanger and Crossler 2011; Smith et al. 2011). This research is contributing to the development of PETs that give individuals greater control over their personal information. By giving individuals more control over how others handle their personal information, these control-centered mechanisms aim to reduce the information asymmetry. This allows customers to clearly communicate how their personal information should be treated, particularly when the digital services base on ML. With more control over the handling of personal information, customers experience fewer privacy concerns, making them more willing to share their data and thus minimizing the potential thread of inaccurate personal information that could reduce the quality of data-driven digital services. Thus, this research answers RQ 2.1.

In addition, previous research has primarily focused on privacy concerns arising from the collection of personal data by companies. For example, personal data are used to train ML models, which in turn provides higher quality recommendations. However, this extensive

collection of customer data leads to privacy concerns among customers, causing them to share less data, which can potentially lead to a decline in digital service quality. This dissertation broadens the perspective on the problem by showing that privacy concerns can arise not only from companies collecting personal data, but also from peers (Zhang et al., 2022). In particular, in digital services provided by companies, users also share data with each other. As a result, this data ends up not only on the company's servers, but also in the hands of peers who can use it as they wish, without regulation. This exacerbates the aforementioned dilemma, as privacy concerns may arise not only from companies, but also from peers. This dissertation extends the existing literature by showing that privacy concerns can arise not only from corporate practices, but also from peer-to-peer exchanges of personal information. In addition to demonstrating that peer-to-peer privacy concerns can exacerbate the dilemma, this dissertation offers a design science-based solution to mitigate peer privacy concerns and give individuals more control over their data. This approach aims to raise awareness of how personal data is handled and ultimately reduce the dilemma by giving individuals a clearer understanding and greater control over their personal data. This addresses RQ 2.1.

Previous research has found that building trust in complex technologies is challenging (McKnight et al. 2002, 2011). This is especially true for digital services based on ML, as ML is often discussed in the literature as complex and as a black box (Adadi and Berrada 2018; Peters et al. 2020; Rudin 2019). This implies that even experts may not always comprehensively grasp how ML systems generate recommendations. The opaque nature of ML systems is particularly problematic if they include customers' personal information since it is unclear how the personal information are used to infer knowledge (Berente et al. 2021; Dinev and Xu 2022). Overall, this research enhance the understanding of how to design data-driven digital services using the design science methodology, with the goal of establishing and maintaining customer trust when processing their personal information. It has been observed that involving costumers in the development of ML systems strengthens trust in these systems and, consequently, in data-driven digital services. This research supports the recommendation that a "human-in-the-loop" approach is advisable for the development of data-driven digital services. Thus, this research contributes to research by suggesting how ML systems should be designed and, importantly, how customers can be involved when processing their personal information. Thus, this research answers RQ 2.2.

Organizational dimension (value creation) - *RQ3.1: What are the key factors driving or inhibiting the adoption of machine learning in data-driven digital services?*

RQ3.2: How do cultural dimensions affect the adoption of artificial intelligence in data-driven digital services, and what role do cultural nuances play in influencing decision making when developing and deploying artificial intelligence in different cultures?

Finally, I shift the focus to organizations to position the next contribution. In this dissertation, I demonstrate the factors organizations should prioritize when establishing digital services based on ML. Through empirical study, I highlight the significant factors contributing to ML system adoption, addressing the calls for research (Jöhnk et al. 2021; Pumplun et al. 2019). While the adoption of technologies has been widely studied (Venkatesh et al. 2003), ML presents specific characteristics and requirements that require a thorough examination of the driving factors influencing its adoption (cp. subchapter 2.2.3). Based on these identified factors, value creation processes can be designed to fully leverage the potential of ML to enhance service quality and provide personalized experiences for customers. Thus, this contribution addresses RQ 3.1. Furthermore, the intercultural multigroup analysis demonstrates the differential impact of these factors across different cultures. Thus, this contribution addresses RQ 3.2.

This dissertation delves deeper into the dilemma between privacy protection and harnessing ML for organizational value creation from three distinct angles. By exploring these perspectives, it becomes evident that achieving a balance between these seemingly conflicting objectives is a multifaceted challenge. Motivated by the insights gained from these perspectives, this dissertation calls for the advancement of a multilevel theoretical framework. This framework seeks to provide a holistic understanding of the complex dynamics at play, offering a structured approach to balancing privacy protection and value creation. By integrating insights from technology, individual behaviors, and organizational strategies, this theoretical framework aims to pave the way for more nuanced and effective solutions to navigate the intricate landscape of privacy and value creation in the context of ML.

8.2 Practical Contributions

In addition to the specified research contributions, this dissertation extends its value by offering practical recommendations for practitioners. Specifically, it presents valuable insights for the following key groups: (1) managers seeking to integrate PETs, (2)

designers tasked with development of PETs tailored to facilitate privacy-centric decision-making, (3) individuals, who want to protect their privacy, and (4) managers aiming to incorporate ML into their value creation processes.

(1) Given the challenges outlined in the barriers to the adoption of PETs (Paper A), the paper offers practical guidance for managers to address the integration pitfalls associated with PET implementation. By providing a transparent overview of these hurdles, managers can focus on strategies to mitigate these challenges effectively. For instance, PETs are inherently complex due to their mathematical foundations. To address this complexity, managers can invest in employees education and training programs aimed at improving awareness and understanding of PETs. By enhancing knowledge and proficiency in PETs, employees can better navigate and utilize these technologies in their respective roles. Furthermore, it is essential to recognize that PETs can be computationally intensive (Dwork 2006). To mitigate this challenge, managers should consider implementing strategies to optimize computational resources and streamline processing workflows. This could involve leveraging cloud computing infrastructure or adopting parallel processing techniques to improve efficiency and reduce computational overhead. Additionally, managers must be aware of the potential risks associated with PET adoption, such as the risk of significant loss of accuracy in analyses (D'Acquisto et al. 2015). To address this concern, managers should carefully evaluate the impact of PETs on data analysis processes and develop strategies to minimize any adverse effects on analytical outcomes. This may involve refining data preprocessing techniques, optimizing algorithm parameters, or exploring alternative modeling approaches to maintain analytical accuracy while preserving privacy.

(2) Building upon the insights from papers B and C, this research offers practical guidance for PET designers to develop systems that prioritize the end user perspective and integrate privacy-friendly design principles, particularly in the context of digital services utilizing ML. Paper B emphasizes the importance of designing systems that protect individual data related to peers in digital services, particularly in scenarios involving data sharing among peers. By leveraging the findings from paper B, designers can implement robust privacy mechanisms that safeguard personal information while facilitating seamless peer interactions. This can be achieved by giving the end users more control over their personal information. Paper C explores the domain of personal information undergoing processing by learning algorithms. Designers can utilize the design principles delineated in paper C to

craft systems that delicately balance personalized service delivery with user privacy. By doing so, designers can establish systems that foster trust among individuals. This might involve integrating privacy mechanisms that align with prevailing data privacy regulations. For instance, to empower end users, organizations could include a feature that allows users to permanently delete their data, thereby reducing the exposure of sensitive user information to learning algorithms.

(3) The research papers B and C, offer practical insights to individuals seeking to protect their personal information within data-driven digital services. These papers specifically address data shared by others about individuals and personal information utilized by learning algorithms. Through these studies, individuals can expand their awareness and understand the options available for safeguarding their personal information. Once this awareness is established, individuals can make informed decisions and only disclose the data they choose to share. This can help alleviate individuals' privacy concerns, build trust in data-driven digital services, and enhance value creation processes based on a user-centric approach.

(4) The research papers D and E, offer valuable insights for managers struggling with the challenge of successfully adopting ML that drive value creation processes, such as deriving patterns of individuals and offering personalized services. These papers shed light on the key drivers and barriers to the adoption of ML, including cultural factors. For example, process compatibility has emerged as a significant driver factor. Given that ML introduces new characteristics like autonomy, existing business processes must be aligned with this new technology. My papers also illuminate how the adoption of ML varies across different cultures, with distinct approaches and priorities. For instance, in cultures with a high level of uncertainty avoidance, such as Germany, organizations should prioritize aligning ML processes with existing practices. Conversely, in cultures with lower uncertainty avoidance, such as the United States, organizations may be more open to ML adoption even if there is not a perfect alignment with current processes, reflecting a greater tolerance for uncertainty. Ultimately, paper E provides insights into the cultural differences in adoption and assist managers involved in global projects in better understanding and managing these variances. By recognizing and navigating cultural nuances, managers can enhance the success of their ML adoption initiatives and effectively drive value creation processes on a global scale.

8.3 Conclusion

In this dissertation, I aim to unfold the dilemma between safeguarding individuals' privacy and fostering value creation within organizations. To dissect this dilemma comprehensively, I conducted five studies, each offering unique insights into the multifaceted nature of the issue along three distinct angles: technological, individual, and organizational perspective.

Exploring the technological perspective, I uncovered PETs designed to shield individuals' personal information in data-driven digital services. However, it became evident that relying solely on technological solutions cannot fully address the complexities of this dilemma, given the many barriers to the adoption of such technologies (Paper A).

Expanding the focus, I delved into how individuals themselves can play a pivotal role in safeguarding their personal information within data-driven digital services. Through the development of user-centered digital services, I demonstrated how individuals can exercise greater control over their data (Paper B). Especially within data-intensive environments where technologies such as ML are utilized to derive inferred knowledge, the increased data processing involved frequently raises privacy concerns among individuals. In response to this challenge, I developed user-centered solutions specifically tailored to enhance trust in digital services relying on ML. (Paper C).

Lastly, I scrutinized the third perspective, analyzing the factors and obstacles influencing the adoption of ML in value creation processes (Paper D). In doing so, I also considered cultural differences, recognizing their impact on the adoption and integration of such technologies (Paper E).

In summary, this dissertation sheds light on the diverse perspectives essential for mitigating the dilemma between privacy protection and value creation within organizations. Through this nuanced examination, I offer fundamental insights that can guide both research and practice in navigating this intricate landscape. The dissertation calls for the advancement of a multilevel theoretical framework, integrating insights from technology, individual behaviors, and organizational strategies. This structured approach aims to ease the dilemma between protecting individual privacy and promoting organizational value creation.

References

Acemoglu, D., Anderson, G. W., Beede, D. N., Buffington, C., Childress, E. E., Dinlersoz, E., Foster, L. S., Goldschlag, N., Haltiwanger, J. C., Kroff, Z., Restrepo, P., and Zolas, N. 2022. "Automation and the Workforce: A Firm-Level View from the 2019 Annual Business Survey," Nber Working Paper Series, Cambridge.

Ackerman, M. S. 2004. "Privacy in Pervasive Environments: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing* (8:6), pp. 430–439. (https://doi.org/10.1007/s00779-004-0305-8).

Acquisti, A. 2002. "Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments," in *Proceedings of the 4th International Conference on Ubiquitous Computing*, Göteborg, Sweden.

Acquisti, A., Friedman, A., and Telang, R. 2006. "Is There a Cost to Privacy Breaches? An Event Study," in *Proceedings of the 27th International Conference on Information Systems*, Milwaukee, Wisconsin, USA. (https://aisel.aisnet.org/icis2006/94/).

Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26–33.

Acquisti, A., Taylor, C., and Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (54:2), American Economic Association, pp. 442–492. (https://doi.org/10.1257/jel.54.2.442).

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.-A., and Bourka, A. 2015. "Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics," The European Union Agency for Network and Information Security (ENISA).

Adadi, A., and Berrada, M. 2018. "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," *IEEE Access* (6:2018), Institute of Electrical and Electronics Engineers Inc., pp. 52138–52160. (https://doi.org/10.1109/ACCESS.2018.2870052).

Adler, R. F., Paley, A., Li Zhao, A. L., Pack, H., Servantez, S., Pah, A. R., Hammond, K., and Consortium, S. O. 2023. "A User-Centered Approach to Developing an AI System Analyzing U.S. Federal Court Data," *Artificial Intelligence and Law* (31:3), Institute for Ionics, pp. 547–570. (https://doi.org/10.1007/s10506-022-09320-z).

Adomavicius, G., and Tuzhilin, A. 2005. "Personalization Technologies: A Process-Oriented Perspective," *Communications of the ACM* (48:10), pp. 83–90. (https://doi.org/Doi 10.1145/1089107.1089109).

Afiouni, R. 2019. "Organizational Learning in the Rise of Machine Learning," in *Proceedings of the 40th Conference on Information Systems*, Munich, Germany. (https://aisel.aisnet.org/icis2019/business_models/business_models/2/).

Agrawal, S., Haritsa, J. R., and Prakash, B. A. 2009. "FRAPP: A Framework for High-Accuracy Privacy-Preserving Mining," *Data Mining and Knowledge Discovery* (18:1), pp. 101–139. (https://doi.org/10.1007/s10618-008-0119-9).

Ajzen, I. 1985. "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control*, J. Kuhl and J. Beckmann (eds.), Springer, Berlin, Heidelberg, pp. 11–39. (https://doi.org/10.1007/978-3-642-69746-3_2).

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211. (https://doi.org/10.1016/0749-5978(91)90020-T).

Alsheiabni, S., Cheung, Y., and Messom, C. 2019. "Factors Inhibiting the Adoption of Artificial Intelligence at Organizational-Level: A Preliminary Investigation," in *Proceedings of 25th Americas Conference on Information Systems*, Cancún, Mexico, pp. 1–10. (https://aisel.aisnet.org/amcis2019/adoption_diffusion_IT/adoption_diffusion_IT/2/).

Altmann, I. 1975. "The Environment and Social Behavior: Privacy Personal Space Territory and Crowding," *Brooks/Cole Pub. Co., Monterey, CA.*

Alyoussef, I. Y., and Al-Rahmi, W. M. 2022. "Big Data Analytics Adoption via Lenses of Technology Acceptance Model: Empirical Study of Higher Education," *Entrepreneurship and Sustainability Issues* (9:3), Entrepreneurship and Sustainability Center, pp. 399–413. (https://doi.org/10.9770/jesi.2022.9.3(24)).

Amershi, S., Weld, D., Vorvoreanu, M., Fourney, A., Nushi, B., Collisson, P., Suh, J., Iqbal, S., Bennett, P. N., Inkpen, K., Teevan, J., Kikin-Gil, R., and Horvitz, E. 2019. "Guidelines for Human-AI Interaction," in *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, Association for Computing Machinery. (https://doi.org/10.1145/3290605.3300233).

