Bringing Light into the Dark Side of Digitalization: Consequences, Antecedents, and Mitigation Mechanisms

Dissertation to obtain the doctoral degree of Economic Sciences (Dr. oec.)

Faculty of Business, Economics and Social Sciences

University of Hohenheim

Institute of Marketing & Management

submitted by

Fabian Schmied

from *Augsburg, Germany*

2022

Date of disputation: September 7, 2022

Supervisor and first reviewer: Prof. Dr. Henner Gimpel

Second reviewer: Prof. Dr. Verena Hüttl-Maack

Exam chairperson: Prof. Dr. Sabine Trepte

Dean of faculty: Prof. Dr. Jörg Schiller

Abstract

As digital technologies permeate all aspects of our professional and private lives, digitalization causes profound changes for individuals, organizations, and societies. The use of digital technologies makes many activities easier, safer, faster, or more comfortable. For example, mobile health applications (e.g., medication reminders) may facilitate individuals' lives with chronic diseases. Smart home applications make many activities more convenient and less place-bound. In addition to many positive changes, digital technologies are also associated with numerous risks and side effects. For instance, increasingly ubiquitous and pervasive digital technologies amplify the threat of privacy breaches or technostress (i.e., stress resulting from the use of digital technologies). Organizations may suffer from complex information technology (IT) projects running out of time and budget. From a societal perspective, the increasing dissemination of misinformation can be seen as a negative consequence of digitalization.

Dealing with the dark side of using digital technologies is not new, but information systems (IS) research has a clear pro-IT bias and there are many negative effects that have not been sufficiently illuminated so far. The above examples show that the use of digital technologies might come along with severe negative consequences for individuals, organizations, and societies. The negative consequences can be triggered by various antecedents. For instance, technostress might be a consequence of frequent interruptions (Galluch et al., 2015)[1]. In addition to identifying the negative consequences of digitalization and their antecedents, it is particularly important to develop appropriate mitigation mechanisms. Besides research, other actors such as companies and policymakers also have a responsibility in this regard. The European General Data Protection Regulation (GDPR), for example, is designed to protect users from inappropriate use of their personal data.

This dissertation provides novel insights for IS researchers to better understand the negative consequences of using digital technologies. It contains a broad overview of the risks and side effects of digitalization and investigates related antecedents and mitigation mechanisms. To reach this goal, regarding research methods, this dissertation relies on the structured analysis of (scientific) literature and (expert) interviews as well as the analysis and interpretation of empirical data. Throughout the included research articles, the data is obtained from several

[1] Galluch, P., Grover, V., & Thatcher, J. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context. *Journal of the Association for Information Systems*, *16*(1), 1–47. https://doi.org/10.17705/1jais.00387

structured literature reviews, semi-structured interviews, and online surveys and analyzed with methods such as qualitative content analysis, exploratory factor analysis, and the Kano model, among others.

Chapter 2 contributes to the research on the negative consequences of digitalization. Section 2.1 provides a comprehensive multi-level taxonomy of the risks and side effects of digitalization (RSEDs). The 11 RSEDs and their 35 subtypes are derived from academic literature, journalistic articles, and expert interviews. Section 2.2 builds on Section 2.1 and is a substantial expansion and improvement of Section 2.1. The iterative taxonomy development process was complemented by four additional cycles. The final taxonomy comprises 11 RSEDs and their 39 subtypes. Both articles show that there is a wide range of risks and side effects of digitalization that need to be explored in more detail in the future.

Chapter 3 focuses on the antecedents of digitalization's negative consequences. Section 3.1 sheds light on individuals' concerns towards automated decision-making. The concerns are derived from academic literature and semi-structured interviews with potential users of algorithm-based technologies. This procedure has resulted in inherent concerns and concerns about potential consequences. Section 3.2 focuses on the evaluation of specific mHealth app features by potential users in Germany and Denmark. The study draws on survey data from both countries analyzed using the Kano method. Further, it comprises a quartile-based sample split approach to identify the underlying relationships between users' characteristics (e.g., privacy concerns) and their perceptions of the mHealth app features. The results show significant differences between Germans and Danes in the evaluation of the app features and demonstrate which of the user characteristics best explain these differences. Both articles shed light on possible antecedents of negative consequences (i.e., user dissatisfaction, non-use) and thus contribute to a better understanding of the occurrence of negative consequences.

Chapter 4 shows exemplary mitigation mechanisms to cope with the negative consequences of digitalization. Section 4.1 takes an organizational perspective and identifies data privacy measures that can be implemented by organizations to protect the personal data of their customers and address their privacy concerns. These measures were evaluated by analyzing data from two independent online surveys with the help of the Kano method. The implementation of most of the measures is mandatory as they are taken for granted and seen as basic needs. Nevertheless, the results indicate that customers might be delighted by the implementation of specific data privacy measures. Section 4.2 focuses on an individual perspective by presenting the concept of a privacy bot that contributes to strengthening the digital sovereignty of internet

users. With the help of the privacy bot, page-long privacy statements can be checked against previously stored individual data protection preferences. A survey among internet users has shown that the Privacy Bot and its functions would be predominantly positively received by them. Both articles provide appropriate mitigation mechanisms to cope with users' privacy concerns. These two examples show that there are a variety of ways to counter the risks and side effects of digitalization.

Overall, this dissertation contributes to the research on the adverse effects of using digital technologies without neglecting their antecedents and appropriate mitigation mechanisms. The research articles included in this dissertation identify various risks and side effects of digitalization that need to be explored in more detail in future research. The two articles on antecedents help to better understand the occurrence of negative consequences of digitalization. The development of appropriate countermeasures, two of which are exemplified in this dissertation, should result in the benefits of digital technologies outweighing their risks.

Zusammenfassung

Da digitale Technologien alle Bereiche unseres beruflichen und privaten Lebens durchdringen, bewirkt die Digitalisierung tiefgreifende Veränderungen für Individuen, Organisationen und Gesellschaften. Viele Aktivitäten werden durch den Einsatz digitaler Technologien einfacher, sicherer, schneller oder bequemer. So können beispielsweise mobile Gesundheitsanwendungen (z. B. Erinnerungen an die Einnahme von Medikamenten) das Leben von Menschen mit chronischen Krankheiten erleichtern. Smart-Home-Anwendungen machen viele Aktivitäten bequemer und weniger ortsgebunden. Neben vielen positiven Veränderungen sind digitale Technologien aber auch mit zahlreichen Risiken und Nebenwirkungen verbunden. So erhöhen die zunehmend allgegenwärtigen digitalen Technologien beispielsweise die Gefahr von Datenschutzverletzungen oder negativen Folgen für die Gesundheit der Individuen (z. B. Technostress). Bei komplexen IT-Projekten in Unternehmen kommt es häufig zu Zeit- und Budgetüberschreitungen. Aus gesellschaftlicher Sicht kann beispielsweise die zunehmende Verbreitung von Fehlinformationen als eine negative Folge der Digitalisierung angesehen werden.

Die Beschäftigung mit den Schattenseiten der Nutzung von digitalen Technologien ist nicht neu, aber die Forschung im Bereich der Informationssysteme (IS) fokussiert sich eindeutig auf die positiven Aspekte der Digitalisierung. Folglich gibt es viele negative Auswirkungen, die bisher noch nicht ausreichend beleuchtet worden sind. Die oben genannten Beispiele zeigen, dass der Einsatz digitaler Technologien mit schwerwiegenden negativen Folgen für Individuen, Organisationen und Gesellschaften einhergehen kann. Diese negativen Folgen können durch verschiedene Einflussfaktoren ausgelöst werden. Beispielsweise kann Technostress eine Folge von häufigen Unterbrechungen sein (Galluch et al., 2015)[2]. Zusätzlich zur Identifizierung der negativen Folgen der Digitalisierung und ihrer Ursachen ist es besonders wichtig, geeignete Schutzmaßnahmen zu entwickeln. Neben der Forschung stehen auch andere Akteure wie Unternehmen und politische Entscheidungsträger in der Verantwortung. Die europäische Datenschutz-Grundverordnung (DSGVO) beispielsweise soll die Nutzer:innen vor einer unangemessenen Nutzung ihrer persönlichen Daten schützen.

Diese Dissertation liefert neue Erkenntnisse für IS-Forscher:innen, um die negativen Folgen der Nutzung digitaler Technologien besser zu verstehen. Sie enthält einen breiten Überblick

[2] Galluch, P., Grover, V., & Thatcher, J. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context. *Journal of the Association for Information Systems*, *16*(1), 1–47. https://doi.org/10.17705/1jais.00387

über die Risiken und Nebenwirkungen der Digitalisierung und untersucht die damit verbundenen Ursachen und Schutzmaßnahmen. Um dieses Ziel zu erreichen, stützt sich die Dissertation forschungsmethodisch auf die strukturierte Analyse von (wissenschaftlicher) Literatur und (Expert:innen-)Interviews sowie auf die Auswertung und Interpretation empirischer Daten. In den enthaltenen Forschungsartikeln werden die Daten aus mehreren strukturierten Literaturrecherchen, halbstrukturierten Interviews und Online-Befragungen gewonnen und u.a. mit Methoden wie der qualitativen Inhaltsanalyse, der explorativen Faktoranalyse und dem Kano-Modell analysiert.

Kapitel 2 leistet einen Beitrag zur Forschung über die negativen Folgen der Digitalisierung. Abschnitt 2.1 liefert eine umfassende mehrstufige Taxonomie der Risiken und Nebenwirkungen der Digitalisierung (RSEDs). Die 11 RSEDs und ihre 35 Untertypen werden aus wissenschaftlicher Literatur, journalistischen Artikeln und Expert:inneninterviews abgeleitet. Abschnitt 2.2 baut auf Abschnitt 2.1 auf und ist eine wesentliche Erweiterung und Verbesserung von Abschnitt 2.1. Der iterative Taxonomieentwicklungsprozess wurde durch vier weitere Zyklen ergänzt. Die endgültige Taxonomie umfasst 11 RSED und 39 Untertypen. Beide Artikel zeigen, dass es ein breites Spektrum an Risiken und Nebenwirkungen der Digitalisierung gibt, das in Zukunft noch genauer erforscht werden muss.

Kapitel 3 befasst sich mit den Ursachen der negativen Folgen der Digitalisierung. Abschnitt 3.1 beleuchtet die Bedenken von Individuen gegenüber automatisierten Entscheidungen. Die Bedenken wurden aus wissenschaftlicher Literatur und halbstrukturierten Interviews mit potenziellen Nutzer:innen algorithmusbasierter Technologien abgeleitet. Dieses Verfahren hat zu inhärenten Bedenken und Bedenken hinsichtlich möglicher Konsequenzen geführt. Abschnitt 3.2 konzentriert sich auf die Bewertung spezifischer Funktionen von mHealth-Apps durch potenzielle Nutzer in Deutschland und Dänemark. Die Studie basiert auf Umfragedaten aus beiden Ländern, die mit der Kano-Methode analysiert wurden. Darüber hinaus umfasst sie einen quartil-basierten Stichproben-Split-Ansatz, um die zugrundeliegenden Beziehungen zwischen den Merkmalen der Nutzer (z.B. Bedenken hinsichtlich des Datenschutzes) und ihrer Wahrnehmung der Funktionen von mHealth-Apps zu ermitteln. Die Ergebnisse zeigen signifikante Unterschiede zwischen Deutschen und Dänen bei der Bewertung der App-Funktionen und zeigen, welche der Nutzermerkmale diese Unterschiede am besten erklären. Beide Artikel beleuchten mögliche Ursachen negativer Folgen (z.B. Unzufriedenheit der Nutzer, Nichtnutzung) und tragen so zu einem besseren Verständnis des Auftretens negativer Folgen bei.

Kapitel 4 zeigt beispielhafte Schutzmaßnahmen zur Bewältigung der negativen Folgen der Digitalisierung. Abschnitt 4.1 nimmt eine organisationale Perspektive ein und identifiziert Datenschutzmaßnahmen, die von Unternehmen umgesetzt werden können, um die personenbezogenen Daten ihrer Kund:innen zu schützen und deren Datenschutzbedenken zu berücksichtigen. Diese Maßnahmen wurden durch die Analyse von Daten aus zwei unabhängigen Online-Umfragen mit Hilfe der Kano-Methode evaluiert. Die meisten Maßnahmen werden als Basisfaktoren angesehen, deren Umsetzung durch die Unternehmen obligatorisch ist. Dennoch zeigen die Ergebnisse, dass die Kunden durch die Umsetzung bestimmter Datenschutzmaßnahmen begeistert werden können. In Abschnitt 4.2 wird eine individuelle Perspektive eingenommen, indem das Konzept eines Privacy Bots vorgestellt wird, der zur Stärkung der digitalen Souveränität von Internetnutzer:innen beiträgt. Mithilfe des Privacy Bots können seitenlange Datenschutzerklärungen mit zuvor gespeicherten individuellen Datenschutzpräferenzen abgeglichen werden. Eine Umfrage unter Internetnutzer:innen hat ergeben, dass der Privacy Bot und seine Funktionen von ihnen überwiegend positiv aufgenommen werden würden. Beide Artikel beschreiben geeignete Schutzmaßnahmen, um den Datenschutzbedenken der Nutzer:innen gerecht zu werden. Diese beiden Beispiele zeigen, dass es eine Vielzahl von Möglichkeiten gibt, den Risiken und Nebenwirkungen der Digitalisierung zu begegnen.