Angelopoulos, S., Brown, M., McAuley, D., Merali, Y., Mortier, R., and Price, D. 2021. "Stewardship of Personal Data on Social Networking Sites," *International Journal of Information Management* (56:February). (https://doi.org/10.1016/j.ijinfomgt.2020.102208).

Anonymous Reddit User. 2020. "Not Wanting My Friends to Post Pictures of Me Without My Permission?," *Reddit*. (https://www.reddit.com/r/AmItheAsshole/comments/ez8q4s/aita_for_not_wanting_my_friends_to_post_pictures/, accessed April 25, 2022).

Apple. 2022. "Use Sharing Suggestions in Photos." (https://support.apple.com/en-us/HT209035, accessed April 25, 2022).

Ardolino, M., Rapaccini, M., Saccani, N., Gaiardelli, P., Crespi, G., and Ruggeri, C. 2018. "The Role of Digital Technologies for the Service Transformation of Industrial Companies," *International Journal of Production Research* (56:6), Taylor and Francis Ltd., pp. 2116–2132. (https://doi.org/10.1080/00207543.2017.1324224).

Auxiert, B., and Anderson, M. 2021. "Social Media Use in 2021," *Pew Research Center*. (https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/, accessed April 26, 2022).

Auxiert, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., and Turner, E. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." (https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/, accessed April 26, 2022).

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., Bonnefon, J. F., and Rahwan, I. 2018. "The Moral Machine Experiment," *Nature* (563), pp. 59–64. (https://doi.org/10.1038/s41586-018-0637-6).

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13–28. (https://doi.org/10.2307/25148715).

Ba, S., and Pavlou, P. A. 2002. "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior," *MIS Quarterly* (26:3),

Management Information Systems Research Center, pp. 243–268. (https://doi.org/10.2307/4132332).

Bachlechner, D., La Fors, K., and Sears, A. M. 2018. "The Role of Privacy-Preserving Technologies in the Age of Big Data," *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy*, San Francisco, California, USA. (https://aisel.aisnet.org/wisp2018/28).

Bahadir, B., and Bahadir, S. C. 2020. "Financial Development and Country-Level Advertising Spending: The Moderating Role of Economic Development and National Culture," *Journal of International Marketing* (28:3), SAGE Publications Ltd, pp. 3–20. (https://doi.org/10.1177/1069031X20936278).

Baines, T., Ziaee Bigdeli, A., Bustinza, O. F., Shi, V. G., Baldwin, J., and Ridgway, K. 2017. "Servitization: Revisiting the State-of-the-Art and Research Priorities," *International Journal of Operations and Production Management* (37:2), Emerald Group Publishing Ltd., pp. 256–278. (https://doi.org/10.1108/IJOPM-06-2015-0312).

Baker, J. 2011. "The Technology–Organization–Environment Framework," in *Information Systems Theory: Explaining and Predicting Our Digital Society* (Vol. 28), Y. K. Dwivedi, M. R. Wade, and S. L. Schneberger (eds.), Springer, New York, NY, pp. 231–245. (https://doi.org/10.1007/978-1-4419-6108-2_12).

Bakis, R., Connors, D. P., Dube, P., Kapanipathi, P., Kumar, A., Malioutov, D., and Venkatramani, C. 2017. "Performance of Natural Language Classifiers in a Question-Answering System," *IBM Journal of Research and Development* (61:4), pp. 1–10. (https://doi.org/10.1147/JRD.2017.2711719).

Baldauf, M., Fröehlich, P., and Endl, R. 2020. "Trust Me, I'm a Doctor-User Perceptions of AI-Driven Apps for Mobile Health Diagnosis," in *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*, Association for Computing Machinery, November 22. (https://doi.org/10.1145/3428361.3428362).

Bansal, G., and Gefen, D. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation Recommended Citation," in *Proceedings of the 29th International Conference on Information Systems* (Vol. 7). (http://aisel.aisnet.org/icis2008/7).

Bansal, G., Zahedi, F., 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), Palgrave, pp. 624–644. (https://doi.org/10.1057/ejis.2014.41).

Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138–150. (https://doi.org/10.1016/j.dss.2010.01.010).

Bansal, G., Zahedi, F. M., and Gefen, D. 2016. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online," *Information and Management* (53:1), pp. 1–21. (https://doi.org/10.1016/j.im.2015.08.001).

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp. 99–120. (https://doi.org/10.1177/014920639101700108).

Baskerville, R. L., Kaul, M., and Storey, V. C. 2015. "Genres of Inquiry on Design-Science Research: Justification and Evaluation of Knowledge Production," *MIS Quarterly* (39:3), pp. 541–564.

Bean, R. 2018. "The State of Machine Learning in Business Today." (https://www.forbes.com/sites/ciocentral/2018/09/17/the-state-of-machine-learning-in-business-today/).

Bedué, P., and Fritzsche, A. 2022. "Can We Trust AI? An Empirical Investigation of Trust Requirements and Guide to Successful AI Adoption," *Journal of Enterprise*

Information Management (35:2), Emerald Publishing Limited, pp. 530–549. (https://doi.org/10.1108/JEIM-06-2020-0233).

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017–1042. (https://doi.org/10.2307/41409971).

Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. *Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes*. (https://doi.org/10.1016/S0963-8687(02)00018-5).

Bélanger, F., and James, T. L. 2020. "A Theory of Multilevel Information Privacy Management for the Digital Era," *Information Systems Research* (31:2), pp. 510–536. (https://doi.org/10.1287/isre.2019.0900).

Benbya, H., Pachidi, S., and Jarvenpaa, S. L. 2021. "Artificial Intelligence in Organizations: Implications for Information Systems Research," *Journal of the Association for Information Systems* (22:2), pp. 281–303. (https://doi.org/10.17705/1jais.00662).

Benbya, H., Strich, F., and Tamm, T. 2024. "Navigating Generative Artificial Intelligence Promises and Perils for Knowledge and Creative Work," *Journal of the Association for Information Systems* (25:1), Association for Information Systems, pp. 23–36. (https://doi.org/10.17705/1jais.00861).

Benenson, Z., Girard, A., and Krontiris, I. 2015. "User Acceptance Factors for Anonymous Credentials: An Empirical Investigation," in *Workshop on the Economics of Information Security*, Delft, Niederlande.

Berente, N., Gu, B., Recker, J., and Santhanam, R. 2021. "Managing Artificial Intelligence," *MIS Quarterly* (45:3), pp. 1433–1450. (https://doi.org/10.25300/MISQ/2021/16274).

Berg, M. 1997. *Rationalizing Medical Work: Decision-Support Techniques and Medical Practices*, New Bakersville: MIT Press.

Besmer, A., and Lipford, H. R. 2010. "Moving Beyond Untagging: Photo Privacy in a Tagged World," in *Proceedings of the '10 Conference on Human Factors in Computing Systems*, E. Mynatt (ed.), Atlanta, Georgia, US, pp. 1563–1572. (https://doi.org/10.1145/1753326.1753560).

Beugelsdijk, S., Klasing, M. J., and Milionis, P. 2019. "Value Diversity and Regional Economic Development," *Scandinavian Journal of Economics* (121:1), Blackwell Publishing Ltd, pp. 153–181. (https://doi.org/10.1111/sjoe.12253).

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., and Venkatraman, N. 2013. "Digital Business Strategy: Toward a Next Generation of Insights," *MIS Quarterly* (37:2), pp. 471–482. (https://doi.org/10.25300/MISQ/2013/37:2.3).

Biczók, G., and Chia, P. H. 2013. "Interdependent Privacy: Let Me Share Your Data," in *Financial Cryptography and Data Security. Lecture Notes in Computer Science*, AR. Sadeghi (ed.), Springer, Berlin, Heidelberg, pp. 338–353.

Bjarnadóttir, M. V., and Anderson, D. 2020. "Machine Learning in Healthcare: Fairness, Issues, and Challenges," *Journal of IEEE Transactions on Artificial Intelligence*, pp. 64–83. (https://doi.org/10.1287/educ.2020.0220).

van Blarkom, G., Borking, J., and Olk, J. 2003. "Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents," Den Haag, Niederlande: Privacy Incorporated Software Agent (PISA) Consortium. (https://doi.org/10.13140/2.1.4888.7688).

Bohanec, M., Robnik-Šikonja, M., and Borštnar, M. K. 2017. "Decision-Making Framework with Double-Loop Learning through Interpretable Black-Box Machine Learning Models," *Industrial Management & Data Systems* (117:7), pp. 1389–1406. (https://doi.org/10.1108/IMDS-09-2016-0409).

Böhme, R., and Koble, S. 2007. "Pricing Strategies in Electronic Marketplaces with Privacy-Enhancing Technologies," *Wirtschaftsinformatik* (49:1), pp. 16–25. (https://doi.org/10.1007/s11576-007-0004-y).

Borgman, H. P., Bahli, B., Heier, H., and Schewski, F. 2013. "Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework," in *Proceedings of the 46th Hawaii International Conference on System Sciences*, Maui, Hawaii, USA.

Boritz, J. E., and No, W. G. 2011. "E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery," *Journal of Information Systems* (25:2), American Accounting Association, pp. 11–45. (https://doi.org/10.2308/isys-10090).

Borking, J. J. 2011. "Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time," in *Computers, Privacy and Data Protection: An Element of Choice*, S. Gutwirth, Y. Poullet, P. De Hert, and R. Leenes (eds.), Dordrecht: Springer, pp. 309–341.

Borking, J. J., and Raab, C. D. 2001. "Laws, PETs and Other Technologies for Privacy Protection," *Journal of Information, Law and Technology* (1), pp. 1–14.

Brakemeier, H., Wagner, A., and Buxmann, P. 2017. "When Risk Perceptions Are Nothing but Guesses – An Evaluability Perspective on Privacy Risks," in *Proceedings of the 17th International Conference on Information Systems*, Seoul, South Korea. (https://aisel.aisnet.org/icis2017/Security/Presentations/16/).

Braun, M., Harnischmacher, C., Lechte, H., and Riquel, J. 2022. "Let's Get Physic(AI)l - Transforming AI-Requirements of Healthcare into Design Principles," in *Proceedings of the 30th European Conference on Information Systems*. (https://aisel.aisnet.org/ecis2022_rip/47).

Brecht, F., Fabian, B., Kunz, S., and Mueller, S. 2011. "Are You Willing to Wait Longer for Internet Privacy?," *Proceedings of the 19th European Conference on Information Systems*, Helsinki, Finland. (https://aisel.aisnet.org/ecis2011/236/).

Brecht, F., Fabian, B., Kunz, S., and Müller, S. 2012. "Communication Anonymizers: Personality, Internet Privacy Literacy and Their Influence on Technology Acceptance," *Proceedings of the 20th European Conference on Information Systems*, Barcelona, Spain. (https://aisel.aisnet.org/ecis2012/214/).

Brhel, M., Meth, H., Maedche, A., and Werder, K. 2015. "Exploring Principles of User-Centered Agile Software Development: A Literature Review Systematic Review Paper," *Information and Software Technology* (61:May 2015), pp. 163–181. (https://doi.org/10.1016/j.infsof.2015.01.004).

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., and Cleven, A. 2015. "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research," *Communications of the Association for Information Systems* (37:1), pp. 205–224. (https://doi.org/10.17705/1cais.03709).

Brownlow, J., Zaki, M., Neely, A., and Urmetzer, F. 2015. "Data and Analytics - Data-Driven Business Models: A Blueprint for Innovation," *Cambridge Service Alliance*.

Brush, A. J. B., Krumm, J., and Scott, J. 2010. "Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location," *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, Copenhagen, Denmark. (https://doi.org/10.1145/1864349.1864381).

Brynjolfsson, E., Hitt, L., and Kim, H. 2011. "Strength in Numbers: How Does Data-Driven Decision-Making Affect Firm Performance?," in *Proceedings of the 32nd International Conference on Information Systems*, Shanghai, China. (https://aisel.aisnet.org/icis2011/proceedings/economicvalueIS/13/).

Brynjolfsson, E., and Mitchell, T. M. 2017. "What Can Machine Learning So? Workforce Implications," *Science* (358:6370), pp. 1530–1534. (https://doi.org/10.1126/science.aap8062).

Brynjolfsson, E., Rock, D., and Syverson, C. 2017. "Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics," *Nber Working Paper Series*.

Buck, C., Hennrich, J., and Lina Kauffmann, A. 2021. "Artificial Intelligence in Radiology – A Qualitative Study on Imaging Specialists' Perspectives," in *Proceedings of the 42nd International Conference on Information Systems* (Vol. 20). (https://aisel.aisnet.org/icis2021/is_health/is_health/20).

Bulger, M., Taylor, G., and Schroeder, R. 2014. "Data-Driven Business Models: Challenges and Opportunities of Big Data," *Oxford Internet Institute*.

Burkert, H. 1997. "Privacy-Enhancing Technologies: Typology, Critique, Vision," in *Technology and Privacy*, P. E. Agre and M. Rotenberg (eds.), Cambridge, Massachusetts, USA: MIT Press, pp. 125–142.

Cao, M., Vonderembse, M. A., Zhang, Q., and Ragu-Nathan, T. S. 2010. "Supply Chain Collaboration: Conceptualisation and Instrument Development," *International Journal of Production Research* (48:22), pp. 6613–6635. (https://doi.org/10.1080/00207540903349039).

Caudill, E. M., and Murphy, P. E. 2000. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy and Marketing* (19:1), pp. 7–19. (https://doi.org/10.1509/jppm.19.1.7.16951).

Cha, S. C., Hsu, T. Y., Xiang, Y., and Yeh, K. H. 2019. "Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges," *IEEE Internet of Things Journal* (6:2), pp. 2159–2187. (https://doi.org/10.1109/Jiot.2018.2878658).

Chan, Y., and Greenaway, K. 2005. "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6:6), pp. 171–198. (https://doi.org/10.17705/1jais.00068).

Chandra, S., and Kumar, K. N. 2018. "Exploring Factors Influencing Organizational Adoption of Augmented Reality in E-Commerce: Empirical Analysis Using Technology-Organization-Environment Model," *Journal of Electronic Commerce Research* (19:3), pp. 237–265.

Chao, C.-Y., Chang, T.-C., Wu, H.-C., Lin, Y.-S., and Chen, P.-C. 2016. "The Interrelationship Between Intelligent Agents' Characteristics and Users' Intention in a Search Engine by Making Beliefs and Perceived Risks Mediators," *Computers in Human Behavior* (64), pp. 117–125. (https://doi.org/10.1016/j.chb.2016.06.031).