Insgesamt leistet diese Dissertation einen Beitrag zur Erforschung der negativen Auswirkungen der Nutzung von digitalen Technologien, ohne deren Ursachen und geeignete Schutzmaßnahmen zu vernachlässigen. Die in dieser Dissertation enthaltenen Forschungsartikel zeigen verschiedene Risiken und Nebenwirkungen der Digitalisierung auf, die in der zukünftigen Forschung noch genauer untersucht werden müssen. Die beiden Artikel zu den Ursachen helfen, das Auftreten von negativen Konsequenzen der Digitalisierung besser zu verstehen. Die Entwicklung geeigneter Schutzmaßnahmen, von denen zwei in dieser Dissertation beispielhaft vorgestellt werden, sollte dazu führen, dass die Vorteile der digitalen Technologien ihre Risiken überwiegen.

Table of contents

List of tables

List of figures

1 Introduction

1.1 Motivation[3]

"Technology isn't inherently good or bad in the first place. It just is. […] It's on us to make sure we're amplifying the good and not amplifying the bad."

— Adam Mosseri, Head of Instagram, 2019[4]

The emergence and adoption of digital technologies may well prove to be the fastest development in human history (Berger et al., 2018). Digitalization denotes "the manifold sociotechnical phenomena and processes of adopting and using [digital] technologies in broader individual, organizational, and societal contexts" (Legner et al., 2017, p. 301). It causes profound changes for individuals, organizations, and societies (Majchrzak et al., 2016; Tarafdar et al., 2015; Vial, 2019).

First and foremost, however, digital technologies were used in an organizational context (Matt et al., 2019). Early corporate digital technologies range from word processing, spreadsheet software, and email programs to enterprise resource planning systems. Of course, individuals used IT, but they mainly did so as representatives of an organization (Matt et al., 2019). Since those early days, the use of digital technologies has extended far into the private sphere (Matt et al., 2019). This development was illustrated by TIME magazine and their person of the year 2006, who was simply named "You". With this unusual choice, the editors wanted to acknowledge the millions of people who were anonymously contributing user-generated content to new platforms such as Wikipedia, YouTube, and MySpace (Grossman, 2006). The editors described Web 2.0 as "a tool for bringing together the small contributions of millions of people and making them matter." In doing so, they recognized the new possibilities that digital technologies opened up for community building and collaboration (Grossman, 2006). In the rather short interim, it has ceased to be of special note let alone surprising that billions of commercial and non-commercial users create digital content, and that they do so every day (Jain & Qian, 2021). These days, our focus tends to favor more advanced digital technologies, such as blockchain, artificial intelligence (AI), and the Internet of Things (IoT). Indeed, in 2021, Gartner's annual Hype Cycle of Emerging Technologies incorporated technologies such

[3] Since it is in the nature of a cumulative dissertation that it consists of individual research papers, this chapter (Introduction) as well as the last chapter (conclusion) partly comprise content taken from the research papers included in this dissertation. To improve the readability of the text, I omit the standard labeling of these citations.

[4] https://time.com/5619999/instagram-mosseri-bullying-artificial-intelligence/

as non-fungible tokens, quantum machine learning, or AI-augmented design (Gartner, 2021). It is fair to say, then, that digital technologies now permeate all aspects of our professional and private lives (Berger et al., 2018; Legner et al., 2017; Matt et al., 2019). The importance of digitalization for developed societies is reflected in the fact that the topic has been discussed in great depth, not only in academia but also in broadsheet newspapers, magazines, and indeed in the wider political discourse (Legner et al., 2017). So dominant a force has digitalization become that its proponents have for several years now led a discussion on whether access to the internet should be recognized as a new human right (Web Foundation, 2020). Meanwhile, governments around the globe have introduced digital services, first to make current interactions between public authorities and citizens more convenient, and to scale up their service delivery capabilities (Amend et al., 2021).

Digitalization presents many potential benefits for individuals, organizations, and societies. As far as individuals are concerned, perhaps the most attractive of those benefits is the fact that digital technologies have made multiple activities we perform in our daily lives not only easier but safer, faster, and more comfortable. For instance, fitness trackers allow individuals to collect and analyze their health data without consulting physicians or other medical experts (Matt et al., 2019). Other mobile health applications (mHealth apps) help their users to better cope with chronic diseases, such as diabetes. Alternatively, they strengthen health competence or adherence, for instance by means of medication reminders, or they store and exchange health-related data, an example of this being the ever more common use of digitalized personal health records (Aitken et al., 2017; Jimenez et al., 2019; Knöppler et al., 2016). Meanwhile, products are becoming ever more convenient due to their smartification, a new age term that denotes the extension of formerly non-digital products by digital functions and services, including such devices as the smart home or the smart fridge, all of which can now be controlled remotely (Matt et al., 2019; Schuh et al., 2019).

From an organizational perspective, digitalization has been found to provide great potential "in terms of innovation, connectivity, efficiency and productivity improvements" (Berger et al., 2018, p. 1). With the help of digital technologies, companies can improve the customer experience, achieve more efficient operations, and establish new business models (Fitzgerald et al., 2014; Hosseini et al., 2017). Evidence of this came with the rapid proliferation of e-scooters, only made possible by virtue of their connection to a smartphone app as a booking and payment platform.

From a societal perspective, digitalization has recently proven enormously helpful in combating global crises, such as the COVID-19 pandemic and the climate crisis (Seidel et al., 2017; Thomas et al., 2020). As most of us have now learned by way of personal experience, remote communication and collaboration tools can help one stay connected and avoid unnecessary contacts (Thomas et al., 2020). Furthermore, since modern IS can trace and collect data about the pandemic, they can help us better understand the crisis and support political decision-making (Thomas et al., 2020). With regard to the climate crisis, digital technologies can be used to reduce global energy consumption as they make it possible and indeed rather simple to increase the efficiency of energy demand and supply systems, which in due course will lead to a reduced energy consumption and less CO_2 emissions (Watson et al., 2010). Also worth mentioning in this context is that digital technologies are often seen as a critical tool that can or rather must be used to achieve the Sustainable Development Goals formulated by the United Nations (United Nations, 2021; Venkatesh et al., 2020). Acting with this conviction, the Indian government has invested in information and communications technologies for development (ICT4D) initiatives such as internet-enabled kiosks for rural India, the purpose of which is to provide broad access to accurate medical information (Venkatesh et al., 2020).

Digitalization comes along with many opportunities for individuals, organizations, and societies. From an individual perspective, digital technologies make many activities easier, safer, faster, or more comfortable. For instance, fitness trackers allow individuals to collect and analyze their health data without consulting physicians or other medical personnel (Matt et al., 2019). Other mobile health applications (mHealth apps) help to cope with chronic diseases (e.g., diabetes), to strengthen health competence or adherence (e.g., medication reminders), or to store and exchange health-related data (e.g., personal health records) (Aitken et al., 2017; Jimenez et al., 2019; Knöppler et al., 2016). Besides, the smartification of products (i.e., the extension of formerly non-digital products by digital functions and services; e.g., smart home, smart fridge) makes them more convenient (e.g., by the ability to control the devices remotely) (Matt et al., 2019; Schuh et al., 2019). From an organizational perspective, digitalization provides great potential “in terms of innovation, connectivity, efficiency and productivity improvements” (Berger et al., 2018, p. 1). With the help of digital technologies, companies may improve the customer experience, achieve more efficient operations, and establish new business models (Fitzgerald et al., 2014; Hosseini et al., 2017). For example, the rapid spread of e-scooters was only made possible by their connection to a smartphone app as a booking and payment platform. From a societal perspective, digitalization can help combat global crises such as the COVID-19 pandemic or the climate crisis (Seidel et al., 2017; Thomas et al., 2020).

For instance, remote communication and collaboration tools help stay connected and avoid unnecessary contacts (Thomas et al., 2020). Further, information systems (IS) tracing and collecting data about the pandemic help understand the crisis and support political decision-making (Thomas et al., 2020). Concerning the climate crisis, digital technologies can reduce global energy consumption by increasing the efficiency of energy demand and supply systems leading to reduced energy consumption and less CO_2 emissions (Watson et al., 2010). In addition, digital technologies are often seen as a critical tool for achieving the Sustainable Development Goals formulated by the United Nations (United Nations, 2021; Venkatesh et al., 2020). For instance, the Indian government invests in information and communications technologies for development (ICT4D) initiatives such as internet-enabled kiosks for rural India to provide access to accurate medical information (Venkatesh et al., 2020).

These valuable opportunities notwithstanding, digitalization is not without risks and unintended side effects that can affect not only individuals, but also organizations and entire societies. It ought to be noted that the use of digital technologies can lead to severe negative consequences for individuals. For instance, their ubiquity in modern life and pervasive influence on our routine activities have made us more vulnerable to the threat of privacy breaches, i.e., incidents of misuse of an individual's personal information (Acquisti et al., 2006). Perhaps the most egregious and therefore the most discussed of these privacy breaches was the Cambridge Analytica scandal. During Donald Trump's 2016 presidential campaign, the company used illegally obtained social media data to target individuals with political advertising tailored specifically to their character profiles (Perrigo, 2018). Yet even when no such ulterior motive is at work, individuals can suffer from the increasing onslaught of digital technologies in the form of technostress, which is a form of stress caused by excessive exposure to digital technologies (Maier et al., 2015; Pirkkalainen & Salo, 2016; Tarafdar et al., 2007). Discussions of technostress often focus on its negative impact on individuals' productivity, but grave concerns are spreading due to its adverse effects on mental health.

Of further concern is that long-established organizations often feel the strain of increased competitive pressure as multiple new market players are capable of introducing disruptive digital business models. For instance, Airbnb and Uber were able to disrupt entire industries overnight because their business models no longer depended on their competitors' gradual acquisition of accommodation or vehicles (Berger et al., 2018; Müller et al., 2020; Ng et al., 2019). Similarly distressing has been the trend that has seen numerous organizations falter or incur additional expenditures due to complex IT projects, many of which have proven to be

challenging, unfit for purpose or so costly as to exceed budgets (Flyvbjerg & Budzier, 2011; Guggenmos et al., 2019; Neumeier & Wolf, 2017).

As for the multitude of societal risks posed by digitalization, an obvious example is the fast and furious dissemination of misinformation via social media, commonly referred to as fake news (Lee, 2016). Especially during the COVID-19 pandemic, health misinformation, such as the dangerous rumor that highly concentrated alcohol may kill the COVID-19 virus, was spread far and wide and at a rate dramatically higher than any quackery promoted in the pre-digital age (Gu & Li, 2020; Islam et al., 2020). Yet even when we look beyond such times of crisis, the use of digital technologies raises several ethical issues that concern societies at large. As illustrated by MIT's moral machine, the development of self-driving cars requires the resolution of a moral dilemma (Awad et al., 2018). Unforeseen incidents may necessitate a decision whether to harm or indeed kill the occupants of a vehicle rather than other road users (Awad et al., 2018). Such examples show that, for all of its life-enhancing opportunities, digitalization poses numerous worrying and as yet unanswered questions.

1.2 Exploring digitalization's negative consequences, its antecedents, and mitigation mechanisms

In addition to the many advantages, the use of digital technologies can have severe negative consequences (Tarafdar et al., 2015). Research articles from various disciplines that address the negative consequences of specific situations or actions also investigate related antecedents and mitigation mechanisms (see Table 1.2-1 for descriptions of these constructs).

Construct	**Description**
Antecedent	Cause or origin of something occurring or happening later
Consequence	Result or effect of something occurring or happening earlier (situation or action)
Mitigation mechanism	Act of reducing harmful or unpleasant consequences

Table 1.2-1: Overview of important constructs when analyzing dark side phenomena

Those constructs can also be found in the IS discipline and its research on the negative consequences of using digital technologies. For instance, Tarafdar et al. (2015, p. 165) describe mitigation mechanisms as necessary as "they can alleviate dark side phenomena and/or their negative outcomes." Mitigation mechanisms can reduce the probability of a negative event occurring and alleviate the consequences of the event (Tarafdar et al., 2015). To develop suitable mitigation mechanisms, it is necessary to understand the consequences themselves and their antecedents. With this in mind, Pirkkalainen and Salo (2016) provide an overview of IS

research on four specific dark side phenomena, i.e., technostress, information overload, IT addiction, and IT anxiety. For each of these dark side phenomena, they discuss relevant research articles and show whether the author(s) focus(es) on one or more aspects out of the triad of antecedents, consequences, and mitigation mechanisms (Pirkkalainen & Salo, 2016). The following paragraphs illustrate this discussion for two of the four dark side phenomena (i.e., technostress and IT addiction).

In efforts to do so, a large body of research on the phenomenon of technostress and its antecedents has been amassed. To date, however, studies on suitable mitigation mechanisms have been few and far between (Pirkkalainen & Salo, 2016). Notable is the research that led Galluch et al. (2015) to identify interruptions as the main antecedents of technostress, in response to which control mechanisms have been proposed to prevent or at least alleviate technostress. Tarafdar et al. (2019) have also discussed numerous techno-stressors as antecedents of technostress, including techno-overload, techno-invasion, techno-uncertainty, techno-insecurity, and techno-complexity. The mitigation mechanisms they proposed are so-called persuasive systems, which is to say systems that can measure negative outcomes, provide diagnostics, and suggest solution approaches, such as reducing the number of applications or taking a break. Having looked at the big picture, Pirkkalainen and Salo (2016) concluded that IS researchers ought to focus more attention on the identification of mechanisms that mitigate technostress, particularly outside the work environment where the main focus has usually been. Instead, they suggest, we should look at the use of digital technologies for everyday and leisure purposes.

In their work on IT addiction, Xu et al. (2012) addressed the phenomenon of online game addiction among adolescents and identified game-related needs for relationships, escapism, and mastery as antecedents (Pirkkalainen & Salo, 2016). Suitable mitigation mechanisms, Xu et al. (2012) found, can be attention switching, rationalization, and parental monitoring (Pirkkalainen & Salo, 2016). Meanwhile, Aziz et al. (2021) have developed an expert system to help with the diagnosis of online game addiction among adolescents and thus mitigate the risks of excessive gaming. Dealing with this same issue, Da Zhan and Chan (2012) had described several antecedents of online game addiction, such as social interaction, social experience, game flow, human needs, and peer influence. They proposed the development of governmental regulations to prevent or reduce online game addiction among adolescents.

Overall, Pirkkalainen and Salo (2016) summarize that there are still significant gaps in research on the four dark side phenomena discussed in their literature review. The research gaps

relate mainly to antecedents and mitigation mechanisms (Pirkkalainen & Salo, 2016). Tarafdar et al. (2015) also argue that research regarding mitigation mechanisms is relatively sparse. As those examples show, there is already IS research on the negative consequences of digitalization, its antecedents, and appropriate mitigation mechanisms. Still, more research is needed in this direction, especially on antecedents and mitigation mechanisms. This dissertation follows those calls for further research and examines the negative consequences of digitalization and its antecedents and appropriate mitigation mechanisms.

The challenge, then, remains and bears repeating: the negative consequences of using digital technologies, much like their antecedents and suitable mitigation mechanisms, require an as yet incomplete differentiated view because they play out on multiple levels (see Table 1.2-2), ranging from individuals and organizations to society at large (Wang et al., 2015). These levels are adapted from Costello et al. (2013) and based on the ecological systems theory of Bronfenbrenner (1981). Since early digital technologies were primarily used in a professional context, the associated negative consequences mainly affected this organizational level. Now, however, digital technologies permeate all aspects of our professional and private lives (Berger et al., 2018; Legner et al., 2017; Matt et al., 2019). It follows the same unfortunate logic, therefore, that the negative consequences of digitalization are now increasingly occurring at individual and societal levels.

Level		**Description**
Individual	Nanosystem / personal	Adverse intrapersonal effects (behavioral, cognitive, bio-medical, etc.)
	Microsystem / interpersonal	Adverse effects on the interaction and relationships in small groups, including the family, workgroup, and friendship networks
Organizational	Mesosystem / organizational	Adverse effects on individual social institutions that have organizational characteristics and are governed by formal (and informal) rules and regulations
	Exosystem / inter-organizational	Adverse effects on the interactions and relationships among organizations
Societal	Macrosystem / socio-economic	Adverse effects on society and economy at large as well as on nation-states and supranational relations

Table 1.2-2: Overview of the levels affected by negative consequences of digitalization

As the table illustrates, a differentiated view of the issue will appreciate that the aforementioned negative consequences like technostress and IT addiction occur on an individual level. Cybersecurity breaches and cybercrime, on the other hand, are examples of negative consequences that primarily affect organizations. Meanwhile, societies at large are affected by such

large-scale trends as extremism and the manipulation of democratic elections through digital technologies.

This dissertation looks at these complex issues with the necessary wide-angle lens to provide an overview of digitalization's negative consequences across all levels. Sharpening the focus on antecedents and suitable mitigation mechanisms will further require a close look at certain dark side phenomena, such as rogue algorithms and the dissolution of privacy, that affect specific levels, particularly the individual and organizational.

Rogue algorithms refer to complex and networked algorithms that exceed human understanding and control. Evermore decisions previously made by humans are supported or replaced by algorithms (Martin, 2019; Wachter et al., 2017). Due to the increasing complexity of these algorithms, individuals will eventually lose control of self-learning systems as their auditability becomes impossible. Already, there are numerous examples of algorithms that discriminate against people based on their gender or origin. After all, AI-based systems that learn from a given set of training data tend to perpetuate the status quo implicit in the given data set. For instance, Amazon's AI-based system was designed to support the company's hiring process and ended up favoring men since it recognized that, prior to its inception, the majority of positions had been held by men (Fritz et al., 2020; Liel & Zalmanson, 2020). For this reason, many users still have reservations about using self-learning systems.

Similar reservations remain about the dissolution of privacy, which is to say the actual or perceived loss of freedom due to an inappropriate intrusion by other individuals, organizations, or states. This issue has been discussed in broad terms, both in the research community and in society at large. Some have described privacy issues as being among the most important ethical, legal, social, and political issues of the information age (Hong & Thong, 2013; Smith et al., 2011). Experts in the field tend to focus on the seven information privacy concerns, identified by Smith et al. (1996), those being collection, unauthorized secondary use (internal), unauthorized secondary use (external), improper access, errors, reduced judgment, and combining data. Such privacy-related issues are becoming increasingly important as digital technologies are extending their reach ever deeper into our professional and private lives (Berger et al., 2018; Legner et al., 2017; Matt et al., 2019).

1.3 Aim and outline of this dissertation

It is regrettable, if somewhat understandable, that the IS discipline is affected by a widespread pro-digital bias (Addas & Pinsonneault, 2015; Chen & Wei, 2019; Clarke, 2016). Although

IS researchers have discussed some dark side phenomena associated with extensive use of digital technologies, such as technostress and data privacy issues, there is no full account of the multiple risks and side effects caused by the current rate and range of digitalization. In an effort to broaden the scope of examination, this dissertation sets out to identify, structure, and communicate the most severe adverse risks and side effects of developing, producing, using, and disposing of digital technologies. In short, it examines the *negative consequences* of digitalization for *individuals*, *organizations*, and *societies*. Hence, the first two research articles included in this dissertation are dedicated to the risks and side effects of digitalization. However, the dissertation is not limited to identifying the *negative consequences* of digitalization but also aims to understand its *antecedents* and show examples of how to positively deal with the risks and side effects (i.e., to present suitable *mitigation mechanisms*). Therefore, the dissertation comprises two research articles that focus on *antecedents* of the *negative consequences* of using digital technologies. The first article identifies and structures the reservations many users have about automated decision-making (ADM), while the second considers privacy concerns as *antecedents* of how satisfied users are with 26 mHealth app features. To look further at the positives, the dissertation also includes two research articles that propose specific *mitigation mechanisms* for data privacy issues. The first article takes an *organizational* perspective, the second an *individual* perspective. By thus expanding the scope of the investigation, this dissertation contributes to the rigorous stocktaking and active management of the adverse effects associated with the use of digital technologies, as demanded by various IS researchers (McCarthy et al., 2020; Tarafdar et al., 2015).

Figure 1.3-1 structures the research articles included in this dissertation. The matrix is divided into columns to distinguish between *antecedents*, *consequences*, and *mitigation mechanisms*, while the horizontal rows show which levels are affected, i.e., the *individual* or the *organizational* and *societal*.

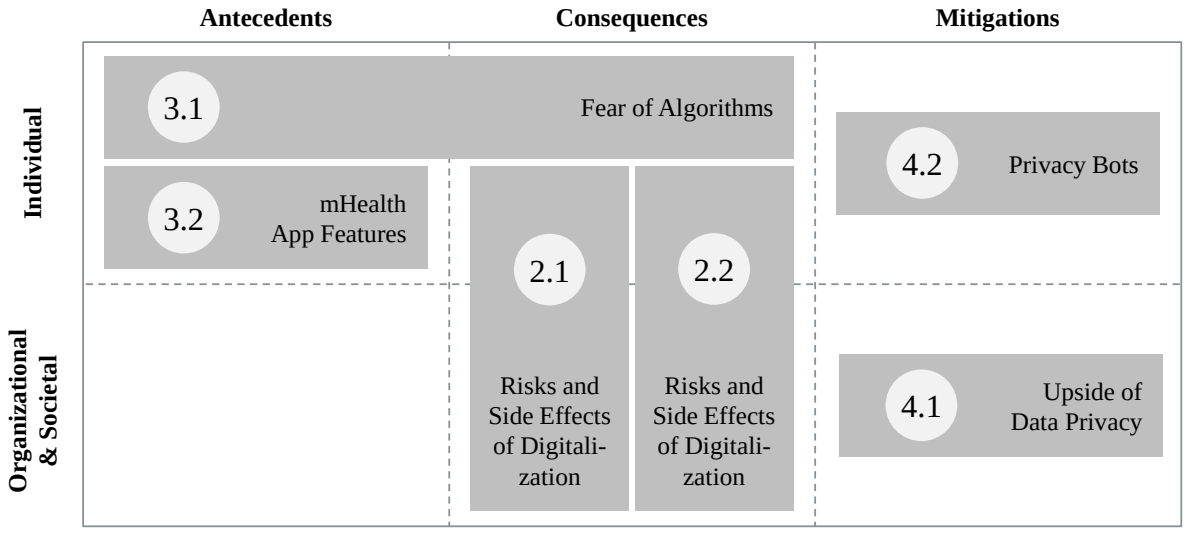


Figure 1.3-1: Structure of this dissertation

Further, Table 1.3-1 provides an overview of the structure of this dissertation with brief summaries of all included research articles. Further provided are the titles, objectives, methods, and co-authors of each of these articles. Chapter 2 addresses the negative consequences of digitalization, Chapter 3 its antecedents, and Chapter 4 the mitigation mechanisms for specific dark side phenomena.

Chapter #	Title of the Research Article Current Publication Status	Objective	Method and Data	Co-Authors
Chapter 2: Negative consequences of digitalization				
2.1	Risks and Side Effects of Digitalization: A Multi-Level Taxonomy of the Adverse Effects of Using Digital Technologies and Media[5] *Published in the Proceedings of the 27th European Conference on Information Systems (ECIS) in Stockholm and Uppsala, Sweden (2019)*	Identifying, structuring, and communicating the most severe risks and side effects of digitalization	Structured literature review, expert interviews, taxonomy development	Gimpel, Henner
2.2	Illuminating the Dark Side: A Multi-Level Taxonomy of the Risks and Side Effects of Digitalization[6] *Working paper*	Identifying, structuring, and communicating the most severe risks and side effects of digitalization	Structured literature review, expert interviews, taxonomy development	Gimpel, Henner
Chapter 3: Antecedents of digitalization's negative consequences				
3.1	Fear of Algorithms: A Synopsis of Concerns About Automated Decision-Making *Working paper*	Identifying concerns about ADM to improve ADM-related offers and services that account for the concerns of individuals	Structured literature review, qualitative content analysis of semi-structured interviews	Bayer, Sarah Waldmann, Daniela
3.2	Understanding the Evaluation of mHealth App Features Based on a Cross-Country Kano Analysis *Published in Electronic Markets, Volume 31, Issue 4, 765-794 (2021)*	Explaining the evaluation of specific personal health record (PHR) app features for user satisfaction	Identification of mHealth app features, quantitative online survey in two countries, Kano model	Gimpel, Henner Manner-Romberg, Tobias Winkler, Till
Chapter 4: Mitigation mechanisms to cope with the negative consequences of digitalization				
4.1	The Upside of Data Privacy – Delighting Customers by Implementing Data Privacy Measures *Published in Electronic Markets, Volume 28, Issue 4, pp. 437-452 (2018)*	Deriving data privacy measures for companies to address customers' data privacy concerns and analyzing the consequences their implementation may have for customer satisfaction	Derivation based on sources from the fields of research as well as practice, two quantitative online surveys, Kano model	Gimpel, Henner Kleindienst, Dominikus Nüske, Niclas Rau, Daniel
4.2	Privacy Bots - Digital Assistants for More Transparency on the Internet[7] *Published in Datenschutz und Datensicherheit, Volume 43, Issue 1, pp. 28-32 (2019)*	Developing a concept for a privacy bot that strengthens users' digital sovereignty	Conceptualization, quantitative online survey	Nüske, Niclas Olenberger, Christian Rau, Daniel

Table 1.3-1: Overview of the research articles in this dissertation

[5] Please note that I was the lead author of this research article
[6] Section 2.1 and 2.2 are closely related as described in the text below.
[7] The original article was published in German and translated into English for this dissertation.

Chapter 2 focuses on risks and side effects, which is to say on the *negative consequences* of digitalization. Section 2.1 provides an overview of 11 RSEDs and the subtypes that affect *individuals*, *organizations*, and *societies*. Two of those RSEDs (*supporting delinquents* and *impairment of health*) and their subtypes are discussed in detail. Section 2.2 expands the findings of Section 2.1 by giving an overview of 11 adapted RSEDs and their 39 subtypes, all of which are described in detail. The two research articles on the RSEDs are further outlined in the following.