Chen, D., and Hahn, J. 2020. "Impact of End-User Privacy Enhancing Technologies (PETs) on Firms' Analytics Performance," *Proceedings of the 40th International Conference on Information Systems*. (https://aisel.aisnet.org/icis2020/digital_commerce/digital_commerce/3/).

Chen, H. C., Chiang, R. H. L., and Storey, V. C. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* (36:4), pp. 1165–1188. (https://doi.org/10.2307/41703503).

Chen, J., Ping, J. W., Xu, Y. C., and Tan, B. C. Y. 2015. "Information Privacy Concern about Peer Disclosure in Online Social Networks," *IEEE Transactions on Engineering Management* (62:3), pp. 311–324. (https://doi.org/10.1109/TEM.2015.2432117).

Chen, J., Ping, W., Xu, Y., and Y Tan, B. C. 2009. "Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context," in *Proceedings of the 30th International Conference on Information Systems*, Phoenix, Arizona, US. (https://aisel.aisnet.org/icis2009/174/).

Chen, Y., Kreulen, J., Campbell, M., and Abrams, C. 2011. "Analytics Ecosystem Transformation: A Force for Business Model Innovation," in *Proceedings of the*

Annual SRII Global Conference, IEEE, pp. 11–20. (https://doi.org/10.1109/SRII.2011.12).

Chin, W. W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (22:1), vii–xvi.

Choi, D., Lowry, P. B., and Wang, G. A. 2020. "The Design of Personal Privacy and Security Risk Scores for Minimizing Consumers' Cognitive Gaps in IoT Settings," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, Maui, Hawaii, USA, pp. 5076–5085. (https://doi.org/10.1016/j.eswa.2012.01.201).

Chong, A. Y. L., and Chan, F. T. S. 2012. "Structural Equation Modeling for Multi-Stage Analysis on Radio Frequency Identification (RFID) Diffusion in the Health Care Industry," *Expert Systems with Applications* (39:10), pp. 8645–8654.

Chwelos, P., Benbasat, I., and Dexter, A. S. 2001. "Research Report: Empirical Test of an EDI Adoption Model," *Information Systems Research* (12:3), pp. 304–231. (https://doi.org/10.1287/isre.12.3.304.9708).

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, (2nd ed.), Hillsdale, NJ: Lawrence Erlbaum Associates.

Collins, C., Dennehy, D., Conboy, K., and Mikalef, P. 2021. "Artificial Intelligence in Information Systems Research: A Systematic Literature Review and Research Agenda," *International Journal of Information Management* (60). (https://doi.org/10.1016/j.ijinfomgt.2021.102383).

Commission, E. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union*.

Conger, S., Pratt, J. H., and Loch, K. D. 2013. "Personal Information Privacy and Emerging Technologies," *Information Systems Journal* (23:5), pp. 401–417. (https://doi.org/10.1111/j.1365-2575.2012.00402.x).

Coombs, C., Hislop, D., Taneva, S. K., and Barnard, S. 2020. "The Strategic Impacts of Intelligent Automation for Knowledge and Service Work: An Interdisciplinary Review," *Journal of Strategic Information Systems* (29:4), Elsevier B.V. (https://doi.org/10.1016/j.jsis.2020.101600).

Cooper, H. 1988. "Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews," *Knowledge in Society* (1), pp. 104–126. (https://doi.org/10.1007/BF03177550).

Cramer, R., Damgård, I., and Maurer, U. 2000. "General Secure Multi-Party Computation from Any Linear Secret-Sharing Scheme," in *Advances in Cryptology — EUROCRYPT 2000.*, B. Preneel (ed.), Springer, Berlin, Heidelberg. (https://doi.org/10.1007/3-540-45539-6_22).

Cramer, R., Damgard, I., and Nielsen, J. B. 2001. "Multiparty Computation from Threshold Homomorphic Encryption," in *Advances in Cryptology — EUROCRYPT 2001*, B. Pfitzmann (ed.), : Springer, Berlin, Heidelberg. (https://doi.org/10.1007/3-540-44987-6_18).

Cruz-Jesus, F., Pinheiro, A., and Oliveira, T. 2019. "Understanding CRM Adoption Stages: Empirical Analysis Building on the TOE Framework," *Computers in Industry* (109), pp. 1–13.

Culnan, M., and Bies, R. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323–342.

Culnan, M. J. 1995. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing* (9:2), pp. 10–19. (https://doi.org/10.1002/dir.4000090204).

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115. (https://doi.org/10.1287/ORSC.10.1.104).

Culnan, M. J., Foxman, E. R., and Ray, A. W. 2008. "Why IT Executives Should Help Employees Secure Their Home Computers," *MIS Quarterly Executive* (7:1), p. 6. (https://aisel.aisnet.org/misqe/vol7/iss1/6).

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673–687. (https://doi.org/10.2307/20650322).

Danezis, G., Lewis, S., and Anderson, R. J. 2005. "How Much Is Location Privacy Worth?," in *Proceedings of the Workshop on the Economics of Information Security Series* (Vol. 5), Citeseer.

Davenport, T. H. 2013. "Analytics 3.0," *Harvard Business Review* (91), pp. 64–72. (https://hbr.org/2013/12/analytics-30).

Davenport, T. H. 2018. "From Analytics to Artificial Intelligence," *Journal of Business Analytics* (1:2), pp. 73–80. (https://doi.org/10.1080/2573234X.2018.1543535).

Davenport, T., Kalakota, R., Davenport, T., and Kalakota, R. 2019. "The Potential for Artificial Intelligence in Healthcare," *Future Healthcare Journal* (6:2), Royal College of Physicians, pp. 94–98.

Davis, F. D. 1986. "A Technology Acceptance Model for Empirically Testing New End-User Information Systems," *Science*, Massachusetts Institute of Technology. (https://doi.org/10.1126/science.146.3652.1648).

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319–339. (https://doi.org/10.2307/249008).

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982–1003. (https://doi.org/10.1287/mnsc.35.8.982).

Demlehner, Q., and Laumer, S. 2020. "Shall We Use It or Not? Explaining the Adoption of Artifificial Intelligence for Car Manufacturing Purposes," in *Proceedings of the 28th European Conference on Information Systems*, Marrakech, Morocco, Virtual. (https://aisel.aisnet.org/ecis2020_rp/177/).

DePietro, R., Wiarda, E., and Fleischer, M. 1990. "The Context for Change: Organization, Technology and Environment," in *The Process of Technological Innovation* (4th ed.), L. G. Tornatzky and M. Fleischer (eds.), Lexington: Lexington Books, pp. 152–175.

Deswarte, Y., and Aguilar Melchor, C. 2006. "Current and Future Privacy Enhancing Technologies for the Internet," *Annals of Telecommunications* (61:3–4), pp. 399–417. (https://doi.org/10.1007/bf03219914).

Dietvorst, B. J., Simmons, J. P., and Massey, C. 2015. "Algorithm Aversion: People Erroneously Avoid Algorithms After Seeing Them Err," *Journal of Experimental Psychology* (144:1), pp. 114–126. (https://doi.org/10.2139/ssrn.2466040).

Diffie, W., and Hellman, M. E. 1976. "New Directions in Cryptography Invited Paper," *IEEE Transaction of Information Technology* (IT-22:6).

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61–80. (https://doi.org/10.1287/isre.1060.0080).

Dinev, T., McConnell, A. R., Smith, H. J., Dinev, T., Raton, B., and Smith, H. J. 2015. "Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box," *Information Systems Research* (26:4), pp. 639–655. (https://doi.org/10.1287/isre.2015.0600).

Dinev, T., and Xu, H. 2022. "Reflections on the 2021 Impact Award: Why Privacy Still Matters," *MIS Quarterly* (46:4), xx–xxxii.

Domingos, P. 2012. “A Few Useful Things to Know About Machine Learning,” *Communications of the ACM* (55:10), pp. 78–87. (https://doi.org/10.1145/2347736.2347755).

Dremel, C., Engel, C., and Mikalef, P. 2020. “Looking Beneath the Surface - Concepts and Research Avenues for Big Data Analytics Adoption in IS Research,” in *Proceedings of the 41st International Conference on Information Systems*, Hyderabad, India, Virtual. (https://aisel.aisnet.org/icis2020/implement_adopt/implement_adopt/1/).

Duan, Y., Edwards, J. S., and Dwivedi, Y. K. 2019. “Artificial Intelligence for Decision Making in the Era of Big Data – Evolution, Challenges and Research Agenda,” *International Journal of Information Management* (48), pp. 63–71. (https://www.sciencedirect.com/science/article/pii/S0268401219300581).

Dwork, C. 2006. “Differential Privacy,” in *Automata, Languages and Programming* (Vol. 4052), M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (eds.), Berlin, Heidelberg: Springer, pp. 1–12. (https://doi.org/10.1007/11787006_1).

Ebrahimi, S., and Hassanein, H. 2019. “Empowering Users to Detect Data Analytics Discriminatory Empowering Users to Detect Data Analytics Discriminatory Recommendations,” in *Proceedings of the 40th International Conference on Information Systems*. (https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/39/).

Eitle, V., and Buxmann, P. 2020. “Cultural Differences in Machine Learning Adoption: An International Comparison between Germany and the United States,” in *Proceedings of the 28th European Conference on Information Systems*, Marrakech, Morocco, Virtual. (https://aisel.aisnet.org/ecis2020_rp/138/).

Emamjome, F., and Rosemann, M. 2021a. “Managing Trust- A Design Theory and Design Principles,” in *Proceedings of the 42nd International Conference on Information Systems* . (https://aisel.aisnet.org/icis2021/dig_innov/dig_innov/22/).

Emamjome, F., and Rosemann, M. 2021b. “Managing Trust-A Design Theory and Design Principles,” in *Proceedings of the 42nd International Conference on Information Systems*. (https://aisel.aisnet.org/icis2021/dig_innov/dig_innov/22/).

Engelbrecht, A., Gerlach, J., and Widjaja, T. 2016. “Understanding the Anatomy of Data-Driven Business Models - Towards an Empirical Taxonomy,” in *Proceedings of the 24th European Conference on Information Systsms*, Istanbul, Turkey. (https://aisel.aisnet.org/ecis2016_rp/128/).

Engelen, A., Brettel, M., and Wiest, G. 2012. “Cross-Functional Integration and New Product Performance - The Impact of National and Corporate Culture,” *Journal of International Management* (18:1), pp. 52–65. (https://doi.org/10.1016/j.intman.2011.07.001).

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., and Thrun, S. 2017. “Dermatologist-Level Classification of Skin Cancer with Deep Neural Networks,” *Nature* (542:7639), Nature Publishing Group, pp. 115–118. (https://doi.org/10.1038/nature21056).

European Union. 2022. “General Data Protection Regulation.” (https://gdpr.eu/tag/gdpr/, accessed April 29, 2022).

Fang, W., Wen, X. Z., Zheng, Y., and Zhou, M. 2017. “A Survey of Big Data Security and Privacy Preserving,” *IETE Technical Review* (34:5), pp. 544–560. (https://doi.org/10.1080/02564602.2016.1215269).

Faraj, S., Pachidi, S., and Sayegh, K. 2018. “Working and Organizing in the Age of the Learning Algorithm,” *Information and Organization* (28:1), pp. 62–70. (https://www.sciencedirect.com/science/article/pii/S1471772718300277).

Feigenbaum Freedman M. Sander T. Shostack A., J. 2002. “Economic Barriers to the Deployment of Existing Privacy Technology,” *Proceedings of the Workshop on Economics and Information Security*, Berkley, CA.

Feri, F., Giannetti, C., and Jentzsch, N. 2016. “Disclosure of Personal Information under Risk of Privacy Shocks,” *Journal of Economic Behavior and Organization* (123), pp. 138–148. (https://doi.org/10.1016/j.jebo.2015.12.001).

Fichman, R. G. 2000. “The Diffusion and Assimilation of Information Technology Innovations,” in *Framing the Domains of IT Management: Projecting the FutureThrough the Past*, R. W. Zmud and R. W. Zmud (eds.), Cincinnati:

Figma. 2023. “The Modern Interface Design Tool.” (https://www.figma.com/de/).

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. C., and Srikumar, M. 2020. “Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI,” *Berkman Klein Center Research Publication*. (https://doi.org/10.2139/ssrn.3518482).

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., and Vayena, E. 2018. “AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations,” *Minds and Machines* (28:4), Springer, pp. 689–707. (https://link.springer.com/article/10.1007%2Fs11023-018-9482-5).

Fornell, C., and Larcker, D. F. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *Journal of Marketing Research* (18:1), pp. 39–50. (https://doi.org/10.2307/3151312).

Franz, A., and Benlian, A. 2022. “Exploring Interdependent Privacy – Empirical Insights into Users’ Protection of Others’ Privacy on Online Platforms,” *Electronic Markets* (32:3), pp. 1–17. (https://doi.org/10.1007/s12525-022-00566-8).

Funke, S., Wiesmaier, A., and Daubert, J. 2017. “Constrained PET Composition for Measuring Enforced Privacy,” *Proceedings of the 12th International Conference on Availability, Reliability and Security*, Reggio Calabria, Italien. (https://doi.org/10.1145/3098954.3098968).

Gan, M. F., Chua, H. N., and Wong, S. F. 2019. “Privacy Enhancing Technologies Implementation: An Investigation of Its Impact on Work Processes and Employee Perception,” *Telematics and Informatics* (38), pp. 13–29. (https://doi.org/10.1016/j.tele.2019.01.002).

Gangwar, H., Date, H., and Ramaswamy, R. 2015. “Understanding Determinants of Cloud Computing Adoption Using an Integrated TAM-TOE Model,” *Journal of Enterprise Information Management* (28:1), pp. 107–130. (https://doi.org/doi.org/10.1108/JEIM-08-2013-0065).

Gaskin, J., and Lowry, P. B. 2014. “Partial Least Squares (PLS) Structural Equation Modeling (SEM) For Building And Testing Behavioral Causal Theory: When To Choose It And How To Use It,” *IEEE Transactions on Professional Communication* (57:2), pp. 123–146. (https://doi.org/10.1109/TPC.2014.2312452).

Gefen, D., Rigdon, E. E., and Straub, D. 2011. “An Update and Extension to SEM Guidelines for Administrative and Social Science Research,” *MIS Quarterly* (35:2), ii–xiv. (https://doi.org/10.2307/23044042).

Gefen, D., Straub, D., and Boudreau, M.-C. 2000. “Structural Equation Modeling and Regression: Guidelines for Research Practice,” *Communications of the Association for Information Systems* (4:7).