The dark side of IT usage is hardly a new development, nor is the acknowledgment of the research community that this is worthy of our attention. By and large, however, research has focused on a scattering of dark side phenomena, such as data privacy issues or technostress. These days, digital technologies are being developed at breakneck speed, so much so that we are engaging with them in evermore ways, and indeed in evermore profound ways, be it in our professional or our private lives. It is, therefore, becoming a matter of vital importance that we gain a holistic understanding of the unintended adverse effects of using digital technologies. To this end, Section 2.1 has the following research aim (RA):

> ***RA:*** *The aim is to identify, structure, and communicate the most severe RSEDs for individuals, organizations, and societies.*

The taxonomy is developed in line with the procedure suggested by Nickerson et al. (2013). The RSEDs are identified in various iterations by analyzing academic literature, journalistic articles, and expert interviews. The taxonomy is intended to create a common understanding of the most severe RSEDs, which in turn is intended to help IS scholars as well as practitioners in their efforts to develop appropriate mitigation mechanisms. When presenting the taxonomy at the European Conference on Information Systems, it had an appropriate intermediate state for publishing it and obtaining feedback from the IS community. However, the overarching taxonomy development process was not finished yet. Thus, work on the taxonomy proceeded after the conference.

Section 2.2 pursues the same research objective as Section 2.1 but does so by substantially expanding and further refining the work of Section 2.1. Indeed, the iterative taxonomy development process went through four additional cycles. As a result, the adapted taxonomy presented in Section 2.2 incorporates feedback from seven blind peer reviews as well as that of participants at three conferences. Furthermore, over 750 academic articles published in renowned IS journals and those presented at the leading international IS conference were ana-

lyzed at this stage. Finally, a range of further insights gleaned from multiple journalistic articles was incorporated into the taxonomy (published between August 2018 and December 2020). As such, the taxonomy presented in section 2.2 is a substantially improved version of the result presented in section 2.1. As both sections have the same overarching aim and, in part, the same results, some text in section 2.2 reiterates what is stated in section 2.1. A reader only interested in the final result might skip over section 2.1 and directly enter section 2.2. Yet, section 2.1 is included in this cumulative dissertation as it was an important and published intermediate step in the research process.

Chapter 3 focuses on the *antecedents* of the negative effects caused by digitalization. It includes two research articles that address those on the individual level. This is further explored in Section 3.1, the focus here shifting to the concerns that *individuals* have about ADM and its potential for *negative consequences*. Section 3.2 considers privacy concerns as an antecedent to the (dis)satisfaction that users experience when engaging with specific mHealth app features. Both of these research articles on *antecedents* of the *negative consequences* of digitalization are discussed in more detail below.

An ever-increasing number of decisions previously made by humans is supported or replaced by algorithms (Martin, 2019; Wachter et al., 2017). Potential use cases range from producing news articles to supporting recruitment processes and calculating recidivism scores (Angwin et al., 2016; Diakopoulos, 2016; van den Broek et al., 2019). Issues such as the complexity of algorithms and the related lack of transparency have led to grave concerns about the use of ADM. To date, some of these issues have been examined in highly specific uses cases, but these have added up to little more than cursory glances, rather than a comprehensive overview of the chief concerns that *individuals* see when dealing with ADM. To achieve the latter, Section 3.1 aims to answer the following research question (RQ):

***RQ:** Which concerns do individuals have about the use of automated decision-making?*

In answer to this question, a structured literature review was conducted in conjunction with a qualitative content analysis of semi-structured interviews. The overview of the concerns that users have developed about ADM includes concerns about the consequences of using ADM as well as the inherent concerns that may be considered as antecedents of specific consequences. It may, therefore, serve as a foundation on which third parties are better able to develop responsible and transparent ADM-related offers and services.

Section 3.2 sheds light on how the impact of specific mHealth app features on user satisfaction is evaluated in two different healthcare contexts, i.e., those of Germany and Denmark. Differences between subgroups are explained by examining varying user characteristic antecedents. The research article answers the following two research questions:

> ***RQ1:*** *How do potential users in Germany and Denmark evaluate a broad set of specific PHR features?*
>
> ***RQ2:*** *Do user characteristics (specifically privacy concerns, mHealth literacy, mHealth self-efficacy, and adult playfulness) explain the differences in the evaluation of PHR features by potential users in Germany and Denmark?*

Among the chief *antecedents* considered in this research article are the privacy concerns that users have been developing to an ever-increasing degree. These privacy concerns are particularly important in the context of mHealth apps, as personal medical data is especially sensitive and vulnerable to privacy breaches (Anderson, 2007; Appari & Johnson, 2010). This is why, in the digitalization of healthcare, privacy concerns pose some of the main barriers to the acceptance and use of healthcare technologies (Anderson, 2007). The empirical investigation conducted for this research article indicates that the evaluation of several mHealth app features is significantly affected by users' privacy concerns. This research article, then, aims to contribute to a better understanding of what constitutes and influences user satisfaction when engaging with a variety of mHealth app features.

Chapter 4 focuses on *mitigation mechanisms* to cope with the negative consequences of digitalization. This chapter includes two research articles. The first research article (Section 4.1) takes an *organizational* perspective and advocates a positive approach to data privacy by identifying and evaluating a set of data privacy measures that could be implemented by organizations to increase user satisfaction. The second research article (Section 4.2) is practitioner-oriented and takes an *individual* perspective and conceptualizes a privacy bot that helps to protect the digital sovereignty of its users. The following paragraphs provide further details about both of these research articles.

Section 4.1 examines how customers perceive specific data privacy measures taken by companies to address their customers' privacy concerns. The research produced to date has mostly dealt with data privacy as a necessary evil that companies simply cannot prevent. More research work is to be done on specific data privacy measures which can account for customers' concerns. With this in mind, this research article looks at the implementation of specific data privacy measures as an appropriate *mitigation mechanism* to cope with data privacy issues

associated with the use of digital technologies. The article in this section answers the following two research questions:

> ***RQ1:*** *Which data privacy measures can companies take?*
>
> ***RQ2:*** *Are some of these measures perceived as attractive measures that delight customers?*

In answer to the first research question, the article compiles 32 specific measures to deal with customers' data privacy concerns. These measures are based on academic literature, legislative texts, corporate privacy statements, and expert interviews. The second research question is answered by applying the Kano model based on data obtained through two online surveys. As the results of these surveys indicate, the implementation of most measures must be deemed mandatory as those measures are considered as basic needs of must-be quality, whose implementation is expected by customers. However, there are also measures of attractive quality that can create a competitive advantage. Overall, this research article outlines a mechanism to mitigate a specific dark side phenomenon of digitalization, i.e., data privacy issues. Furthermore, it indicates the potential to please customers with the wider implementation of certain data privacy measures.

Section 4.2 primarily addresses IS practitioners by conceptualizing a digital assistant that helps protect the digital sovereignty of its users. The research article in this section has the following research aim:

> ***RA:*** *The article aims to conceptualize a suitable user-centered mitigation mechanism to cope with the risk of inappropriate privacy intrusions when using digital services*.

The main feature of the privacy bot is to evaluate corporate privacy statements. The article proposes three different methods to evaluate such corporate privacy statements. Based on user preferences, the privacy bot recommends whether or not a digital service should be used. Furthermore, the article discusses how this concept was evaluated by 78 internet users.

The research articles outlined above are prefaced by an introduction in Chapter 1 that includes the motivation of this dissertation, provides its theoretical foundation, and describes its outline. The research articles are then followed by a discussion and conclusion in Chapter 5. This final section further provides a summary of this dissertation's results and implications, a consideration of opportunities for further research, and an overall conclusion.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. In *International Conference on Information Systems*, Milwaukee, Wisconsin, USA.

Addas, S., & Pinsonneault, A. (2015). The many faces of information technology interruptions: a taxonomy and preliminary investigation of their performance effects. *Information Systems Journal*, *25*(3), 231–273. https://doi.org/10.1111/isj.12064

Aitken, M., Clancy, B., & Nass, D. (2017). *The Growing Value of Digital Health: Evidence and Impact on Human Health and the Healthcare Systems.* IQVIA Institute for Human Data Science. https://www.iqvia.com/insights/the-iqvia-institute/reports/the-growing-value-of-digital-health

Amend, J., Kaiser, J., Uhlig, L., Urbach, N., & Völter, F. (2021). What Do We Really Need? A Systematic Literature Review of the Requirements for Blockchain-based E-government Services. In *16th International Conference on Wirtschaftsinformatik*, Essen, Germany.

Anderson, J. G. (2007). Social, ethical and legal barriers to e-health. *International Journal of Medical Informatics*, *76*(5-6), 480–483. https://doi.org/10.1016/j.ijmedinf.2006.09.016

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks.* ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279–314. https://doi.org/10.1504/IJIEM.2010.035624

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., Bonnefon, J.-F., & Rahwan, I. (2018). The Moral Machine experiment. *Nature*, *563*(7729), 59–64. https://doi.org/10.1038/s41586-018-0637-6

Aziz, A., Setyawan, B. W., & Saddhono, K. (2021). Using Expert System Application to Diagnose Online Game Addiction in Junior High School Students: Case Study in Five Big City in Indonesia. *ISI (Ingénierie Des Systèmes D'information)*, *26*(5), 445–452. https://doi.org/10.18280/isi.260503

Berger, S., Denner, M.-S., & Roeglinger, M. (2018). The Nature of Digital Technologies - Development of a Multi-Layer Taxonomy. In *European Conference on Information Systems*, Portsmouth, UK.

Bronfenbrenner, U. (1981). *Die Ökologie der menschlichen Entwicklung: Natürliche und geplante Experimente*. Klett-Cotta.

Chen, X., & Wei, S. (2019). Enterprise social media use and overload: A curvilinear relationship. *Journal of Information Technology*, *34*(1), 22–38. https://doi.org/10.1177/0268396218802728

Clarke, R. (2016). Big data, big risks. *Information Systems Journal*, *26*(1), 77–90. https://doi.org/10.1111/isj.12088

Costello, G. J., Donnellan, B., & Curley, M. (2013). A Theoretical Framework to Develop a Research Agenda for Information Systems Innovation. *Communications of the Association for Information Systems*, *33*(1), Article 26, 433–462.

Da Zhan, J., & Chan, H. C. (2012). Government Regulation of Online Game Addiction. *Communications of the Association for Information Systems*, *30*. https://doi.org/10.17705/1CAIS.03013

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM*, *59*(2), 56–62. https://doi.org/10.1145/2844110

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing Digital Technology: A New Strategic Imperative. *MIT Sloan Management Review*, *55*(2), 1–12.

Flyvbjerg, B., & Budzier, A. (2011). Why Your IT Project May Be Riskier than You Think. *Harvard Business Review*, *89*(9), 23–25. https://doi.org/10.2139/ssrn.2229735

Fritz, A., Brandt, W., Gimpel, H., & Bayer, S. (2020). Moral agency without responsibility? Analysis of three ethical models of human-computer interaction in times of artificial intelligence (AI). *De Ethica*, *6*(1), 3–22. https://doi.org/10.3384/de-ethica.2001-8819.20613

Galluch, P., Grover, V., & Thatcher, J. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context. *Journal of the Association for Information Systems*, *16*(1), 1–47. https://doi.org/10.17705/1jais.00387

Gartner. (2021). *Gartner Identifies Key Emerging Technologies Spurring Innovation Through Trust, Growth and Change*. https://www.gartner.com/en/newsroom/press-releases/2021-08-23-gartner-identifies-key-emerging-technologies-spurring-innovation-through-trust-growth-and-change

Grossman, L. (2006, December 25). Time Person of the Year You. *TIME*, 168(26), pp. 38–41. https://web.p.ebscohost.com/ehost/detail/detail?vid=14&sid=3e3564db-7f4f-408f-823d-22fdee2e4199%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=23469016&db=buh

Gu, R., & Li, M. X. (2020). Investigating the Psychological Mechanism of Individuals' Health Misinformation Dissemination on Social Media. In *International Conference on Information Systems,* Virtual Conference.

Guggenmos, F., Hofmann, P., & Fridgen, G. (2019). How ill is your IT Portfolio? – Measuring Criticality in IT Portfolios Using Epidemiology. In *International Conference on Information Systems,* Munich, Germany.

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MISQ (MIS Quarterly)*, *37*(1), 275–298.

Hosseini, S., Roeglinger, M., & Schmied, F. (2017). Omni-Channel Retail Capabilities: An Information Systems Perspective. In *International Conference on Information Systems,* Seoul, South Korea.

Islam, M. S., Sarkar, T., Khan, S. H., Mostofa Kamal, A.-H., Hasan, S. M. M., Kabir, A., Yeasmin, D., Islam, M. A., Amin Chowdhury, K. I., Anwar, K. S., Chughtai, A. A., & Seale, H. (2020). Covid-19-Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis. *The American Journal of Tropical Medicine and Hygiene*, *103*(4), 1621–1629. https://doi.org/10.4269/ajtmh.20-0812

Jain, S., & Qian, K. (2021). Compensating Online Content Producers: A Theoretical Analysis. *Management Science*, *67*(11), 7075–7090. https://doi.org/10.1287/mnsc.2020.3862

Jimenez, G., Lum, E., & Car, J. (2019). Examining Diabetes Management Apps Recommended From a Google Search: Content Analysis. *JMIR MHealth and UHealth*, *7*(1), e11848. https://doi.org/10.2196/11848

Knöppler, K., Neisecke, T., & Nölke, L. (2016). *Digital-Health-Anwendungen für Bürger: Kontext, Typologie und Relevanz aus Public-Health-Perspektive* [Entwicklung und Erprobung eines Klassifikationsverfahrens]. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Studie_VV_Digital-Health-Anwendungen_2016.pdf

Lee, J. (2016). Opportunity or risk? How news organizations frame social media in their guidelines for journalists. *The Communication Review*, *19*(2), 106–127. https://doi.org/10.1080/10714421.2016.1161328

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Business & Information Systems Engineering*, *59*(4), 301–308. https://doi.org/10.1007/s12599-017-0484-2

Liel, Y., & Zalmanson, L. (2020). What If an AI Told You That 2 + 2 Is 5? Conformity to Algorithmic Recommendations. In *International Conference on Information Systems,* Virtual Conference.

Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. *Information Systems Journal*, *25*(3), 275–308. https://doi.org/10.1111/isj.12068

Majchrzak, A., Markus, M. L., & Wareham, J. (2016). Designing for Digital Transformation: Lessons for Informations Systems Research from the Study of ICT and Societal Challenges. *MISQ (MIS Quarterly)*, *40*(2), 267–277.

Martin, K. (2019). Designing ethical algorithms. *MIS Quarterly Executive*, *18*(2), 129–142. https://doi.org/10.17705/2msqe.00012

Matt, C., Trenz, M., Cheung, C. M. K., & Turel, O. (2019). The digitization of the individual: conceptual foundations and opportunities for research. *Electronic Markets, 29*(3), 315–322. https://doi.org/10.1007/s12525-019-00348-9

McCarthy, S., Rowan, W., Lynch, L., & Fitzgerald, C. (2020). Blended Stakeholder Participation for Responsible Information Systems Research. *Communications of the Association for Information Systems*(47), Article 33, 716–742.

Müller, M., Neumann, J., Gutt, D., & Kundisch, D. (2020). Toss a Coin to your Host - How Guests End up Paying for the Cost of Regulatory Policies. In *International Conference on Information Systems,* Virtual Conference.

Neumeier, A., & Wolf, T. (2017). Getting a Grip on IT Project Complexity â•fi Concluding to Underlying Causes. In *International Conference on Information Systems,* Seoul, South Korea.

Ng, E., Tan, B., & Meng, Tian (2019). The Dark Side of the Sharing Economy: The Negative Implications of Ridesharing for a Traditional Taxi Business. In *International Conference on Information Systems,* Munich, Germany.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336–359. https://doi.org/10.1057/ejis.2012.26

Perrigo, B. (2018, October 1). Whistle-Blower Christopher Wylie on Life After Taking Down Cambridge Analytica. *TIME*, 192(13), pp. 12–13.

Pirkkalainen, H., & Salo, M. (2016). Two Decades of the Dark Side in the Information Systems Basket: Suggesting Five Areas for Future Research. In *European Conference on Information Systems*, Istanbul, Turkey.

Schuh, G., Zeller, V., Hicking, J., & Bernardy, A. (2019). Introducing a methodology for smartification of products in manufacturing industry. *Procedia CIRP*, *81*, 228–233. https://doi.org/10.1016/j.procir.2019.03.040

Seidel, S., Bharati, P., Fridgen, G., Watson, R. T., Albizri, A., Boudreau, M.-C., Butler, T., Chandra Kruse, L., Guzman, I., Karsten, H., Lee, H., Melville, N., Rush, D., Toland, J., & Watts, S. (2017). The Sustainability Imperative in Information Systems Research. *Communications of the Association for Information Systems*, *40*, 40–52. https://doi.org/10.17705/1CAIS.04003

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MISQ (MIS Quarterly)*, *35*(4), 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MISQ (MIS Quarterly)*, *20*(2), 167–196.

Tarafdar, M., Cooper, C. L., & Stich, J.-F. (2019). The technostress trifecta - techno eustress, techno distress and design: Theoretical directions and an agenda for research. *Information Systems Journal*, *29*(1), 6–42. https://doi.org/10.1111/isj.12169

Tarafdar, M., Gupta, A., & Turel, O. (2015). Editorial: Special issue on 'dark side of information technology use': an introduction and a framework for research. *Information Systems Journal*, *25*(3), 161–170. https://doi.org/10.1111/isj.12070

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems*, *24*(1), 301–328.

Thomas, O., Hagen, S., Frank, U., Recker, J., Wessel, L., Kammler, F., Zarvic, N., & Timm, I. (2020). Global Crises and the Role of BISE. *Business & Information Systems Engineering*, *62*(4), 385–396. https://doi.org/10.1007/s12599-020-00657-w

United Nations. (2021). *Digital Government*. https://publicadministration.un.org/en/ict4d

van den Broek, E., Sergeeva, A., & Huysman, M. (2019). Hiring Algorithms: An Ethnography of Fairness in Practice. In *International Conference on Information Systems*, Munich, Germany.

Venkatesh, V., Sykes, T. A., & Zhang, X. (2020). ICT for Development in Rural India: A Longitudinal Study of Women's Health Outcomes. *MISQ (MIS Quarterly)*, *44*(2), 605–629. https://doi.org/10.25300/MISQ/2020/12342

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wang, J., Xiao, N., & Rao, H. R. (2015). Research Note—An Exploration of Risk Characteristics of Information Security Threats and Related Public Information Search Behavior. *Information Systems Research*, *26*(3), 619–633. https://doi.org/10.1287/isre.2015.0581

Watson, R. T., Boudreau, M.-C., & Chen, A. J. (2010). Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. *MISQ (MIS Quarterly)*, *34*(1), 23–38.

Web Foundation. (2020). *It's time to recognise internet access as a human right*. https://webfoundation.org/2020/10/its-time-to-recognise-internet-access-as-a-human-right/

Xu, Z., Turel, O., & Yuan, Y. (2012). Online game addiction among adolescents: motivation and prevention factors. *European Journal of Information Systems*, *21*(3), 321–340. https://doi.org/10.1057/ejis.2011.56

2 Negative consequences of digitalization

2.1 Risks and side effects of digitalization: a multi-level taxonomy of the adverse effects of using digital technologies and media

Abstract: Achieving a bright digital future requires knowing and managing the adverse effects of digitalization. The objective of this paper is to identify, structure, and communicate the most severe adverse risks and side effects of digitalization. To this end, we apply an iterative taxonomy development process informed by academic literature, journalistic articles, and expert interviews. The result is a comprehensive multi-level taxonomy of the adverse effects of IT use. The taxonomy shall serve as platform for further research on identifying and managing the risks and side effects of digitalization. It supports information system scholars in proper net benefit assessments of the effect of increasing use of ever more intelligent, interconnected, and pervasive IT-based systems. Further, it supports the anticipation and management of adverse effects in the design of such systems.

Keywords: IT use, dark side of IT, affordances, taxonomy

Authors: Henner Gimpel, Fabian Schmied

Status: This article is published in the Proceedings of the 27th European Conference on Information Systems (ECIS) in Stockholm and Uppsala, Sweden (2019) and was nominated for the award for the Best Complete Research Paper.

2.1.1 Introduction

Over the past 70 years, digital technologies and media made our lives easier, safer, healthier, and longer (Tian & Xu, 2015). Our organizations became more productive, and our economies grew (Hitt & Brynjolfsson, 1996; G. Lee et al., 2018). As a consequence, many information systems scholars focus on the positive effects of digital technologies and media. However, the use of digital technologies and media may also have adverse, unexpected, and unintended effects, especially as IT becomes ever more intelligent, interconnected, and pervasive. The Internet "dramatically transformed the world" (Kim et al., 2011, p. 675). The role of information systems scholars is to research and teach a set of diverse topics associated with IT-based systems and to inform their design and use to achieve a transformation toward the better. Despite a widespread pro-IT bias, this requires a rigorous stocktaking and active management of the risks and side effects associated with the increasing use of IT-based systems. "The recognition that ICT can have both positive and negative effects, both intended and unintended, deepens our field's theorization of ICT" (Majchrzak et al., 2016, p. 273). As information systems scholars, we should ensure that the many positive aspects of digitalization outweigh the related risks and side effects to provide net benefits. To support this, our aim is to provide a multi-level taxonomy that can contribute to a net benefit assessment of the effects of digitalization on individuals, organizations, and societies.

Studying the "dark side of IT" is not new; the term refers to a "collection of 'negative' phenomena that are associated with the use of IT, and that have the potential to infringe the well-being of individuals, organisations and societies" (Tarafdar et al., 2015, p. 61). Pirkkalainen and Salo (2016) review two decades of dark side research in the AIS Senior Scholars' Basket of Journals. They identify 37 articles and detect four types of dark side phenomena: technostress, information overload, IT addiction, and IT anxiety. This is a good starting point. However, considering only: individual-level effects; non-malicious IT use; and effects reported in top information systems journals narrows the scope of the study. Effects on an organizational or a societal level were neglected. Kim et al. (2011) present a taxonomy of the dark side of the Internet (as subset of digital technology and media). They identify technology-centric dark side effects like spam, malware, hacking, and violation of digital property rights. Further, they identify non-technology-centric dark side effects like online theft, cyberbullying, and aiding crime. All their effects base on malicious use of the Internet, that is, on digital technologies and media supporting delinquents.

Two exemplary topics show that the dark side of digitalization is broader and goes beyond the scope of even the two taxonomies of Kim et al. (2011) and Pirkkalainen and Salo (2016) combined: First, digitalization can enable complex and networked (machine learning) algorithms that are beyond proper human understanding and control. These might become discriminating leading to unjust or prejudicial treatment of different categories of people. A specific example is Google's image recognition software wrongly categorizing black people as "gorillas" (USA TODAY, 2015). Further examples are provided in the discussion. Second, digitalization contributed to the emergence of superpowerful corporations, that is, extremely influential national and supra-national institutions that might suppress competition, innovation, and regulation. A specific example is the public debate around Facebook's relation to U.S. political events, privacy problems, and conflict between the firm's social mission and profit growth (TIME, 2018, Vol. 191, Issue 15). These are only two exemplary topics to demonstrate that the dark side of digitalization is broader than prior taxonomies – further topics and examples become evident below.

The "Bright ICT" initiative by the AIS takes a positive stance on shaping the future and simultaneously acknowledges the existence of negative aspects. The initiative's first core research topic—the "Bright Internet"—aims at reducing cybercrime (J. K. Lee, 2015). Here, too, one sees a yet narrow focus. The aim of this paper is to complement these approaches and move the discourse to the next level. Given the present disenchantment with Silicon Valley high tech and media companies and the perception that digital technologies and media contribute to the destruction of democratic processes—to cite just two examples—we believe the time is right for the creation of a "holistic map" of the adverse effects of digitalization; this would mobilize scholars to participate in illuminating the dark side of IT.

The objective of this paper is to identify, structure, and communicate the most severe risks and side effects of digitalization (RSED hereafter). Development, production, use, and disposal of digital technologies and media (DTM hereafter) may have consequences beyond the immediate aim. Identifying and assessing these consequences is difficult because of their ambivalence, complexity, and novelty, besides the biases of observers. To overcome these challenges, we apply a taxonomy development methodology and triangulate the RSED by: reviewing extant knowledge encapsulated in academic writing; reviewing journalistic reflections on digitalization; and conducting workshops and interviews with scholars from various disciplines.

The taxonomy contributed by the paper shall serve as platform for further theoretical and empirical research on identifying and managing RSED. According to Gregor (2006), the taxonomy is a "theory for analyzing", that is the most basic type of theory that describes and classifies by summarizing the commonalities found in discrete observations. According to Majchrzak et al. (2016), the taxonomy is a "theory of the problem" that aims to elucidate a specific challenge. Majchrzak et al. (2016) assert that researchers often have a pro-IT bias and subconsciously avoid acknowledging IT-related harms. They call for researchers to explicitly consider the unintended consequences of IT artefacts and IT use. Our taxonomy provides a structure to respond to this call in a systematic way and overcome some subconscious biases.

From an ethical standpoint, the rapid evolution of digitalization creates normative uncertainty that calls for a reflection on the ethical aspects of DTM's role in various social contexts. Our paper and future work building on it shall enrich the societal dialogue on whether to accept RSED and how to manage them, given the substantial (net) benefits of digitalization.

2.1.2 Methodology

We follow the iterative taxonomy development procedure suggested by Nickerson et al. (2013) to identify, structure, and communicate the most severe RSED. The taxonomy's intended users are information systems scholars. The meta-characteristic is the types of risks and side effects associated with the actualization of affordances of DTM. The ending conditions are the ones suggested by Nickerson et al. (2013, Tables 2 and 3).

So far, we have completed five cycles of the iterative taxonomy development process (Nickerson et al., 2013). Each cycle followed an empirical-to-conceptual approach of identifying (new) RSED and their common characteristics, as well as grouping and structuring RSED. Each cycle builds on the previous one so that the taxonomy matures over time. The implementation of the cycles partly overlapped in time. Cycle 1 identified RSED from the academic literature. Specifically, we searched in the AIS eLibrary for the keywords "dark side" and "bright side" as well as the keywords arising from a full text search for "dark side". Here and in the following cycles focusing on literature search, identified papers were analyzed by the research team in order to identify RSED, subtypes of RSED, manifestations of RSED and to infer the conceptualization of RSED and their adversity. Cycle 2 centers around two workshops with scholars from the disciplines of ethics and law, as cycle 1 suggested that these disciplines' perspectives could be especially relevant for understanding the conceptualization of RSED and to understand conventional (ethical and legal) categorizations of effects and attribution of responsibility and accountability. Cycle 3 reviewed journalistic reflections on

digitalization in leading print media. Specifically, we reviewed all editions of the weekly magazines TIME and DER SPIEGEL from June 2017 until July 2018. Both cover relevant topics globally. Whereas TIME focuses more on the US, the world's largest economy, Der Spiegel focuses on Germany—the largest economy in Europe. While reviewing additional newspapers or magazines could in principle provide additional insights, we restricted the search to one lead magazine per country in the assumption that highly relevant topics should be covered by these magazines. In terms of country focus, China might appear as a natural additional country to look for lead media. However, limits to free speech in China impede this. Journalistic articles are a useful supplement to scientific contributions as they have a shorter lead time in picking up news than academic outlets and are not bound by the scope of individual disciplines or communities. In addition, they shape public perception, attitudes and norms towards DTM and RSED. Cycle 4 returns to academic publications for a systematic review of all volumes of MIS Quarterly and the Journal of the AIS (search for »"dark side" OR downside OR risk OR adverse OR negative OR "side effect"« in title or abstract without any time restriction; the 156 results obtained processed manually). Cycle 5 focuses on expert interviews from other disciplines to broaden our focus and to put findings from the previous cycles in perspectives from other disciplines. Specifically, we searched for scholars in ethics, criminology, sociology, psychology, and economic and social history as the prior cycles suggested that these disciplines relate to the RSED. In each of these disciplines we looked for a scholar with more than 10 years of research experience, a strong publication record in his field of expertise. To gain a fresh perspective, we specifically did not look for scholars highly involved in digitalization research; however, we searched for experts who have some weak ties to studying digitalization to assure a minimum amount of reflection of the digitalization already before the interview. Given these search criteria, we identified five experts (one from each of the aforementioned disciplines), all of whom agreed to take part in an individual semi-structured, one-hour interview. All interviews were recorded. Recordings and field notes were subsequently analyzed using open substantive coding. Coding constantly stipulated conceptual ideas that were constantly compared against the emerging taxonomy of RSED. Beyond identifying new RSED and their subtypes, the interviews proved useful in conceptualizing RSED and especially the adversity of RSED.

As suggested by Nickerson et al. (2013), along these cycles, we identify examples and characteristics of RSED to develop a structured presentation that is concise, robust, comprehensive, extendible, and explanatory. Conceptual-to-empirical iterations might be a fruitful addition to the taxonomy development process. One might argue that digitalization enhances the

non-digital effects. Hence, one might use a list of all adverse effects in the world and consider whether digitalization contributes to them. Second, because each affordance of DTM may lead to RSED, one might use a list of all affordances of DTM and identify potential RSED. Unfortunately, neither of these lists exists. Hence, we focus on empirical-to-conceptual iterations.

The methodology adopted has two key limitations: First, "theories of the problem […] make explicit value judgments that the situation is problematic from the perspective of certain stakeholders" (Majchrzak et al., 2016, p. 271). From our (i.e., the authors') socialization and the media reviewed, we have a culturally-biased Western perspective despite knowing that assessment of the valence of an effect depends on culture and DTM exert "a nonuniform effect on societal transformations that varies with the stage of economic development" (G. Lee et al., 2018, p. 234). Second, we only integrate RSED that are found in print or mentioned by the experts in interviews or workshops. This leads to a bias (but not an exclusive restriction) toward: rather short-term effects already observable at the current stage of digitalization and vague perceptions of potential risks emerging in the future. Thus, the specific RSED, their subtypes and manifestations and the underlying affordances of DTM will likely evolve over time.

2.1.3 Conceptualization

The following are the definitions of the primary constructs that are relevant for our research. **Digitalization** refers to the sociotechnical phenomena and processes of adopting and using digital technologies and media in individual, organizational, and societal contexts (Legner et al., 2017). **Digital technologies and media (DTM)** comprise all the electronic devices (hardware) and applications (software) that use information in the form of numerical codes (usually binary codes), as well as all the media (i.e., means and channels of general communication in society) that are coded in formats that can be processed by these devices and applications.

2.1.3.1 Risks and side effects of digitalization

Risk and side effects of digitalization (RSED) are secondary adverse effects (side effects) or the possibility of such effects (risks) because of digitalization. These are not effects of DTM themselves; they are the consequences of attitudes, decisions, and behavior related to DTM (Decker, 2013). According to common categorizations of technological consequences (Decker, 2013), RSED are (possible) secondary effects that are unwanted and unintended, but not the main ones. They may be certain or uncertain, expected or unexpected, and result from individual actions or emerge from the dynamics of collective actions. They may be direct

effects or mediated ones; further, they may moderate other effects outside the domain of digitalization. Although, side effects may describe positive and negative effects, the term is commonly used to describe adverse effects (e.g., in pharmacy and medicine). Within this paper, we focus on the negative connotation of side effects.

2.1.3.2 Adverse effects

RSED are adverse effects that cause harm. There is no objective criterion of adversity or harm shared across individuals, cultures, and ages. Judging adversity is not a matter of consensus or majority voting. Thus, we adopt the perspective of an impartial spectator assessing whether an effect is sufficiently adverse, sufficiently common, or likely to qualify as RSED. The concept of an impartial spectator was first mentioned by Adam Smith in 1759 (Raphael, 2007). A perfectly impartial and well-informed spectator is an imaginary person that guides our decisions by virtually judging our actions according to common moral principles. To support our judgement about what the impartial spectator considers as adverse, we turn to the philosophy of law: an effect is adverse if it negatively affects recognized interests in a sufficient manner. These interests might be legal interests of natural persons (e.g., integrity of life, health, and freedom of action); legal interests of legal persons (e.g., physical or intellectual property); or collective legal interests (e.g., payment of taxes). This does not imply that RSED are illegal. They have the same effect as socially harmful behavior but may also include, for example, self-harm and incidental harm. For example, social-media whitewashing and excessive exposure to images of presumably perfect bodies may lead to body image insecurity, eating disorders, and suicidal behavior, especially for (female) adolescents. Although there is nothing illegal in this, the individual legal rights of bodily integrity and right to health are curtailed, and we posit that an impartial spectator would consider this specific side effect of digital social media use as adverse.

2.1.3.3 Affordances

The theory of **affordances** stems from the ecological psychology and shed light on how animals perceive their environment (Gibson, 1979; Giermindl et al., 2017). Accordingly, affordances arise from the relationship between an artefact and a goal-oriented actor or actors. Each DTM artefact has latent affordances that are action possibilities for at least one goal-oriented actor with the relevant action capabilities (Thapa & Sein, 2018). Affordances are potentialities; to have influence, they need to be actualized. How they are perceived and actualized is contextually influenced by cultural, social, and technical factors (Thapa & Sein, 2018). When an affordance is actualized, it might have the desired main effect and it might

have risks and side effects for the very actor actualizing the affordance (self-referring) or others (externality). See Figure 2.1-1 for a stylized model. Focusing on affordances of DTM, rather than the technologies and media themselves, pinpoints that RSED are not a technological issue and are not determined by DTM. Rather, RSED depend on how: (i) we humans design, build, and use DTM and (ii) digitalization affects our attitudes, norms, and behavior. Affordances exist at multiple layers. At a low technical level, DTM allow the digitization of analog signals, persistently store digital data, and so on. Building on this, at a higher yet technical level, DTM afford encryption, big data handling, and so on. At a higher sociotechnical level, they afford low transaction costs, automated decisions and actions, rapid innovation and diffusion, and so on. In our study, this sociotechnical level is the main focus because it is more directly related to the RSED than the technical affordances and outlasts individual DTM.

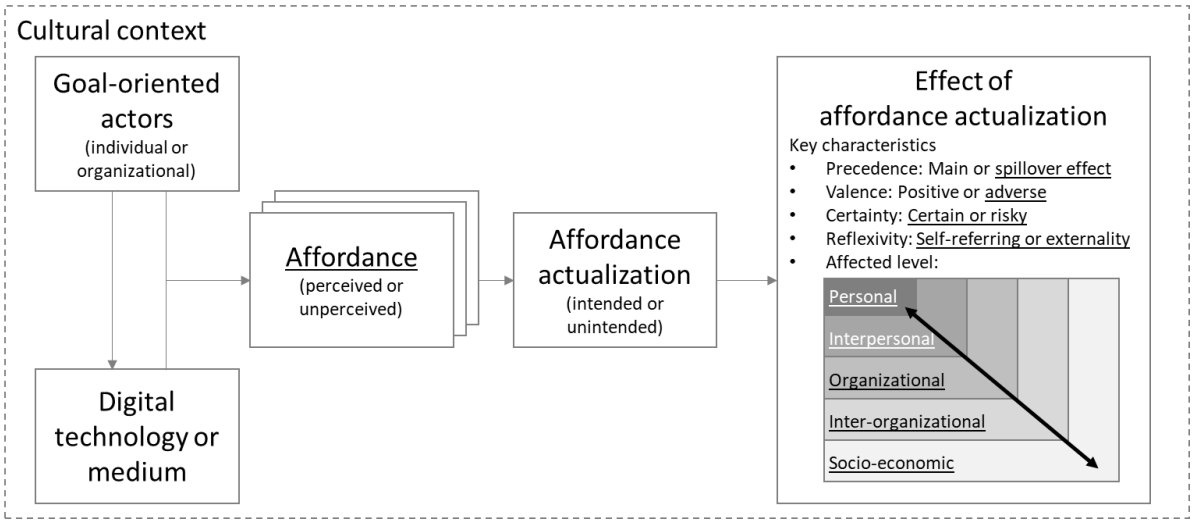


Figure 2.1-1: Stylized model of the emergence and types of effects of affordance actualization (underlining indicates focus of the present paper)

2.1.3.4 Affected level

The actualization of affordances can affect multiple levels, ranging from an individual person to society at large. Specifically, we consider five levels (see Table 2.1-1) that are similar to those in Costello et al. (2013) and based on Bronfenbrenner's ecological systems theory. Effects can propagate from one level to the other. An example are effects like technostress from IT unreliability (personal level), which might reduce individuals' socializing (interpersonal level) and work performance (organizational level).

Level	Description	Example of specific risks and side effects
Individual / personal	Adverse intrapersonal effects (behavioral, cognitive, bio-medical, etc.)	Negative psychological effects, such as IT anxiety or technostress
Microsystem / interpersonal	Adverse effects on the interaction and relationships in small groups including the family, work group, and friendship networks	Personal attacks, such as cyberbullying or digital sex crimes
Mesosystem / organizational	Adverse effects on individual social institutions with organizational characteristics with formal (and informal) rules and regulations for operation	IT operational risks, such as system malfunction
Exosystem / inter-organizational	Adverse effects on the interactions and relationships among organizations	Market power of quasi-monopolies hindering competitors and suppressing other companies
Macrosystem / societal	Adverse effects on society and economy at large as well as on nation states and supranational relations	Unscrupulous public discourse, such as hate speech in social media or an "artificial intelligence singularity"

Table 2.1-1: Overview on level affected by risks and side effects of digitalization

2.1.4 Taxonomy of risks and side effects of digitalization

RSED and their subtypes are the core of the taxonomy. They are defined in Table 2.1-2. In the following, RSED are printed in bold font, their subtypes in bold and italic font. To illustrate the rather abstract RSED and subtypes, the subsequent text provides manifestations of the subtypes and even more specific individual examples. Further, the subtypes of the RSED are related to affordances of DTM and the level they affect. Framing the RSED always includes the word "can" to highlight the potentiality rather than determinism of its occurrence. The descriptions of the subtypes put the adverse effects in the foreground in definitive terms. This does not imply that they are universally true today or in the future. They might only apply under specific circumstances or might be risks perceived from today's point of view.

For clarity of the presentation, RSED (level 1, highest level of abstraction) are written in italic bold font; subtypes of the RSED (level 2) in plain bold font; manifestations of the subtypes (level 3) italic font; and specific examples of the manifestations (level 4, lowest level of abstraction) in plain font.

Table 2.1-2 defines all 11 RSED and 35 subtypes. For space restrictions, the subsequent discussion of manifestations and examples is limited to 2 of the 11 RSED. The mapping of the 35 subtypes to affordances and affected levels is fully displayed in Figure 2.1-2.