Gerlach, J., Eling, N., Wessels, N., and Buxmann, P. 2019. “Flamingos on a Slackline: Companies’ Challenges of Balancing the Competing Demands of Handling Customer Information and Privacy,” *Information Systems Journal* (29:2), pp. 548–575. (https://doi.org/10.1111/isj.12222).

Gerlach, J., Scheunert, A., and Breitner, M. H. 2022. "Personal Data Protection Rules! Guidelines for Privacy-Friendly Smart Energy Services," in *Proceedings of the 30th European Conference on Information Systems*, Timisoara, Romania. (https://aisel.aisnet.org/ecis2022_rp/123/).

Gerlach, J., Widjaja, T., and Buxmann, P. 2015. "Handle with Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior," *Journal of Strategic Information Systems* (24:1), Elsevier B.V., pp. 33–43. (https://doi.org/10.1016/j.jsis.2014.09.001).

Gibney, E. 2018. "The Scant Science Behind Cambridge Analytica's Controversial Marketing Techniques," *Nature*. (https://www.nature.com/articles/d41586-018-03880-4).

Gillath, O., Ai, T., Branicky, M. S., Keshmiri, S., Davison, R. B., and Spaulding, R. 2021. "Attachment and Trust in Artificial Intelligence," *Computers in Human Behavior* (115), Pergamon. (https://doi.org/10.1016/j.chb.2020.106607).

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., and Schmied, F. 2018. "The Upside of Data Privacy – Delighting Customers by Implementing Data Privacy Measures," *Electronic Markets* (28:4), Springer Verlag, pp. 437–452. (https://doi.org/10.1007/s12525-018-0296-3).

Glikson, E., and Woolley, A. W. 2020. "Human Trust in Artificial Intelligence: Review of Empirical Research," *Academy of Management Annals* (14:2), pp. 627–660. (https://doi.org/10.5465/annals.2018.0057).

Glowalla, P., and Sunyaev, A. 2013. "Process-Driven Data Quality Management through Integration of Data Quality into Existing Process Models: Application of Complexity-Reducing Patterns and the Impact on Complexity Metric," *Business and Information Systems Engineering* (5:6), Gabler Verlag, pp. 433–448. (https://doi.org/10.1007/s12599-013-0297-x).

Goasduff, L. 2020. "2 Megatrends Dominate the Gartner Hype Cycle for Artificial Intelligence, 2020." (https://www.gartner.com/smarterwithgartner/2-megatrends-dominate-the-gartner-hype-cycle-for-artificial-intelligence-2020/).

Goduscheit, R. C., and Faullant, R. 2018. "Paths Toward Radical Service Innovation in Manufacturing Companies—A Service-Dominant Logic Perspective," *The Journal of Product Innovation Management* (35:5), pp. 701–719.

Goldberg, I. 2003. "Privacy-Enhancing Technologies for the Internet II: Five Years Later," in *Privacy Enhancing Technologies* (Vol. 2482), R. Dingledine and P. Syverson (eds.), Berlin, Heidelberg: Springer, pp. 1–12. (https://doi.org/10.1007/3-540-36467-6_1).

Goldberg, I. 2008. "Privacy-Enhancing Technologies for the Internet III: Ten Years Later," in *Digital Privacy Theory, Technologies, and Practices*, A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. De di Vimercati (eds.), Auerbach Publications, pp. 25–40.

Goldberg, I., Wagner, D., and Brewer, E. 1997. "Privacy-Enhancing Technologies for the Internet," *Proceedings of the 42nd IEEE International Computer Conference*, Washington, D.C., USA, pp. 103–109. (https://doi.org/10.1109/CMPCON.1997.584680).

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., and Zhdanov, D. 2018. "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas," *MIS Quarterly* (42:1), MIS Quarterly, pp. 143–164. (https://doi.org/10.25300/MISQ/2018/13839).

Greenaway, K. E., and Chan, Y. E. 2013. "Designing a Customer Information Privacy Program Aligned with Organizational Priorities," *MIS Quarterly Executive* (12:3), pp. 137–150.

Greenaway, K. E., Chan, Y. E., and Crossler, R. E. 2015. "Company Information Privacy Orientation: A Conceptual Framework," *Information Systems Journal* (25:6), pp. 579–606. (https://doi.org/10.1111/isj.12080).

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337–355. (https://doi.org/10.25300/MISQ/2013/37.2.01).

Gregor, S., Kruse, L., and Seidel, S. 2020. "Research Perspectives: The Anatomy of a Design Principle," *Journal of the Association for Information Systems* (21:6), Association for Information Systems, pp. 1622–1652. (https://doi.org/10.17705/1jais.00649).

Greve, M., Lichtenberg, S., Diederich, S., and Benedikt Brendel, A. 2020. "Supporting Non-Communicable Disease Prevention through a MHealth Application in Decentralized Healthcare Systems: Action Design Research in Eswatini," in *Proceedings of the 28th European Conference on Information Systems*. (https://aisel.aisnet.org/ecis2020_rp/154/).

Grover, V., and Goslar, M. D. 1993. "The Initiation, Adoption, and Implementation of Telecommunications Technologies in U.S. Organizations," *Journal of Management Information Systems* (10:1), pp. 141–163. (https://doi.org/10.1080/07421222.1993.11517994).

Guilloteau, S., and Mauree, V. 2012. "Privacy in Cloud Computing." (https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf).

Gutierrez, A., Boukrami, E., and Lumsden, R. 2015. "Technological, Organisational and Environmental Factors Influencing Managers' Decision to Adopt Cloud Computing in the UK," *Journal of Enterprise Information Management* (28:6), pp. 788–807. (https://doi.org/10.1108/JEIM-01-2015-0001).

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2016. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, (2nd ed.), Los Angeles: Sage Publications.

Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. 2012. "An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research," *Journal of the Academy of Marketing Science* (40:3), pp. 414–433. (https://doi.org/10.1007/s11747-011-0261-6).

Hair, J. S., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. 2006. *Multivariate Data Analysis*, (6th ed.), Pearson Prentice Hall.

Handrich, M. 2021. "Alexa, You Freak Me Out - Identifying Drivers of Innovation Resistance and Adoption of Intelligent Personal Assistant," in *Proceeding of the 42nd International Conference on Information Systems*. (https://aisel.aisnet.org/icis2021/is_implement/is_implement/11).

Harborth, D., Cai, X., and Pape, S. 2019. "Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym," in *ICT Systems Security and Privacy Protection* (Vol. 562), G. Dhillon, F. Karlsson, K. Hedström, and A. Zúquete (eds.), Cham: Springer, pp. 253–267.

Harborth, D., and Pape, S. 2018. "Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust," *Proceedings of the 24th Americas Conference on Information Systems*, New Orleans, USA. (https://aisel.aisnet.org/amcis2018/Security/Presentations/15/).

Harborth, D., and Pape, S. 2020. "How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor," *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* (51:1), pp. 51–69. (https://doi.org/10.1145/3380799.3380805).

Harfouche, A., Quinio, B., Skandrani, S. R., and Marciniak, R. 2017. "A Framework for Artificial Knowledge Creation in Organizations," in *Proceedings of the 38th International Conference on Information Systems*, Seoul, South Korea. (https://doi.org/https://aisel.aisnet.org/icis2017/General/Presentations/15/).

Hartmann, P. M., Zaki, M., Feldmann, N., and Neely, A. 2014. *Big Data for Big Business? A Taxonomy of Data-Driven Business Models Used by Start-up Firms*, Cambridge Service Alliance.

Hartmann, P. M., Zaki, M., Feldmann, N., and Neely, A. 2016. "Capturing Value from Big Data - A Taxonomy of Data-Driven Business Models Used by Start-up Firms," *International Journal of Operations & Production Management* (36:10), pp. 1382–1406. (https://doi.org/10.1108/Ijopm-02-2014-0098).

Hendrik, O. J., Sunday, O. O., and Oludayo, O. O. 2013. "A PET Evaluation Framework for Relational Databases," *Proceedings of the 2013 International Conference on Social Computing*, Washington, D.C., USA, pp. 612–617. (https://doi.org/10.1109/SocialCom.2013.92).

Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 115–135. (https://doi.org/10.1007/s11747-014-0403-8).

Henseler, J., Ringle, C. M., and Sarstedt, M. 2016. "Testing Measurement Invariance of Composites Using Partial Least Squares," *International Marketing Review* (33:3), pp. 405–431. (https://doi.org/10.1108/IMR-09-2014-0304).

Henseler, J., Ringle, C. M., and Sinkovics, Rudolf R. 2009. "The Use of Partial Least Squares Path Modeling in International Marketing," in *New Challenges to International Marketing (Advances in International Marketing* (Vol. 20), R.R. Sinkovics and P. N. Ghauri (eds.), Emerald Group Publishing Limited, pp. 277–319. (https://doi.org/10.1108/S1474-7979(2009)0000020014).

Hevner, A., March, S., Park, J., and Ram, S. 2004. "Research Essay Design Science in Information," *MIS Quarterly* (28:1), pp. 75–105.

Hirsch, D. D. 2014. "That's Unfair-or Is It: Big Data, Discrimination and the FTC's Unfairness Authority," *Kentucky Law Journal* (103:3), pp. 345–361. (https://uknowledge.uky.edu/klj/vol103/iss3/3/).

Hochheiser, H. 2002. "The Platform for Privacy Preference as a Social Protocol: An Examination within the US Policy Context," *ACM Transactions on Internet Technology* (2:4), pp. 276–306. (https://doi.org/10.1145/604596.604598).

Hoehle, H., Zhang, X., and Venkatesh, V. 2015. "An Espoused Cultural Perspective to Understand Continued Intention to Use Mobile Applications: A Four-Country Study of Mobile Social Media Application Usability," *European Journal of Information Systems* (24), pp. 337–359. (https://doi.org/10.1057/ejis.2014.43).

Hoff, K. A., and Bashir, M. 2015. "Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust," *Human Factors* (57:3), SAGE PublicationsSage CA: Los Angeles, CA, pp. 407–434. (https://doi.org/10.1177/0018720814547570).

Hoffman, D. 2018. "Privacy with Big Data: A Framework," in *Proceedings of the 24th Americas Conference on Information Systems*, New Orleans, USA. (https://aisel.aisnet.org/amcis2018/DataScience/Presentations/39/).

Hofmann, P., Oesterle, S., Rust, P., and Urbach, N. 2019. "Machine Learning Approaches along the Radiology Value Chain - Rethinking Value Propositions," in *Proceedings of the 27th European Conference on Information Systems*, Stockholm, Sweden. (https://aisel.aisnet.org/ecis2019_rp/158/).

Hofmann, S., Müller, O., and Rossi, M. 2020. "Designing for Digital Transformation Co-Creating Services with Citizens and Industry," in *Proceedings of the 15th*

International Conference on Design Science Research in Information Systems and Technology (Vol. 12388 LNCS), pp. 93–98. (https://link.springer.com/book/10.1007/978-3-030-64823-7).

Hofstede, G. 1980. *Culture's Consequences: International Differences in Work-Related Values*, Sage, Beverly Hills, CA.

Hofstede, G. 2001. *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations*, (2nd ed.), Thousand Oaks, CA: Sage Publications.

Hong, W., and Thong, J. Y. L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Ouarterly* (37:1), pp. 275–298. (https://doi.org/10.25300/MISQ/2013/37.1.12).

Hu, M. 2020. "Cambridge Analytica's Black Box," *Big Data and Society*, SAGE Publications Ltd. (https://doi.org/10.1177/2053951720938091).

Hui, K. L., Teo, H., and Lee, S. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, pp. 19–33. (https://doi.org/10.2307/25148779).

Humbert, M., Trubert, B., and Huguenin, K. 2019. "A Survey on Interdependent Privacy," *ACM Computing Surveys* (52:6), pp. 1–40. (https://doi.org/10.1145/3360498).

Hunke, F., and Wambsganß, T. 2017. "Turning Data into Value: Towards an Ideation Tool for Key Activities of Data-Driven Business Models," in *Proceedings of the 3rd Karlsruhe Service Summit Research Workshop*, Karlsruhe, Germany.

Hwang, Y. 2005. "Investigating Enterprise Systems Adoption: Uncertainty Avoidance, Intrinsic Motivation, and the Technology Acceptance Model," *European Journal of Information Systems* (14:2), pp. 150–161. (https://doi.org/10.1057/palgrave.ejis.3000532).

Iacovou, C. L., Benbasat, I., and Dexter, A. S. 1995. "Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology," *MIS Quarterly* (19:4), pp. 465–485. (https://doi.org/10.2307/249629).

IPSOS. 2022. "Global Opinions and Expectations About Artificial Intelligence: A Global Advisor Survey." (https://www.ipsos.com/sites/default/files/ct/news/documents/2022-01/Global-opinions-and-expectations-about-AI-2022.pdf, accessed March 7, 2024).

Jain, P., Gyanchandani, M., and Khare, N. 2016. "Big Data Privacy: A Technological Perspective and Review," *Journal of Big Data* (3), pp. 1–25. (https://doi.org/10.1186/s40537-016-0059-y).

Javidan, M., Dorfman, P. W., De Luque, M. S., and House, R. J. 2006. "In the Eye of the Beholder: Cross Cultural Lessons in Leadership from Project GLOBE," *Academy of Management Perspectives* (20:1), pp. 67–90. (https://doi.org/10.5465/AMP.2006.19873410).

Jia, H., and Xu, H. 2015. "Measuring Individuals' Concerns over Collective Privacy on Social Networking Sites," in *Proceedings of the 36th International Conference on Information Systems*, Fort Worth, Texas, US. (https://aisel.aisnet.org/icis2015/proceedings/SecurityIS/11/).

Jiang, Z., Heng, C. S., and Choi, B. C. F. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), INFORMS Inst.for Operations Res.and the Management Sciences, pp. 579–595. (https://doi.org/10.1287/isre.1120.0441).

Jöhnk, J., Weißert, M., and Wyrtki, K. 2021. "Ready or Not, AI Comes— An Interview Study of Organizational AI Readiness Factors," *Business and Information Systems Engineering* (63:1), pp. 5–20. (https://doi.org/10.1007/s12599-020-00676-7).

John-Mathews, J.-M. 2021. "Critical Empirical Study on Black-Box Explanations in AI," in *Proceeding of the 42nd International Conference on Information Systems*, Austin, TX, US. (https://aisel.aisnet.org/icis2021/ai_business/ai_business/13/).