Risk or side effect (RSED)	Subtypes of the RSED
Adverse exchange: Digitalization can facilitate the exchange of information or goods that may be desired by the transaction partners but whose effect is socially undesirable.	**Unscrupulous public discourse:** Objectionable public exchange of information and socially harmful forms of public discourse via DTM.
	Socially undesired transactions: DTM-enabled conclusion of economic transactions that are socially undesirable.
Supporting delinquents: Digitalization can make it easier for malefactors to do harmful deeds and thereby promotes the occurrence of harmful deeds.	**Personal attacks:** Non-criminal attacks among individuals via DTM.
	Cybercrime: Criminal activities carried out in part or fully via DTM.
	Aggravation of prosecution: Criminal prosecution by investigating authorities becoming more difficult due to DTM.
	Cyberterrorism: The politically motivated use of DTM to cause severe disruption or widespread fear in society.
	Cyberwarfare: Use of DTM to disrupt the activities of a state or organization, especially the deliberate attacking of DTM for strategic or military purposes.
Adverse economic shifts: Digitalization can shift economic equilibria and thus may place some parties in a worse position than they would be without digitalization.	**Displacement of traditional structures:** Supplanting traditional economic structures due to DTM harms beneficiaries of the traditional structures.
	Superpowerful corporations: Extremely influential national and supranational institutions and/or quasi-monopolies due to DTM create dependencies and suppress competition, innovation, and regulation.
	Loss of international competitiveness: Nation states and regions loose competitiveness as economic location in global competition due to innovation in DTM along with regional agglomeration and network effects.
Shifting political control: Digitalization can shift political powers and dynamics and may facilitate political changes that are undesirable for a substantive majority of people.	**Trend towards extremism:** Extreme measures or views gain political influence due to DTM.
	Political regimes strengthening control: Autocrat regimes using DTM to strengthen and lengthen their political control.
	Lack of policy making: Retarded enactment and revision of laws and policies regarding DTM-related progress creates an insufficient regulation.
Vulnerable IT operations: Digitalization can worsen or stop organizational operations, as critical DTM assets may not be available or working as expected.	**IT operational risks:** The risks of DTM-related losses resulting from inadequate or failed DTM-based systems or processes.
	Failure propagation: Failures propagate among DTM-based interconnected systems within organizations or across value networks.
Impairment of health: Digitalization can adversely affect individuals' health.	**Reduction of psychological health:** DTM-related infliction of mental disease, illness, or malfunction.
	Addiction and follow-up problems: Persistent, compulsive, and excessive use of DTM at an intensity that leads to individually harmful cognitive or behavioral adaptation. Note: Addiction to DTM is a special form of reduction of psychological health. Its relevance and specificity justify identifying it as a separate subtype.
	Reduction of physical health: DTM-related infliction of bodily disease, illness, or malfunction.
Environmental deterioration: Resource requirements originating from digitalization can change environmental sustainability to the worse.	**Climate impact of energy demand:** Negative climate change triggered by energy demand along the lifecycle of digital technologies.
	Consumption of material resources: Unsustainable level of use of material resources to manufacture digital technologies without proper recycling or reuse.
Ethical challenges: Digitalization can lead to new ethical dilemmas or change how ethical dilemmas are resolved.	**Dissolution of privacy:** DTM-related actual or perceived loss of freedom from unauthorized intrusion by other people or organizations.
	Dehumanization of work: DTM-triggered worsening of work conditions that deprives work of positive humane qualities.
	Loss of autonomy to act: Reduced individual freedom from external control or influence resulting from DTM use.
	Erosion of solidarity: DTM-triggered reduction of social and economic support commonly based on a sense of togetherness and advocacy for one another.

	Ethical programming: Designing, coding, and/or training DTM in a way that their causal agency is non-reductionist and in line with underlying human moral agency.
	Diffusion of responsibility: Lack of accountability for actions and their consequences in DTM-based actor networks.
Ambivalent decision environment: Digitalization can put decision-makers in undesired situations of untrustworthy or contradictory information on facts and agency.	**Uninformative information:** Assumed information becoming uninformative in DTM-based environments characterized by information overload, filtering, and questionable trustworthiness.
	Uncertain agency: Lack of transparency of the nature and agency of technical or social actors in DTM-based systems.
Undesirable behavioral adaptation: Digitalization can lead to a change of traditional competencies and behaviors in a socially undesirable manner.	**Technology-reliance along with increasing incompetence:** Increasing reliance of DTM leading to loss of socially or individually desirable human competencies.
	Data fixation: Reduction of the perception of the world to what is recorded and communicated in digital technologies and media in the form of data.
	Resistance to change and uncertainty: Opposition to change as a reaction to the uncertainty and partial perceived, dreaded, detrimental effects of change.
	Distraction from a principal activity: Harmful loss of focus on a principal activity due to the simultaneous use of DTM.
Losing control over algorithms: Digitalization can enable complex and networked algorithms that are beyond proper human understanding and control.	**Lack of auditability:** Algorithms encoded in DTM not being available for methodical examination and review.
	Discriminating algorithms: Use of algorithms encoded in DTM leading to unjust or prejudicial treatment of different categories of people.
	Technological singularity: An artificial superintelligence as a specific digital technology abruptly triggering runaway technological growth, resulting in detrimental effects for humanity.

Table 2.1-2: Overview of RSED and related subtypes

As first example, we consider the RSED ***supporting delinquents***: **Personal attacks** as subtype of this RSED manifests in *violent cyber-attacks* like cyberbullying (J. K. Lee, 2015), cybermobbing, cyberstalking. Such violent crime in the cyberspace is fostered by DTM allowing for low-cost anonymity or unverified pseudonyms in online media and simplified broadcasting via bulk e-mails or in social media. A more specific related manifestation are *digital sex-attacks* like revenge porn, cyber-grooming, sexting (TIME, 2017, Vol. 190, Issue 2/3; DER SPIEGEL, 7/2018). The third key manifestation of **personal attacks** are *physical violence caused by symbolic display of physical violence in computer games*. All these effects occur on an inter-personal level, as they involve the personal relationship between at least one attacker and at least one victim.

Cybercrime is a further subtype of ***supporting delinquents***. Cybercriminal activities comprise *cyber-enabled crime* (i.e., traditional crimes, such as fraud or theft that are facilitated by DTM), *cyber-dependent crime* (i.e., crimes that evolved after the emergence of specific DTM), and *platform crime* (i.e., crimes that are even more technology-focused and use for example the characteristics of botnets) (Schirrmacher et al., 2018). The manifold examples of **cybercrime** include (identity) theft (Kim et al., 2011; DER SPIEGEL, 41/2017), ransomware,

fake shops, computer fraud, chargeback fraud (Guo et al., 2018), concealment of data, and unauthorized sharing of digital content (Beekhuyzen et al., 2015). Cybercriminal activities are facilitated by DTM as they enable criminals to act anonymously, provide a tremendously high interconnectedness, and an ever-increasing amount of innovations and new possibilities (J. K. Lee, 2015; Schirrmacher et al., 2018). Cybercriminal activities may harm individuals, organizations or societies at large as proven by the WannaCry attack in 2017 (Schirrmacher et al., 2018).

Another subtype of ***supporting delinquents*** is the **aggravation of prosecution** that comprise inter alia the *technological and organizational backwardness of law enforcement authorities* that prevents for example the identification of anonymous perpetrators (TIME, 2017, Vol. 190, Issue 2/3). This effect is fostered by the rapid innovation and diffusion of new DTM. Another manifestation is the *predictability of police actions* that are planned by using algorithms (cf. predictive policing and predictive tax assessment) (Ashby & Tompson, 2017). A third manifestation is the *difficulty of prosecution beyond national borders* that is required due to the supranationalism of DTM such as the World Wide Web, which is emblematic for the high interconnectedness of DTM (TIME, 2017, Vol. 190, Issue 2/3). As societies at large aim at prosecuting perpetrators, the **aggravation of prosecution** is an effect that impairs on a societal level.

Cyberwarfare as a further subtype of ***supporting delinquents*** occurs on a supranational level and comprise manifestations such as *espionage*, *sabotage*, *propaganda*, or *economic disruption* (Hay & LaFountain, 2017; Kim et al., 2011; DER SPIEGEL, 2/2018). In many countries, there are national programs to establish and strengthen cyberwarfare capabilities (Kim et al., 2011). The **cyberwarfare** is enabled by the low-cost ubiquity of DTM and the rapid innovation and diffusion of new technologies that may lead to a strategic advantage towards competitors and enemies. Warlike actions that are enabled by DTM affect the societal level.

Finally, the RSED ***supporting delinquents*** comprises **cyberterrorism** as fifth subtype. The threat of **cyberterrorism** is enlarged by the fact that (critical) infrastructures, such as transportation, energy or telecommunication have become vulnerable due to a high level of interconnectedness (J. K. Lee, 2015). As **cyberterrorism** affects (critical) infrastructures, this subtype occurs on a societal level.

As a second example, we consider the RSED ***impairment of health***: The **reduction of psychological health** as a subtype of ***impairment of health*** comprises the manifestation *reduced mental health from excessive use of DTM*. Related effects that may occur are for example

sleep disorder (TIME, 2017, Vol. 190, Issue 19; DER SPIEGEL, 41/2018) or burnout (Pirkkalainen & Salo, 2016). Further the reduction of psychological health manifests in *technostress (digital stress)*, i.e., stress that results directly from the use of DTM (Galluch et al., 2015; Maier et al., 2015; Pirkkalainen & Salo, 2016; Tams et al., 2018), *IT anxiety* (Thatcher & Perrewé, 2002), and *body image insecurity* (e.g., social media images from super thin models may lead to insecurity and eating disorders) (TIME, 2017, Vol. 190, Issue 19). The manifold manifestations of the **reduction of psychological health** are fostered primarily by the high social interconnectedness and the ubiquity of DTM. As any health impairment the effects harm on an individual level. The **reduction of psychological health** is already strongly covered in extant information systems research like, for example, reviewed by Pirkkalainen and Salo (2016).

Another more specific subtype of ***impairment of health*** is **addiction and follow-up problems**. An addiction to DTM may result in serious mental or physical complaints, such as depressions or overweight (DER SPIEGEL, 46/2017). An *excessive smartphone or internet usage* is fostered by persuasive technologies based on business models that focus on eyeball time, that is, the time a visitor spends on a specific app or website (TIME, 2018, Vol. 191, Issue 15). Smartphone addiction is caused by a lack of self-regulation (Soror et al., 2015). The *excessive usage of computer games* allows users to escape from problems in other domains by experiencing power, achieving an instant gratification, and being part of a community of gamers (Ledder, 2013; DER SPIEGEL, 1/2018). Such addictions may lead to a *worsening of human cognition* (e.g., less deep thinking, less nuanced ideas, worse memory), a *reduction of emotional intelligence* (e.g., empathy) (TIME, 2017, Vol. 190, Issue 27/28), a neglect of responsibilities (e.g., at school, at work), a *deterioration of adolescents' mood* (e.g., loneliness, envy, suicidal thoughts) (Pirkkalainen & Salo, 2016), and an impaired development of the self-image due to reduced intense, personal contact. Furthermore, frequent users of DTM may develop a *fear of missing out* (Ledder, 2013). Additionally, there is some research that link *changes to children's brains* to media multitasking (TIME, 2018, Vol. 191, Issue 15; TIME, 2017, Vol. 190, Issue 19). The subtype **addiction and follow-up problems** may be traced back to the low-cost ubiquity of DTM and affects primarily on an individual level.

Additionally, the RSED ***impairment of health*** manifests in the **reduction of physical health**. There may be a **reduction of physical health** that results *directly from excessive use of DTM*, such as short-sightedness, lack of activity, and obesity (DER SPIEGEL, 41/2018). Further, the use of DTM may indirectly cause a reduction of physical health, e.g., *the spread of infectious diseases*. For example, the introduction of Craigslist in the USA led to an increased ratio

of HIV infections due to the possibility of arranging physical meetings between people who have not met before (Chan & Ghose, 2014). Other indirect effects are for example *injuries caused by distraction* (e.g., car accidents that result from the use of smartphones while driving). The **reduction of physical health** is primarily fostered by the high social interconnectedness and the low-cost ubiquity of DTM. As any health-related issues, the **reduction of physical health** affects on an individual level.

There are cross-relations between the different subtypes of ***impairment of health***: Addiction is a special form of psychological illness; psychological and physical illness may be mutually dependent. Three of the four dark side phenomena identified in the extensive literature review by Pirkkalainen and Salo (2016) belong to the RSED impairment of health, namely technostress, IT addiction, and IT anxiety. Their fourth dark side phenomenon – information overload – belongs to the RSED ambivalent decision environment.

These two examples – the RSED supporting delinquents and impairment of health – illustrate the manifestations and examples underlying the RSED and their subtypes as well as the reasoning on the affordances of DTM and the affected level. Figure 2.1-2 lists all 35 subtypes, relates them to the respective affordances and levels affected and (by color coding) to the 11 RSED. The different sizes and overlays of boxes have only graphical reasons and do not indicate similarity or importance.