Jordan, A., Mitchell, A., and Mulligan, D. 2015. "Data, Privacy, and the Greater Good," *Science* (349:6245), American Association for the Advancement of Science, pp. 253–255. (https://doi.org/10.1126/science.aac4520).

Junior, C. H., Oliveira, T., and Yanaze, M. 2019. "The Adoption Stages (Evaluation, Adoption, and Routinisation) of ERP Systems with Business Analytics Functionality in the Context of Farms," *Computers and Electronics in Agriculture* (156), pp. 334–348. (https://doi.org/10.1016/j.compag.2018.11.028).

Jussupow, E., Spohrer, K., and Heinzl, A. 2022. "Radiologists' Usage of Diagnostic AI Systems," *Business & Information Systems Engineering* (64:3), pp. 293–309. (https://doi.org/10.1007/s12599-022-00750-2).

Kahneman, D. 2011. *Thinking, Fast and Slow*, Farrar, Straus and Giroux.

Kane, G. C., Young, A. G., Majchrzak, A., and Ransbotham, S. 2021. "Avoiding an Oppressive Future of Machine Learning: A Design Theory for Emancipatory Assistants," *MIS Quarterly: Management Information Systems* (45:1), University of Minnesota, pp. 371–396. (https://doi.org/10.25300/MISQ/2021/1578).

Kantarcioglu, M., Bensoussan, A., and Hoe, S. C. 2010. "When Do Firms Invest in Privacy-Preserving Technologies?," in *Decision and Game Theory for Security*, T. Alpcan, L. Buttyán, and J. Baras (eds.), Berlin, Heidelberg: Springer, pp. 72–86.

Kantarcioglu, M., Bensoussan, A., and Hoe, S. C. 2011. "Investment in Privacy-Preserving Technologies under Uncertainty," in *Decision and Game Theory for Security*, J. Baras, J. Katz, and E. Altman (eds.), Berlin, Heidelberg: Springer, pp. 219–238.

Karunagaran, S., Mathew, S., and Lehner, F. 2016. "Differential Adoption of Cloud Technology: A Multiple Case Study of Large Firms and SMEs," *Proceedings of the 37th International Conference on Information Systems*, Dublin, UK. (https://aisel.aisnet.org/icis2016/ITImplementation/Presentations/12/).

Karwatzki, S., Dytynko, O., Trenz, M., and Veit, D. 2017. "Beyond the Personalization-Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* (34:2), pp. 369–400. (https://doi.org/10.1080/07421222.2017.1334467).

Karwatzki, S., Trenz, M., and Veit, D. 2022. "The Multidimensional Nature of Privacy Risks: Conceptualisation, Measurement and Implications for Digital Services," *Information Systems Journal* (32:6), John Wiley and Sons Inc, pp. 1126–1157. (https://doi.org/10.1111/isj.12386).

Kaur, D., Uslu, S., Rittichier, K. J., and Durresi, A. 2022. "Trustworthy Artificial Intelligence: A Review," *ACM Computing Surveys* (55:2), ACM PUB27 New York, NY, pp. 1–38. (https://doi.org/10.1145/3491209).

Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. 2009. "A 'Nutrition Label' for Privacy," in *Proceedings of the 5th Symposium On Usable Privacy and Security* (Vol. 1990). (https://doi.org/10.1145/1572532.1572538).

Khlif, H., Hussainey, K., and Achek, I. 2015. "The Effect of National Culture on the Association between Proftability and Corporate Social and Environmental Disclosure: A Meta-Analysis," *Meditari Accountancy Research* (23:3), Emerald Group Publishing Ltd., pp. 296–321. (https://doi.org/10.1108/MEDAR-12-2014-0064).

Kim, J., Giroux, M., and Lee, J. C. 2021. "When Do You Trust AI? The Effect of Number Presentation Detail on Consumer Trust and Acceptance of AI Recommendations," *Psychology & Marketing* (38:7), John Wiley & Sons, Ltd, pp. 1140–1155. (https://doi.org/10.1002/mar.21498).

Kim, S., and Garrison, G. 2010. "Understanding Users' Behaviors Regarding Supply Chain Technology: Determinants Impacting the Adoption and Implementation of RFID Technology in South Korea," *International Journal of Information Management* (30:5), pp. 388–398. (https://doi.org/10.1016/j.ijinfomgt.2010.02.008).

Kim, Y., and Peterson, R. 2017. "A Meta-Analysis of Online Trust Relationships in E-Commerce," *Journal of Interactive Marketing* (38:1). (https://doi.org/10.1016/j.intmar.2017.01.001).

Knight, R. 2015. "Convincing Skeptical Employees to Adopt New Technology," *Harvard Business Review*.

Köchling, A., Riazy, S., Wehner, M. C., and Simbeck, K. 2021. "Highly Accurate, But Still Discriminatory: A Fairness Evaluation of Algorithmic Video Analysis in the Recruitment Context," *Business and Information Systems Engineering* (63:1), Springer Gabler, pp. 39–54. (https://doi.org/10.1007/s12599-020-00673-w).

Kohli, R., and Melville, N. P. 2019. "Digital Innovation: A Review and Synthesis," *Information Systems Journal* (29:1), Blackwell Publishing Ltd, pp. 200–223. (https://doi.org/10.1111/isj.12193).

Kosta, E., Dumortier, J., Ribbers, P., Fairchild, A., Tseng, J., Liesbach, K., et al., and Consortium, P. 2008. "Requirements for Privacy Enhancing Tools," *PRIME Project Deliverable D*, (G. Schumacher, ed.).

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109–125. (https://doi.org/10.1057/jit.2010.6).

Krontiris, I., Benenson, Z., Girard, A., Sabouri, A., Rannenberg, K., Schoo, P., and 2015, A. P. F. 2016. "Privacy-ABCs as a Case for Studying the Adoption of PETs by Users and Service Providers," in *Privacy Technologies and Policy*, B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, and S. Schiffner (eds.), Cham: Springer, pp. 104–123.

Kruse, L., Wunderlich, N., and Beck, R. 2019. "Artificial Intelligence for the Financial Services Industry: What Challenges Organizations to Succeed," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Maui, Hawaii, USA. (https://aisel.aisnet.org/hicss-52/os/practice-based_research/4/).

Kuechler, B., and Vaishnavi, V. 2008. "On Theory Development in Design Dcience Research: Anatomy of a Research Project," *European Journal of Information Systems* (17:5), Taylor & Francis, pp. 489–504. (https://doi.org/10.1057/ejis.2008.40).

Kühne, B., and Böhmann, T. 2019. "Data-Driven Business Models - Building the Bridge Between Data and Value," *Proceedings of the 27th European Conference on Information Systems*, Stockholm & Uppsala, Sweden. (https://aisel.aisnet.org/ecis2019_rp/167/).

Kyriacou, D., and Davis, H. C. 2008. "Moving Towards Life-Long User Modeling," in *Proceedings of the 8th IEEE International Conference on Advanced Learning Technologies*, pp. 647–648. (https://doi.org/10.1109/ICALT.2008.77).

LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., and Kruschwitz, N. 2011. "Big Data, Analytics and the Path From Insights to Value," *MIT Sloan Management Review* (52:2), pp. 21–32.

Lebovitz, S., Levina, N., and Lifshitz-Assaf, H. 2021. "Is AI Ground Truth Really 'True'? The Dangers of Training and Evaluating AI Tools Based on Experts' Know-What," *MIS Quarterly* (45:3), pp. 1501–1525. (https://doi.org/10.25300/MISQ/2021/16564).

Lee, D. J., Ahn, J. H., and Bang, Y. 2011. "Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection," *MIS Quarterly* (35:2), pp. 423–444. (https://doi.org/10.2307/23044050).

Lee, J. D., and See, K. A. 2004. "Trust in Automation: Designing for Appropriate Reliance," *Human Factors* (46:4), SAGE PublicationsSage UK: London, England, pp. 50–80.

Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., and Wagner, D. 2017. "A Usability Evaluation of Tor Launcher," *Proceedings of the '17 Symposium of Privacy*

Enhancing Technologies (2017:3), pp. 90–109. (https://doi.org/10.1515/popets-2017-0030).

Lee, M. K., Jain, A., Cha, H. J., Ojha, S., and Kusbit, D. 2019. "Procedural Justice in Algorithmic Fairness," *Proceedings of the ACM on Human-Computer Interaction* (3:CSCW), pp. 1–26.

Leidner, D. E., and Kayworth, T. 2006. "A Review of Culture in Information Systems Research: Toward a Theory of Information Culture Conflict," *MIS Quarterly* (2), pp. 357–399. (https://doi.org/10.2307/25148735).

Levene, H. 1960. "Robust Tests for Equality of Variances," in *Contributions to Probability and Statistics: Essays in Honor of Harold Hotelling, Stanford University Press*, I. Olkin (ed.), Stanford University Press, Palo Alto, pp. 278–292.

Levy, Y., and Ellis, T. J. 2006. "A Systems Approach to Conduct an Affective Literature Review in Support of Information Systems Research," *Informing Science Journal* (9), pp. 181–212. (https://doi.org/10.28945/479).

Li, C., Li, D. Y., Miklau, G., and Suciu, D. 2014. "A Theory of Pricing Private Data," *ACM Transactions on Database Systems* (39:4), pp. 1–28. (https://doi.org/10.1145/2691190.2691191).

Li, J. 2015. "The Benefit of Being Physically Present: A Survey of Experimental Works Comparing Copresent Robots, Telepresent Robots and Virtual Agents," *International Journal of Human-Computer Studies* (77), pp. 23–37.

Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28). (https://doi.org/10.17705/1CAIS.02828).

Li, Y., and Hahn, J. 2022. "Review of Research on Human Trust in Artificial Intelligence," in *Proceedings of the 43rd International Conference on Information Systems* (Vol. 8). (https://aisel.aisnet.org/icis2022/ai_business/ai_business/8/).

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp. 59–87. (https://doi.org/10.2307/25148781).

Lim, T. S., and Loh, W. Y. 1996. "A Comparison of Tests of Equality of Variances," *Computational Statistics and Data Analysis* (22:3), pp. 287–301. (https://doi.org/10.1016/0167-9473(95)00054-2).

Liu, B., Pavlou, P. A., and Cheng, X. 2022. "Achieving a Balance between Privacy Protection and Data Collection: A Field Experimental Examination of a Theory-Driven Information Technology Solution," *Information Systems Research* (33:1), INFORMS Inst.for Operations Res.and the Management Sciences, pp. 203–223. (https://doi.org/10.1287/ISRE.2021.1045).

Liu, H., Wang, Y., Fan, W., Liu, X., Li, Y., Jain, S., Liu, Y., Jain, A., and Tang, J. 2022. "Trustworthy AI: A Computational Perspective," *ACM Transactions on Intelligent Systems and Technology* (14:1), pp. 1–59.

Liu, Y., Jain, A., Eng, C., Way, D. H., Lee, K., Bui, P., Kanada, K., Oliveira Marinho, G., Gallegos, J., Gabriele, S., Gupta, V., Singh, N., Natarajan, V., Hofmann-Wellenhof, R., Corrado, G. S., Peng, L. H., Webster, D. R., Ai, D., Huang, S. J., Liu, Y., Dunn, R. C., and Coz, D. 2020. "A Deep Learning System for Differential Diagnosis of Skin Diseases," *Nature Medicine* (26:6), Nature Publishing Group, pp. 900–908.

Lohoff, L., and Rühr, A. 2021. "Introducing (Machine) Learning Ability as Antecedent of Trust in Intelligent Systems Intelligent Systems," in *Proceedings of the 42nd International Conference on Information Systems*, pp. 6–14. (https://aisel.aisnet.org/ecis2021_rp).

London Economics. 2010. "Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs)," The European Commission DG Justice, Freedom and Security.

De Long, D. W., and Fahey, L. 2000. "Diagnosing Cultural Barriers to Knowledge Management," *Academy of Management Executive* (14:4), Academy of Management, pp. 113–127. (https://doi.org/10.5465/ame.2000.3979820).

Loucks, J., Hupfer, S., David, J., and Murphy, T. 2019. "Future in the Balance? How Countries Are Pursuing an AI Advantage," *Deloitte Insights*.

Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. 2016. "'Cargo Cult' Science in Traditional Organization and Information Systems Survey Research: A Case for Using Nontraditional Methods of Data Collection, Including Mechanical Turk and Online Panels," *Journal of Strategic Information Systems* (25:3), pp. 232–240. (https://doi.org/10.1016/j.jsis.2016.06.002).

Lusch, R. F., and Nambisan, S. 2015. "Service Innovation: A Service-Dominant Logic Perspective," *MIS Quarterly* (39:1), pp. 155–175. (https://doi.org/10.25300/MISQ/2015/39.1.07).

Maas, J. B., Van Fenema, P. C., and Soeters, J. 2018. "Post-Implementation ERP Usage: A Longitudinal Study of the Impact of Control and Empowerment," *Information Systems Management* (35:4), pp. 330–347. (https://doi.org/10.1080/10580530.2018.1503804).

Magnusson, P., and Peterson, R. 2014. "The Influence of National Cultural Values on the Use of Rewards Alignment to Improve Sales Collaboration," *International Marketing Review* (31:1), pp. 30–50. (https://doi.org/10.1108/IMR-09-2012-0151).

Maguire, M. 2001. "Methods to Support Human-Centred Design," *International Journal of Human Computer Studies* (55:4), Academic Press, pp. 587–634. (https://doi.org/10.1006/ijhc.2001.0503).

Majeed, A., Bhana, R., Haq, A., Kyaruzi, I., Pervaz, S., and Williams, M.-L. 2016. "Internet of Everything (IoE): Analysing the Individual Concerns over Privacy Enhancing Technologies (PETs)," *International Journal of Advanced Computer Scienceand Applications* (7:3). (https://doi.org/10.14569/IJACSA.2016.070303 PDF).

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. (https://doi.org/10.1287/isre.1040.0032).

Manyika, J. 2011. "Big Data: The Next Frontier for Innovation, Competition, and Productivity." (https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx).

Margulis, S. T. 1977a. "Conceptions of Privacy – Current Status and Next Steps," *Journal of Social Issues* (33:3), pp. 5–21. (https://doi.org/10.1111/j.1540-4560.1977.tb01879.x).

Margulis, S. T. 1977b. "Privacy as a Behavioral Phenomenon – Introduction," *Journal of Social Issues* (33:3), p. 1. (https://doi.org/10.1111/j.1540-4560.1977.tb01878.x).

Margulis, S. T. 2003. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2), pp. 243–261. (https://doi.org/10.1111/1540-4560.00063).

Martins, R., Oliveira, T., and Thomas, M. A. 2016. "An Empirical Analysis to Assess the Determinants of SaaS Diffusion in Firms," *Computers in Human Behavior* (62), pp. 19–33. (https://doi.org/10.1016/j.chb.2016.03.049).

May, A., Dremel, C., Sagodi, A., and van Giffen, B. 2020. "Realizing Digital Innovation from Artificial Intelligence," in *Proceedings of the 41st International Conference on Information Systems*, Hyderabad, India, Virtual. (https://aisel.aisnet.org/icis2020/digital_innovation/digital_innovation/6/).

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model Of Organizational Trust," *Academy of Management Review* (20:3), Academy of

Management Briarcliff Manor, NY 10510, pp. 709–734. (https://doi.org/10.2307/258792).
McAfee, A., and Brynjolfsson, E. 2012. "Big Data: The Management Revolution," *Harvard Business Review*, pp. 60–68.
McCarthy, J. 2007. "From Here to Human-Level AI," *Artificial Intelligence* (171:18), pp. 1174–1182. (https://doi.org/10.1016/j.artint.2007.10.009).
McCoy, S., Galletta, D. F., and King, W. R. 2007. "Applying TAM Across Cultures: The Need for Caution," *European Journal of Information Systems* (16:1), pp. 81–90. (https://doi.org/10.1057/palgrave.ejis.3000659).
McKenzie, J. F., Wood, M. L., Kotecki, J. E., Clark, J. K., and Brey, R. A. 1999. "Establishing Content Validity: Using Qualitative and Quantitative Steps," *American Journal of Health Behavior* (23:4), pp. 311–318. (https://doi.org/10.5993/AJHB.23.4.9).
McKnight, D. H., Carter, M., Thatcher, J. B., and Clay, P. F. 2011. "Trust in a Specific Technology: An Investigation of Its Components and Measures," *ACM Transactions on Management Information Systems* (2:2), pp. 1–25. (https://doi.org/10.1145/1985347.1985353).
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.
Mehler, M., Turan Akdag, M., and Zöll, A. 2023. "Exploring the Effect of National Culture on Emerging Technologies: A Glimpse into the Future Technologies," in *Proceedings on the 27th Pacific Asia Conference on Information Systems*, PACIS. (https://aisel.aisnet.org/pacis2023/12/).
Meta. 2022. "About Meta's Intellectual Property Tools." (https://www.facebook.com/business/help/611786833293457, accessed April 25, 2022).
Mettler, T., Eurich, M., and Winter, R. 2014. "On the Use of Experiments in Design Science Research: A Proposition of an Evaluation Framework," *Communications of the Association for Information Systems* (34:1), Association for Information Systems, pp. 223–240. (https://doi.org/10.17705/1cais.03410).
Metzger, M. J. 2004. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication* (9:4). (https://doi.org/10.1111/j.1083-6101.2004.tb00292.x).
Meyer, G., Adomavicius, G., Johnson, P. E., Elidrisi, M., Rush, W. A., Sperl-Hillen, J. M., and OConnor, P. J. 2014. "A Machine Learning Approach to Improving Dynamic Decision Making," *Information Systems Research* (25:2), pp. 239–263. (https://doi.org/10.1287/isre.2014.0513).
Miles, M. B., Huberman, A. M., and Saldana, J. 2019. *Qualitative Data Analysis A Methods Sourcebook*, Arizona State University, USA: SAGE Publications Inc.
Miller, S., Batenburg, R., and van de, L. 2006. "National Culture Influences on European ERP Adoption," in *Proceedings of the 40th European Conference on Information Systems*. (http://aisel.aisnet.org/ecis2006/100).
Milne, A., and Boza, A. 1999. "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing* (13:1). (https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9).
Mitchell, T. M. 1997. *Machine Learning*, New York, NY: McGraw-Hill.
Morlok, T. 2016. "Sharing Is (Not) Caring - The Role of External Privacy in Users' Information Disclosure Behaviors on Social Network Sites," in *Proceedings of the*

20th Pacific Asia Conference on Information Systems. (https://aisel.aisnet.org/pacis2016/75/).

Muhtaroğlu, F. C. P., Demir, S., Obalı, M., and Girgin, C. 2013. "Business Model Canvas Perspective on Big Data Applications," in *Proceedings of the '13 IEEE International Conference on Big Data*, IEEE, pp. 32–37. (https://doi.org/10.1109/BigData.2013.6691684).

Muntermann, J., and Roßnagel, H. 2009. "On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market," in *Proceedings of the 14th Nordic Conference on Secure IT Systems*, pp. 1–14. (https://doi.org/10.1007/978-3-642-04766-4).

Murray, A., Rhymer, J., and Sirmon, D. G. 2021. "Humans and Technology: Forms of Conjoined Agency in Organizations," *Academy of Management Review* (46:3), Academy of Management, pp. 552–571. (https://doi.org/10.5465/amr.2019.0186).

Myers, M. D., and Tan, F. B. 2002. "Beyond Models of National Culture in Information Systems Research," *Journal of Global Information Management* (10:1), pp. 24–32.

Nasif, E. G., Al-Daeaj, H., Ebrahimi, B., and Thibodeaux, M. S. 1991. "Methodological Problems in Cross-Cultural Research: An Updated Review," *Management International Review* (31:1), pp. 79–91.

Ngassam, N., Ologeanu-Taddei, R., and Bourdon, I. 2021. "Design of E-Health Application to Enhance Health Information Quality: The Case of a Digital Allergy Card," in *Proceedings of the 29th European Conference on Information Systems*, pp. 6–14. (https://aisel.aisnet.org/ecis2021_rp).

Nguyen, D. K., Broekhuizen, T., Dong, J. Q., and Verhoef, P. C. 2019. "Digital Readiness: Construct Development and Empirical Validation," in *Proceedings of the 40th International Conference on Information Systems*, Munich, Germany. (https://aisel.aisnet.org/icis2019/business_models/business_models/15/).

Nguyen, T.-T., Sim, K., Kuen, A., Odonnell, R. R., Lim, S. T., Wang, W., and Nguyen, H. D. 2021. "Designing AI-Based Conversational Agent for Diabetes Care in a Multilingual Context," in *Proceedings of the 25th Pacific Asia Conference on Information Systems*. (Proceedings of the 25th Pacific Asia Conference on Information Systems).

Norman, D. A., and Draper, S. W. 1986. *User Centred System Design-New Perspectives on Human/Computer Interaction*.

Nunnally, J. C. 1978. "Psychometric Theory," *McGraw-Hill, New York* (2n Edition).

Oetzel, M. C., and Spiekermann, S. 2012. "Privacy-by-Design through Systematic Privacy Impact Assessment - A Design Science Approach," in *Proceedings of the 20th European Conference on Information Systems*, Barcelona, Spain. (https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1159&context=ecis2012).

Oliveira, T., and Fraga, M. 2011. "Literature Review of Information Technology Adoption Models at Firm Level," *The Electronic Journal Information Systems Evaluation* (14:1), pp. 110–121.

Oppliger, R. 2005. "Privacy-Enhancing Technologies for the World Wide Web," *Computer Communications* (28:16), pp. 1791–1797. (https://doi.org/10.1016/j.comcom.2005.02.003).

Orange. 2014. "The Future of Digital Trust: A European Study on the Nature of Consumer Trust and Personal Data." (https://www.enriquedans.com/wp-content/uploads/2022/02/the-future-of-digital-trust.pdf).

Ostrom, A. L., Parasuraman, A., Bowen, D. E., Patricio, L., and Voss, C. A. 2015. "Service Research Priorities in a Rapidly Changing Context," *Journal of Service*

Research (18:2), SAGE Publications Inc, pp. 127–159. (https://doi.org/10.1177/1094670515576315).

Özbilen, P. 2017. "The Impact of Natural Culture on New Technology Adoption by Firms: A Country Level Analysis," *International Journal of Innovation, Management and Technology* (8:4), pp. 299–305. (https://doi.org/10.18178/ijimt.2017.8.4.745).

Ozdemir, Z. D., Jeff Smith, H., and Benamati, J. H. 2017. "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study," *European Journal of Information Systems* (26:6), pp. 642–660. (https://doi.org/10.1057/s41303-017-0056-z).

Paefgen, J., Staake, T., and Thiesse, F. 2012. "Resolving the Misalignment between Consumer Privacy Concerns and Ubiquitous IS Design: The Case of Usage-Based Insurance," in *Proceedings of the 33th International Conference on Information Systems*, Orlando, US. (https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/6/).

Palan, S., and Schitter, C. 2018. "Prolific.Ac—A Subject Pool for Online Experiments," *Journal of Behavioral and Experimental Finance* (17), Elsevier, pp. 22–27. (https://doi.org/10.1016/j.jbef.2017.12.004).

Parmar, R., Mackenzie, I., Cohn, D., and Gann, D. 2014. "The New Patterns of Innovation," *Harvard Business Review*.

Patki, N., Wedge, R., and Veeramachaneni, K. 2016. "The Synthetic Data Vault," in *Proceedings of the '16 IEEE International Conference on Data Science and Advanced Analytics*, pp. 399–410. (https://doi.org/10.1109/DSAA.2016.49).

Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly* (35:4), pp. 977–988. (https://doi.org/10.2307/41409969).

Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), INFORMS Inst.for Operations Res.and the Management Sciences, pp. 37–59. (https://doi.org/10.1287/isre.1040.0015).

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45–77. (https://doi.org/10.2753/MIS0742-1222240302).

Pelkola, D. 2012. "A Framework for Managing Privacy-Enhancing Technology," *IEEE Software* (29:3), pp. 45–49. (https://doi.org/10.1109/ms.2012.47).

Peters, F., Pumplun, L., and Buxmann, P. 2020. "Opening the Black Box: Consumer's Willingness to Pay for Transparency of Intelligent Systems," in *Proceedings of the 28th European Conference on Information Systems*, Marrakech, Morocco, Virtual. (https://aisel.aisnet.org/ecis2020_rp/90/).

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*, State University of New York Press.

Pfeffer, J. 1981. "Power in Organizations," *American Journal of Sociology* (88:3), pp. 605–608.

Pfeffer, J., and Salancik, G. 1978. *The External Control of Organizations: A Resource Dependence Perspective*, New York, Harper & Row.

Png, I. P. L., Tan, B. C. Y., and Wee, K. L. 2001. "Dimensions of National Culture and Corporate Adoption of IT Infrastructure," *IEEE Transactions on Engineering Management* (48:1), pp. 36–45. (https://doi.org/10.1109/17.913164).

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879–903. (https://doi.org/10.1037/0021-9010.88.5.879).

Pu, Y., and Grossklags, J. 2017. "Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter?," in *Proceedings of the 30th Symposium on Usable Privacy and Security*, Santa Clara, CA, USA.

Pumplun, L., Peters, F., Gawlitza, J. F., and Buxmann, P. 2023. "Bringing Machine Learning Systems into Clinical Practice: A Design Science Approach to Explainable Machine Learning-Based Clinical Decision Support Systems," *Journal of the Association for Information Systems* (24:4), pp. 953–979. (https://doi.org/10.17705/1jais.00820).

Pumplun, L., Tauchert, C., and Heidt, M. 2019. "A New Organizational Chassis for Artificial Intelligence - Exploring Organizational Readiness Factors," in *Proceedings of the 26th European Conference on Information Systems*, Stockholm, Sweden. (https://aisel.aisnet.org/ecis2019_rp/106/).

PWC. 2017. "Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise?" (https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf, accessed March 9, 2024).

Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J. F., Breazeal, C., Crandall, J. W., Christakis, N. A., Couzin, I. D., Jackson, M. O., Jennings, N. R., Kamar, E., Kloumann, I. M., Larochelle, H., Lazer, D., McElreath, R., Mislove, A., Parkes, D. C., Pentland, A. 'Sandy,' Roberts, M. E., Shariff, A., Tenenbaum, J. B., and Wellman, M. 2019. "Machine Behaviour," *Nature* (568), Nature Publishing Group, pp. 477–486. (https://doi.org/10.1038/s41586-019-1138-y).

Rai, A. 2020. "Explainable AI: From Black Box to Glass Box," *Journal of the Academy of Marketing Science* (48:1), pp. 137–141. (https://doi.org/10.1007/s11747-019-00710-5).

Rai, A., Brown, P., and Tang, X. 2009. "Organizational Assimilation of Electronic Procurement Innovations," *Journal of Management Information Systems* (26:1), pp. 257–296. (https://doi.org/10.2753/MIS0742-1222260110).

Rai, A., Constantinides, P., and Sarker, S. 2019. "Next-Generation Digital Platform: Toward Human-AI Hybrids," *MIS Quarterly* (43:February), pp. 1–9.

Rana, R., Staron, M., Hansson, J., Nilsson, M., and Meding, W. 2014. "A Framework for Adoption of Machine Learning in Industry for Software Defect Prediction," in *Proceedings of the 9th International Conference on Software Engineering and Applications*, Vienna, Austria, pp. 383–392. (https://ieeexplore.ieee.org/document/7293887).

Ransbotham, B. S., Khodabandeh, S., and Fehling, R. 2019. "Winning With AI," *MIT Sloan Management Review*.

Raptis, D. A., Mettler, T., Tzanas, K., and Graf, R. 2012. "A Novel Open-Source Web-Based Platform Promoting Collaboration of Healthcare Professionals and Biostatisticians: A Design Science Ppproach," *Informatics for Health & Social Care* (37:1), pp. 22–36. (https://doi.org/10.3109/17538157.2011.590257).

Reay, I., Dick, S., and Miller, J. 2009. "An Analysis of Privacy Signals on the World Wide Web: Past, Present and Future," *Information Sciences* (179:8), pp. 1102–1115. (https://doi.org/10.1016/j.ins.2008.12.012).

Reay, I. K., Beatty, P., Dick, S., and Miller, J. 2007. "A Survey and Analysis of the P3P Protocol's Agents, Adoption, Maintenance, and Future," *IEEE Transactions on Dependable and Secure Computing* (4:2), pp. 151–164. (https://doi.org/10.1109/tdsc.2007.1004).

Renner, M., Lins, S., Söllner, M., Thiebes, S., and Sunyaev, A. 2021. "Achieving Trustworthy Artificial Intelligence: Multi-Source Trust Transfer in Artificial In-Telligence-Capable Technology," in *Proceedings of the 42nd International*

Conference on Information Systems. (https://aisel.aisnet.org/icis2021/hci_robot/hci_robot/15/).

Riedl, R. 2022. "Is Trust in Artificial Intelligence Systems Related to User Personality? Review of Empirical Evidence and Future Research Directions," *Electronic Markets* (32), Springer, pp. 2021–2051. (https://doi.org/10.1007/s12525-022-00594-4).

Ringle, C. M., Wende, S., and Becker, J.-M. 2015. *SmartPLS 3*.

Robinson, S. C. 2020. "Trust, Transparency, and Openness: How Inclusion of Cultural Values Shapes Nordic National Public Policy Strategies for Artificial Intelligence," *Technology in Society* (63), Pergamon. (https://doi.org/10.1016/j.techsoc.2020.101421).

Rogers, B. 2015. "The Social Costs of Uber," *University of Chicago Law Review Online* (82:1), pp. 85–102.

Rogers, E. 1995. *Diffusion of Innovations*, (4th ed.), New York: Free Press.

Rogers, E. M., and Shoemaker, F. F. 1971. *Communication of Innovations: A Cross-Cultural Approach*, (2nd ed.), Free Press.

Roshanov, P. S., Fernandes, N., Wilczynski, J. M., Hemens, B. J., You, J. J., Handler, S. M., Nieuwlaat, R., Souza, N. M., Beyene, J., van Spall, H. G. C., Garg, A. X., and Haynes, R. B. 2013. "Features of Effective Computerised Clinical Decision Support Systems: Meta-Regression of 162 Randomised Trials," *BMJ* (346), British Medical Journal Publishing Group. (https://doi.org/10.1136/bmj.f657).

Rossnagel, H., Samarati, P., Tunstall, M., Posegga, J., Markantonakis, K., and Sauveron, D. 2010. *The Market Failure of Anonymity Services*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 340–354.

Rowe, F. 2014. "What Literature Review Is Not: Diversity, Boundaries and Recommendations," *European Journal of Information Systems* (23:3), pp. 241–255. (https://doi.org/10.1057/ejis.2014.7).

Rubinstein, I. 2011. "Regulating Privacy by Design," *Berkeley Technology Law Journal* (26:3), University of California School of Law, pp. 1409–1456.

Rudin, C. 2019. "Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead," *Nature Machine Intelligence* (1:5), pp. 206–215. (https://doi.org/10.1038/s42256-019-0048-x).

Rudin, C., and Ustun, B. 2018. "Optimized Scoring Systems: Toward Trust in Machine Learning for Healthcare and Criminal Justice," *Interfaces* (48:5), pp. 449–466. (https://doi.org/10.1287/inte.2018.0957).

Russell, S. J. and P. Norvig. 2021. *Artificial Intelligence: A Modern Approach*, (4th ed.), Upper Saddle River: Pearson Education. .

Ryan, G. W., and Bernard, H. R. 2000. "Data Management and Analysis Methods," in *Handbook of Qualitative Research* (2nd ed.), N. K. Denzin and Y. S. Lincoln (eds.), Sage Publication, Inc., pp. 769–802.

Ryan, G. W., and Bernard, H. R. 2003. "Techniques to Identify Themes in Qualitative Data," *Field Methods* (15:1), pp. 85–109. (https://doi.org/10.1177/1525822X0223956).

Rzepka, C., and Berger, B. 2018. "User Interaction with AI-Enabled Systems: A Systematic Review of IS Research," in *Proceedings of the 39th International Conference on Information Systems*, San Francisco, CA, USA. (https://aisel.aisnet.org/icis2018/general/Presentations/7/).

Samuel, A. L. 1959. "Some Studies in Machine Learning Using the Game of Checkers," *IBM Journal of Research and Development* (3:3), pp. 210–229. (https://doi.org/10.1147/rd.33.0210).

Schillewaert, N., Ahearne, M. J., Frambach, R. T., and Moenaert, R. K. 2005. "The Adoption of Information Technology in the Sales Force," *Industrial Marketing Management* (34:4), pp. 323–336. (https://doi.org/10.1016/j.indmarman.2004.09.013).

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., and Yu, Y. 2017. "Protecting Customer Privacy When Marketing with Second-Party Data," *International Journal of Research in Marketing* (34:3), Elsevier B.V., pp. 593–603. (https://doi.org/10.1016/j.ijresmar.2017.02.003).

Schoeman, F. D. 1992. *Privacy and Social Freedom*, Cambridge: Cambridge University Press. (https://doi.org/10.1017/CBO9780511527401).

Schreiner, M., Hess, T., and Faranak, F. 2013. "On the Willingness to Pay for Privacy as a Freemium Model: First Empirical Evidence," in *Proceedings of the 21st European Conference on Information Systems*, Utrecht, Niederlande. (https://aisel.aisnet.org/ecis2013_rip/30/).

Schryen, G. 2015. "Writing Qualitative IS Literature Reviews - Guidelines for Synthesis, Interpretation, and Guidance of Research," *Communications of the Association for Information Systems* (37:12), pp. 286–325. (https://doi.org/10.17705/1CAIS.03712).

Schuetz, S., and Venkatesh, V. 2020. "Research Perspectives: The Rise of Human Machines: How Cognitive Computing Systems Challenge Assumptions of User-System Interaction," *Journal of the Association for Information Systems* (21:2), pp. 460–482. (https://doi.org/10.17705/1jais.00608).

Schweiger, A., Sunyaev, A., Leimeister, J. M., and Krcmar, H. 2007. "Information Systems and Healthcare XX: Toward Seamless Healthcare with Software Agents," *Communications of the Association for Information Systems* (19:33), pp. 692–709. (https://doi.org/10.17705/1CAIS.01933).

Seddon, P. B., Constantinidis, D., Tamm, T., and Dod, H. 2017. "How Does Business Analytics Contribute to Business Value?," *Information Systems Journal* (27:3), pp. 237–269. (https://doi.org/10.1111/isj.12101).

Seničar, V., Jerman-Blažič, B., and Klobučar, T. 2003. "Privacy-Enhancing Technologies — Approaches and Development," *Computer Standards & Interfaces* (25:2), pp. 147–158. (https://doi.org/10.1016/s0920-5489(03)00003-5).

Shaphiro, S., and Wilk, M. B. 1965. "An Analysis of Variance Test for Normality," *Biometrika* (52:3), pp. 591–611. (https://doi.org/10.2307/2333709).

Shapiro, C., Carl, S., and Varian, H. R. 1998. *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business Press.

Sheridan, T. B. 2019. "Individual Differences in Attributes of Trust in Automation: Measurement and Application to System Design," *Frontiers in Psychology* (10), p. 1117. (https://doi.org/10.3389/fpsyg.2019.01117).

Shimojo, A., Kamada, S., Matsumoto, S., and Nakamura, M. 2010. "On Integrating Heterogeneous Lifelog Services," in *Proceedings of the 12th International Conference on Information Integration and Web-Based Applications & Services*, pp. 263–272. (https://doi.org/10.1145/1967486.1967529).

Siau, K., and Wang, W. 2018. "Building Trust in Artificial Intelligence, Machine Learning, and Robotics," *Cutter Business Technology Journal* (31:2), pp. 47–53.

Sidorova, A., and Rafiee, D. 2019. "AI Agency Risks and Their Mitigation Through Business Process Management: A Conceptual Framework," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Maui, Hawaii, USA, pp. 5837–5845.

Signal. 2022. "View-Once Media." (https://support.signal.org/hc/en-us/articles/360038443071-View-once-Media, accessed May 3, 2022).

Sjöström, J., Ågerfalk, P., and Hevner, A. R. 2022. "The Design of a System for Online Psychosocial Care: Balancing Privacy and Accountability in Sensitive Online

Healthcare Environments," *Journal of the Association for Information Systems* (23:1), pp. 237–263. (https://doi.org/10.17705/1jais.00717).
Skinner, G., Han, S., and Chang, E. 2006. "An Information Privacy Taxonomy for Collaborative Environments," *Information Management & Computer Security* (14:4), pp. 382–394. (https://doi.org/10.1108/09685220610690835).
Smith, H. J. 2008. "Information Privacy and Its Management," *MIS Quarterly Executive* (3:4). (https://aisel.aisnet.org/misqe/vol3/iss4/6).
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1015.
Smith, H. J., Milburg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196. (https://doi.org/10.2307/249477).
Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477–560. (https://doi.org/10.2307/40041279).
Solove, D. J. 2018. "Strategic Privacy by Design: An Interview with Jason Cronk." (https://teachprivacy.com/strategic-privacy-by-design/).
Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. 2015. "The Challenges of Personal Data Markets and Privacy," *Electronic Markets* (25:2), pp. 161–167. (https://doi.org/10.1007/s12525-015-0191-0).
Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, Tampa, Florida, pp. 38–47.
Squicciarini, A. C., Shehab, M., and Paci, F. 2009. "Collective Privacy Management in Social Networks," in *Proceedings of the 18th International World Wide Web Conference*, New York, NY, US, pp. 521–530. (https://doi.org/10.1145/1526709.1526780).
Srite, M., and Karahanna, E. 2006. "The Role of Espoused National Cultural Values in Technology Acceptance," *MIS Quarterly* (30:3), pp. 679–704. (https://doi.org/10.2307/25148745).
Statista. 2022. "Most Popular Global Mobile Messenger Apps as of January 2022, Based on Number of Monthly Active Users." (https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/, accessed April 28, 2022).
Stieglitz, S., Mirbabaie, M., Fromm, J., and Melzer, S. 2018. "The Adoption of Social Media Analytics for Crisis Management – Challenges and Opportunities," in *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK. (https://aisel.aisnet.org/ecis2018_rp/4/).
Stone, E. F., Gueutal, G. H., Gardner, D. G., and McClure, S. A. 1983. "Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," . . *Journal of Applied Psychology* (68:3), pp. 459–468. (https://doi.org/10.1037/0021-9010.68.3.459).
Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Srite, M. 2002. "Toward a Theory-Based Measurement of Culture," *Journal of Global Information Management* (10:1), IGI Publishing, pp. 13–23. (https://doi.org/10.4018/jgim.2002010102).
Strich, F., Mayer, A.-S., and Fiedler, M. 2021. "What Do I Do in a World of Artificial Intelligence? Investigating the Impact of Substitutive Decision-Making AI Systems on Employees' Professional Role Identity," *Journal of the Association for Information Systems* (22:2). (https://doi.org/10.17705/1jais.00663).
Sturm, T., Koppe, T., Scholz, Y., and Buxmann, P. 2021. "The Case of Human-Machine Trading as Bilateral Organizational Learning," in *Proceedings of the 42th*

International Conference on Information Systems, Austin, TX, USA. (https://aisel.aisnet.org/icis2021/ai_business/ai_business/3/).

Sturm, T., and Peters, F. 2020. "The Impact of Artificial Intelligence on Individual Performance: Exploring the Fit between Task, Data, and Technology," in *Proceedings of the 28th European Conference on Information Systems*, Marrakech, Morocco, Virtual. (https://aisel.aisnet.org/ecis2020_rp/200/).

Stutzman, F., and Kramer-Duffield, J. 2010. "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook," in *Proceedings of the Conference on Human Factors in Computing Systems* (Vol. 3), pp. 1553–1562. (https://doi.org/10.1145/1753326.1753559).

Such, J. M., Porter, J., Preibusch, S., and Joinson, A. 2017. "Photo Privacy Conflicts in Social Media: A Large-Scale Empirical Study," in *Proceedings of the '17 Conference on Human Factors in Computing Systems*, Denver, Colorado, US, pp. 3821–3832. (https://doi.org/10.1145/3025453.3025668).

Taddei, S., and Contena, B. 2013. "Privacy, Trust and Control: Which Relationships with Online Self-Disclosure?," *Computers in Human Behavior* (29:3), Pergamon, pp. 821–826. (https://doi.org/10.1016/J.CHB.2012.11.022).

Takiddin, A., Schneider, J., Yang, Y., Abd-Alrazaq, A., and Househ, M. 2021. "Artificial Intelligence for Skin Cancer Detection: Scoping Review," *Journal of Medical Internet Research* (23:11). (https://doi.org/10.2196/22934).

Tavani, H. 2000. "Privacy-Enhancing Technologies as a Panacea for Online Privacy Concerns - Some Ethical Considerations," *Journal of Information Ethics* (9:2), pp. 26–36.

Taylor, R. H., Menciassi, A., Fichtinger, G., Fiorini, P., and Dario, P. 2016. "Medical Robotics and Computer-Integrated Surgery," in *Springer Handbook of Robotics*, B. Siciliano and O. Khatib (eds.), Springer, pp. 1657–1684.

Templeton, G. F. 2011. "A Two-Step Approach for Transforming Continuous Variables to Normal: Implications and Recommendations for IS Research," *Communications of the Association for Information Systems* (28:1), pp. 41–58. (https://doi.org/10.17705/1CAIS.02804).

Tene, O., and Polonetsky, J. 2012. "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property* (11:5), pp. 239–273. (https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1).

Tene, O., and Polonetsky, J. 2013. "A Theory of Creepy: Technology, Privacy and Shifting Social Norms," *Yale Journal of Law and Technology* (16). (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326830).

Teodorescu, M. H. M., Morse, L., Awwad, Y., and Kane, G. C. 2021. "Failures of Fairness in Automation Require a Deeper Understanding of Human-ML Augmentation," *MIS Quarterly* (45:3), pp. 1483–1499. (https://doi.org/10.25300/MISQ/2021/16535).

Thiebes, S., Lins, S., and Sunyaev, A. 2020. "Trustworthy Artificial Intelligence," *Electronic Markets* (31), pp. 447–464. (https://doi.org/10.1007/s12525-020-00441-4).

Thiesse, F., Floerkemeier, C., Fleisch, E., and Sorensen, C. 2007. "Assessing the Impact of Privacy-Enhancing Technologies for RFID in the Retail Industry," in *Proceedings of the 13th Americas Conference on Information Systems*, Colorado, USA. (https://aisel.aisnet.org/amcis2007/223/).

Thomas, K., Grier, C., and Nicol, D. M. 2010. "UnFriendly: Multi-Party Privacy Risks in Social Networks," in *Privacy Enhancing Technologies. Lecture Notes in Computer Science* (Vol. 6205), N. J. Atallah, M.J., Hopper (ed.), Springer, Berlin, Heidelberg, pp. 236–252.

Thompson, J. D. 1967. "Organization in Action: Social Science Bases of Administrative Theory," *McGraw-Hill Book Company*. (https://doi.org/10.4324/9781315125930).

Thrall, J. H., Li, X., Li, Q., Cruz, C., Do, S., Dreyer, K., and Brink, J. 2018. "Artificial Intelligence and Machine Learning in Radiology: Opportunities, Challenges, Pitfalls, and Criteria for Success," *Journal of the American College of Radiology* (15:3), Elsevier B.V., pp. 504–508. (https://doi.org/10.1016/j.jacr.2017.12.026).

Tofangchi, S., Hanelt, A., and Boehrnsen, F. 2017. "Distributed Cognitive Expert Systems in Cancer Data Analytics: A Decision Support System for Oral and Maxillofacial Surgery," in *Proceedings of the 38th Conference on Information Systems*. (https://aisel.aisnet.org/icis2017/IT-and-Healthcare/Presentations/19/).

Tong, Y., Tan, C. H., Sia, C. L., Shi, Y., and Teo, H. H. 2022. "Rural-Urban Healthcare Access Inequality Challenge: Transformative Roles of Information Technology," *MIS Quarterly* (46:4), pp. 1937–1985. (https://doi.org/10.25300/MISQ/2022/14789).

Toreini, E., Aitken, M., Coopamootoo, K., Elliott, K., Zelaya, C. G., and van Moorsel, A. 2020. "The Relationship Between Trust in AI and Trustworthy Machine Learning Technologies," in *Proceedings of the '20 Conference on Fairness, Accountability, and Transparency*, Association for Computing Machinery, Inc, January 27, pp. 272–283. (https://doi.org/10.1145/3351095.3372834).

Tornatzky, L. G., and Fleischer, M. 1990. "The Process of Technological Innovation," in *Technological Innovation as a Process*, Lexington, pp. 27–50.

Tornatzky, L. G., and Klein, K. J. 1982. "Innovation Characteristics and Innovation Adoption-Implementation: A Meta-Analysis of Findings," *IEEE Transactions on Engineering Management* (1), pp. 28–45. (https://doi.org/10.1109/TEM.1982.6447463).

Tractinsky, N., and Jarvenpaa, S. L. 1995. "Information Systems Design Decisions in a Global versus Domestic Context," *MIS Quarterly* (19:4), pp. 507–529. (https://doi.org/10.2307/249631).

Tremblay, M. C., Hevner, A. R., and Berndt, D. J. 2010. "Focus Groups for Artifact Refinement and Evaluation in Design Research," *Communications of the Association for Information Systems* (26:27), pp. 599–618. (https://doi.org/10.17705/1CAIS.02627).

Turner, E. C., and Dasgupta, S. 2003. "Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals," *Information Systems Management* (20:1), pp. 8–18. (https://doi.org/10.1201/1078/43203.20.1.20031201/40079.2).

Tuunanen, T., Lumivalo, J., Vartiainen, T., Zhang, Y., and Myers, M. M. 2023. "Micro-Level Mechanisms to Support Value Co-Creation for Design of Digital Services," *Journal of Service Research* (0:0), SAGE Publications Inc., pp. 1–16. (https://doi.org/10.1177/10946705231173116).

Tuunanen, T., and Peffers, K. 2018. "Population Targeted Requirements Acquisition," *European Journal of Information Systems* (27:6), pp. 686–711. (https://doi.org/10.1080/0960085X.2018.1476015).

U.S. Department of Health and Human Services. 2022. "Health Insurance Portability and Accountability Act." (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html, accessed April 29, 2022).

Vaishnavi, V. K., and Kuechler, W. 2007. *Design Science Research Methods and Patterns Innovating Information and Communication Technology*, Boston, MA: Auerbach Publications. (https://doi.org/10.1201/9781420059335).

Vemou, K., and Karyda, M. 2015. "Evaluating Privacy Practices in Web 2.0 Services," in *Proceedings on the 9th Mediterranean Conference on Information Systems*, Samos, Greece. (https://aisel.aisnet.org/mcis2015/7/).

Venable, J., and Baskerville, R. 2010. "Eating Our Own Cooking: Toward a More Rigorous Design Science of Research Methods," *Electronic Journal of Business Research Methods* (10:2), pp. 141–153.

Venkatesh, V., and Bala, H. 2012. "Adoption and Impacts of Interorganizational Business Process Standards: Role of Partnering Synergy," *Information Systems Research* (23:4), pp. 1131–1157. (https://doi.org/10.1287/isre.1110.0404).

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425–478. (https://doi.org/10.2307/30036540).

Waarts, E., and van Everdingen, Y. 2005. "The Influence of National Culture on the Adoption Status of Innovations: An Empirical Study of Firms Across Europe," *European Management Journal* (23:6), pp. 601–610. (https://doi.org/10.1016/j.emj.2005.10.007).

Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *Journal of Strategic Information Systems* (22:2), pp. 157–174. (https://doi.org/10.1016/j.jsis.2013.01.003).

Walsham, B. G. 2002. "Cross-Cultural Software Production and Use," *MIS Quarterly* (26:4), pp. 359–380. (https://doi.org/10.2307/4132313).

Wang, Chong, Zhang, N., and Wang, Cong. 2021. "Managing Privacy in the Digital Economy," *Fundamental Research* (5:1), pp. 543–551. (https://doi.org/10.1016/j.fmre.2021.08.009).

Wang, N., Xu, H., and Grossklags, J. 2011. "Third-Party Apps on Facebook: Privacy and the Illusion of Control," *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*. (https://doi.org/10.1145/2076444.2076448).

Wang, P. 2019. "On Defining Artificial Intelligence," *Journal of Artificial General Intelligence* (10:2), pp. 1–37. (https://doi.org/10.2478/jagi-2019-0002).

Wang, X., and Zander, S. 2018. "Extending the Model of Internet Standards Adoption: A Cross-Country Comparison of IPv6 Adoption," *Information & Management* (55:4), North-Holland, pp. 450–460. (https://doi.org/10.1016/J.IM.2017.10.005).

Wang, Y., and Kobsa, A. 2008. "Privacy-Enhancing Technologies," in *Handbook of Research on Social and Organizational Liabilities in Information Security*, M. Gupta and R. Sharman (eds.), IGI Global, pp. 203–227.

Warren, S. V, and Brandeis, L. D. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), Harvard Law Review Association, pp. 193–220. (https://doi.org/10.2307/1321160).

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), Xiii–Xxiii. (https://doi.org/10.2307/4132319).

Weill, P., and Vitale, M. 1999. "Assessing the Health of an Information Systems Applications Portfolio: An Example from Process Manufacturing," *MIS Quarterly* (23:4), pp. 601–624. (https://doi.org/10.2307/249491).

Weiner, B. J. 2009. "A Theory of Organizational Readiness for Change," *Implementation Science* (4:67). (https://doi.org/10.1186/1748-5908-4-67).

Welzer, T., and Hölbl, M. 2000. "Influence of Cultural Issues on Data Quality Dimensions," in *Proceedings of the 4th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications*, Maribor, Slovenia.

Westin, A. F. 1968. "Privacy and Freedom," *Washington and Lee Law Review* (25), pp. 3–4. (https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20).

WhatsApp. 2022. "About View Once." (https://faq.whatsapp.com/general/chats/about-view-once/?lang=en, accessed May 3, 2022).

Williams, K., Chatterjee, S., and Rossi, M. 2008. "Design of Emerging Digital Services: A Taxonomy," *European Journal of Information Systems* (17:5), Palgrave Macmillan Ltd., pp. 505–517. (https://doi.org/10.1057/ejis.2008.38).

Wright, S. A., and Schultz, A. E. 2018. "The Rising Tide of Artificial Intelligence and Business Automation: Developing an Ethical Framework," *Business Horizons* (61:6), Elsevier Ltd, pp. 823–832. (https://doi.org/10.1016/j.bushor.2018.07.001).

Wu, I. L., and Chuang, C. H. 2010. "Examining the Diffusion of Electronic Supply Chain Management with External Antecedents and Firm Performance: A Multi-Stage Analysis," *Decision Support Systems* (50:1), pp. 103–115. (https://doi.org/10.1016/j.dss.2010.07.006).

Wu, X., Zhu, X., Wu, G.-Q., and Ding, W. 2013. "Data Mining with Big Data," *IEEE Transactions on Knowledge and Data Engineering* (26:1), pp. 97–107. (https://doi.org/10.1109/TKDE.2013.109).

Wulf, J., Mettler, T., and Brenner, W. 2017. "Using a Digital Services Capability Model to Assess Readiness for Using a Digital Services Capability Model to Assess Readiness for the Digital Consumer the Digital Consumer," *MIS Quarterly Executive* (16:3), pp. 8–31. (https://aisel.aisnet.org/misqe/vol16/iss3/4).

Xie, E., Teo, H. H., and Wan, W. 2006. "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior," *Marketing Letters* (17:1), Springer, pp. 61–74. (https://doi.org/10.1007/s11002-006-4147-1).

Xu, H. 2007. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," in *Proceedings on the 28th International Conference on Information Systems*, Paris, France. (https://aisel.aisnet.org/icis2007/125/).

Xu, H. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in *Proceedings on the 29th International Conference on Information Systems*. (https://aisel.aisnet.org/icis2008/6/).

Xu, H. 2009. "Consumer Responses to the Introduction of Privacy Protection Measures: An Exploratory Research Framework," *International Journal of E-Business Research* (5:2), pp. 21–47. (https://doi.org/10.4018/jebr.2009040102).

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798–824. (https://doi.org/10.17705/1jais.00281).

Xu, J., Benbasat, I., and Cenfetelli, R. T. 2014. "The Nature and Consequences of Trade-off Transparency in the Context of Recommendation Agents," *MIS Quarterly* (38:2), pp. 379–406. (https://doi.org/10.25300/MISQ/2014/38.2.03).

Xu, W., Ou, P., and Fan, W. 2017. "Antecedents of ERP Assimilation and Its Impact on ERP Value: A TOE-Based Model and Empirical Test," *Information Systems Frontiers* (19:1), pp. 13–30. (https://doi.org/10.1007/s10796-015-9583-0).

Yang, R., and Wibowo, S. 2022. "User Trust in Artificial Intelligence: A Comprehensive Conceptual Framework," *Electronic Markets* (32), Springer, pp. 2053–2077. (https://doi.org/10.1007/s12525-022-00592-6).

Yen, C., and Chiang, M.-C. 2021. "Trust Me, If You Can: A Study on the Factors That Influence Consumers' Purchase Intention Triggered by Chatbots Based on Brain Image Evidence and Self-Reported Assessments," *Behaviour & Information Technology* (40:11), pp. 1177–1194. (https://doi.org/10.1080/0144929X.2020.1743362).

Yeniyurt, S., and Townsend, J. D. 2003. "Does Culture Explain Acceptance of New Products in a Country?: An Empirical Investigation," *International Marketing Review* (20:4), pp. 377–396. (https://doi.org/10.1108/02651330310485153).

Yoo, Y., Boland, R. J., Lyytinen, K., and Majchrzak, A. 2012. "Organizing for Innovation in the Digitized World," *Organization Science* (23:5), pp. 1398–1408. (https://doi.org/10.1287/orsc.1120.0771).

Zhang, C., and Conrad, F. G. 2014. "Speeding in Web Surveys: The Tendency to Answer Very Fast and Its Association with Straightlining," *Survey Research Methods* (8:2), pp. 127–135. (https://doi.org/10.18148/srm/2014.v8i2.5453).

Zhang, N., Wang, C., Karahanna, E., and Xu, Y. 2022. "Peer Privacy Concerns: Conceptualization and Measurement," *MIS Quarterly* (46:1), pp. 491–530. (https://doi.org/10.25300/MISQ/2022/14861).

Zhang, Z., Nandhakumar, J., Hummel, J. T., and Waardenburg, L. 2020. "Addressing the Key Challenges of Developing Machine Learning AI Systems for Knowledge-Intensive Work," *MIS Quarterly Executive* (19:4), pp. 221–238. (https://aisel.aisnet.org/misqe/vol19/iss4/5).

Zheng, Z., and Pavlou, P. A. 2010. "Toward a Causal Interpretation for Structural Models: A New Bayesian Networks Method for Observational Data with Latent Variables," *Information Systems Research* (21:2), pp. 365–391.

Zhu, K., Kraemer, K. L., and Dedrick, J. 2004. "Information Technology Payoff in E-Business Environments: An International Perspective on Value Creation of E-Business in the Financial Services Industry," *Journal of Management Information Systems* (21:1), pp. 17–54. (https://doi.org/10.1080/07421222.2004.11045797).

Zhu, K., Kraemer, K. L., and Xu, S. 2006. "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business," *Management Science* (52:10), pp. 1557–1576. (https://doi.org/10.1287/mnsc.1050.0487).

Zhu, K., Kraemer, K., and Xu, S. 2003. "Electronic Business Adoption by European Firms: A Cross-Country Assessment of the Facilitators and Inhibitors," *European Journal of Information Systems* (12:4), pp. 251–268. (https://doi.org/10.1057/palgrave.ejis.3000475).

Zibuschka, J., Kurowski, S., Roßnagel, H., Schunck, C. H., and Zimmermann, C. 2019. "Anonymization Is Dead – Long Live Privacy," in *Lecture Notes in Informatics*, H. Roßnagel (ed.), Bonn: Open Identity Summit 2019.

Zolas, N., Kroff, Z., Brynjolfsson, E., McElheran, K., Beede, D. N., Buffington, C., Goldschlag, N., Foster, L., and Dinlersoz, E. 2020. *Advanced Technologies Adoption and Use By U.S. Firms: Evidence From the Annual Business Survey*. (https://doi.org/10.3386/w28290).

Zöll, A., Olt, C. M., and Buxmann, P. 2021. "Privacy-Sensitive Business Models: Barriers of Organizational Adoption of Privacy-Enhancing Technologies," in *Proceedings of the 29th European Conference on Information Systems*. (https://aisel.aisnet.org/ecis2021_rp/34/).

Zolnowski, A., Christiansen, T., and Gudat, J. 2016. "Business Model Transformation Patterns of Data-Driven Innovations," in *Proceeding of the 24th European Conference on Information Systems*, Istanbul, Turkey. (https://aisel.aisnet.org/ecis2016_rp/146/).

Zomerdijk, L. G., and Voss, C. A. 2010. "Service Design for Experience-Centric Services," *Journal of Service Research* (13:1), pp. 67–82. (https://doi.org/10.1177/1094670509351960).