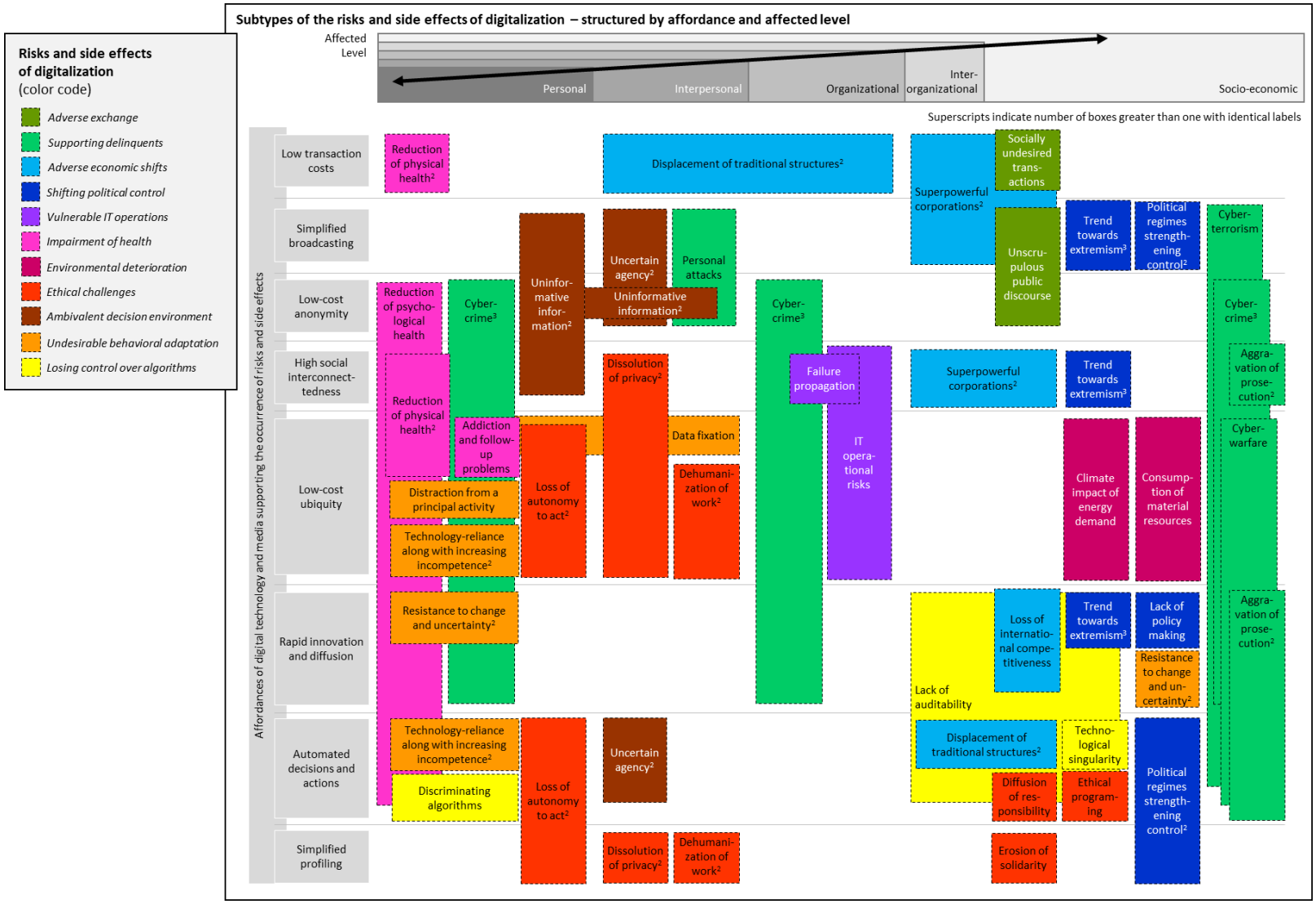


Figure 2.1-2: Maps of risks and side effects of digitalization and their subtypes by affordances and levels affected

2.1.5 Discussion and conclusion

The contribution of this paper is a taxonomy of the risks and side effects of digitalization (RSED). Our taxonomy provides a holistic map of RSED at different levels ranging from the individual to society at large. Specifically, the taxonomy comprises 11 RSED, and their 35 subtypes.

This holistic perspective broadens the conceptualization of the dark side of IT use. It includes phenomena previously studied under the label "dark side of IT" as, for example, discussed by Tarafdar et al. (2015) and Pirkkalainen and Salo (2016). These prior dark side phenomena are primarily included in the RSED ***impairment of health***, ***ambivalent decision environment***, and ***vulnerable IT operations***. Phenomena included in the taxonomy of the dark side of the Internet presented by Kim et al. (2011) belong to the RSED ***supporting delinquents***. Our taxonomy further comprises additional phenomena studied in information systems but not under the label 'dark side'. Examples include echo chambers and filter bubbles (included in the RSED ***ambivalent decision environment***) and privacy (included in the RSED ***ethical challenges***). Beyond that, the taxonomy covers perceptions of current negative effects and potential future risks that are hardly yet addressed in information systems research like technology-reliance along with increasing human incompetence (included in 'undesirable behavioral adaptations'), discriminating algorithms (included in 'losing control over algorithms'), and cyberterrorism (included in 'supporting delinquents').

The intended users of our taxonomy of RSED are primarily information systems scholars. Due to the broad character of our taxonomy, we see various fields of application in information systems research. However, the taxonomy may be adopted in other disciplines, such as criminology, psychology, and political science that also study digitalization from their disciplinary perspectives.

For scholars, the taxonomy provides a terminology of RSED that may be observed in business and everyday life, but – to some extent – have not yet been discussed in scientific literature. The terminology of RSED may be adopted in future research projects considering the effects of digitalization. Further, it may help to identify focus areas of previous research and gaps to focus on in the future.

In development of new DTM-based systems, design science researchers may consider the affordances and can use the taxonomy for a first identification of potential RSED. Additionally, researchers may take a complementary perspective by systematically considering all lev-

els affected starting with the one (s)he wishes to improve but also considering potential externalities at other levels. At each level, the researcher should evaluate whether the related RSED may occur when using the new IT-based system.

In behavioral science, researchers may use our taxonomy as a basis for manifold research questions. For instance, empirical research should evaluate the importance of the single RSED for the different levels affected in order to enable a prioritization for the development of appropriate countermeasures. Furthermore, the taxonomy may be helpful to examine the perception of digitalization within groups of different cultures, ages, or professions.

Further, practitioners working on the analysis and design of DTM-based systems can use our taxonomy in order to identify potential RSED related to the use of specific IT-based systems. With that knowledge, practitioners may choose DTM-based systems that minimize the effects of RSED, develop appropriate countermeasures, or at least inform about the potential RSED. An example: A developer working on an artificial-intelligence-enabled assistance system (Maedche et al., 2019) might identify the affordances of the system including automated decisions on behalf of its user. The developer might then use the map of RSED presented in this paper and identify "discriminating algorithms" as an RSED subtype that might originate from this affordance. Investigating the issue deeper, the developer who was previously unaware of the issue might search the news for examples. For instance, in 2015, a programmer revealed that Google's image recognition software categorized black people as "gorillas" (USA TODAY, 2015). Further, in 2016, Microsoft launched a Twitter account for Tay, a self-learning chatbot. Twitter users were engaged to communicate with Tay. As Tay rapidly adopted insulting and racist comments from other users, the chatbot was shut down on the same day (The Guardian, 2016). To dig deeper, the developer might turn to academic literature and find a discussion that being non-discriminatory is an important moral principle but biased training data might lead algorithms to become discriminatory (Maedche et al., 2019). There, the developer will find further examples, specifically Amazon's presumably sexist recruitment support system (no longer operational) and Northpointe's presumably racist recidivism scores used in the US criminal justice system (currently operational). Looking further at the map of RSED, the developer will see many other RSED subtypes related to the affordance of automated decisions. Considering the description of these affordances, the developer might start considering how to ensure ethics-by-design for her or his system.

Policy experts can use the taxonomy of RSED to evaluate whether present legislation is sufficient to cover the effects of innovative DTM. For instance, our taxonomy shed light on the

negative effects of DTM on individuals who need to be protected by legislation in a particular way. By an earlier identification of (potential) RSED, the taxonomy may help to reduce the retarded enactment and revision of laws that are affected by the socio-technical progress.

As any research, our taxonomy of RSED comes along with limitations. As digitalization is enabled by a multitude of innovative DTM that evolve continuously, also the RSED will change over time. Potentially, some of the RSED will disappear, others will change, and additional RSED will appear. Hence, our taxonomy should be seen as a snapshot of recent RSED. Having multiple layers of abstraction and focusing on affordances rather than individual technologies, we expect the top-level RSED to remain up-to-date for five or ten years. However, at latest beyond that, they need periodic review and refinement.

As we exclusively considered current RSED, future research may give an outlook on potential RSED related to emerging DTM. By focusing on weekly magazines, interview partners, and workshop participants from Germany and the USA, we took a primarily Western perspective. In addition, the taxonomy of RSED may be biased by the authors' Western moral principles. Hence, further research may shed light on different perceptions of RSED between various cultural areas.

Although, we tried to broaden our view by identifying relevant RSED by studying the weekly magazines TIME and DER SPIEGEL and by conducting expert interviews with researchers from various disciplines (e.g., ethics, criminology, sociology), we then focused on academic literature from IS discipline to verify and illustrate the RSED. Hence, the integration of academic articles from other disciplines may be an appropriate extension to our work.

Furthermore, upcoming research should examine the impact of the identified RSED and develop appropriate countermeasures for individuals, organizations and societies at large. Depending on the respective RSED, this research question should be examined in joint research projects with scientists from appropriate disciplines (e.g., criminology, psychology, political science). By evaluating whether users of DTM are aware of the related RSED, researchers should identify potential information gaps (within certain groups) that may be addressed by future educational campaigns.

Senior IS scholars "have called for adopting a "positive lense" in IS research" (Agogo & Hess, 2017, p. 1). Yet, we believe that our discipline benefits from a detailed and comprehensive theoretical perspective on the dark side of IT use and digitalization. This is especially true as information systems scholars tend to have a pro-IT bias and need support in overcoming this bias (Majchrzak et al., 2016). Adverse effects of the increasing use of digital technologies and

media are a reality and they are increasingly present in the perception of many and in mass media. We as information systems scholars need a sound understanding of these effects in order to support the public debate and to mitigate the risks and side effects to digitalization with the overall aim to contribute to the net benefits of digitalization. Metaphorically speaking one could say that you have to know the corners and angles of the dark side if you want to provide light. Our taxonomy maps the dark side of digitalization. As theory of the problem and theory for analysis, it provides a basis for illuminating the dark side.

References

Agogo, D., & Hess, T. J. (2017). "Yin and Yang": Integrating the Bright Side into Dark Side Research in IS. In *Americas Conference on Information Systems,* Boston, Massachusetts, USA.

Ashby, M. P. J., & Tompson, L. (2017). Routine Activities and Proactive Police Activity: A Macro-scale Analysis of Police Searches in London and New York City. *Justice Quarterly*, *34*(1), 109–135.

Beekhuyzen, J., Hellens, L. von, & Nielsen, S. (2015). Illuminating the underground: the reality of unauthorised file sharing. *Information Systems Journal*, *25*(3), 171–192. https://doi.org/10.1111/isj.12069

Chan, J., & Ghose, A. (2014). Internet's Dirty Secret: Assessing the Impact of Online Intermediaries in HIV Transmission. *MISQ (MIS Quarterly)*, *38*(4), 955–976.

Costello, G. J., Donnellan, B., & Curley, M. (2013). A Theoretical Framework to Develop a Research Agenda for Information Systems Innovation. *Communications of the Association for Information Systems*, *33*(1), Article 26, 433–462.

Decker, M. (2013). Technikfolgen. In A. Grunwald (Ed.), *Handbuch Technikethik* (pp. 33–38). Verlag J. B. Metzler. https://doi.org/10.1007/978-3-476-05333-6_6

Galluch, P., Grover, V., & Thatcher, J. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context. *Journal of the Association for Information Systems*, *16*(1), 1–47. https://doi.org/10.17705/1jais.00387

Gibson, J. J. (1979). *The Ecological Approach to Visual Perception*. Lawrence Erlbaum Associates.

Giermindl, L., Strich, F., & Fiedler, M. (2017). Why do you NOT use the Enterprise Social Network? Analyzing Non-Users' reasons through the lens of Affordances. In *International Conference on Information Systems,* Seoul, South Korea.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MISQ (MIS Quarterly)*, *30*(3), 611–642.

The Guardian. (2016). *Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter*. https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

Guo, Y., Bao, Y., Stuart, B. J., & Le-Nguyen, K. (2018). To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce. *Information Systems Journal*, *28*(2), 359–383. https://doi.org/10.1111/isj.12144

Hay, B., & LaFountain, S. (2017). CyberWarfare: Offensive and Defensive Software Technologies (Introduction). In *Hawaii International Conference on System Sciences,* Waikoloa Village, Hawaii, USA. http://aisel.aisnet.org/hicss-50/

Hitt, L. M., & Brynjolfsson, E. (1996). Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value. *MISQ (MIS Quarterly)*, *20*(2), 121–142.

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. https://doi.org/10.1016/j.is.2010.11.003

Ledder, S. (2013). Computerspiele. In A. Grunwald (Ed.), *Handbuch Technikethik* (pp. 258–263). Verlag J. B. Metzler.

Lee, G., Shao, B. B. M., & Vinze, A. (2018). The Role of ICT as a Double-Edged Sword in Fostering Societal Transformations. *Journal of the Association for Information Systems*, *19*(3), 209–246. https://doi.org/10.17705/1jais.00490

Lee, J. K. (2015). Research Framework for AIS Grand Vision of the Bright ICT Initiative. *MISQ (MIS Quarterly)*, *39*(2), iii–xii.

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Business & Information Systems Engineering*, *59*(4), 301–308. https://doi.org/10.1007/s12599-017-0484-2

Maedche, A., Legner, C., Benlian, A., Berger, B., Gimpel, H., Hess, T., Hinz, O., Morana, S., & Söllner, M. (2019). AI-Based Digital Assistants. *Business & Information Systems Engineering*, *61*(4), 535–544. https://doi.org/10.1007/s12599-019-00600-8

Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. *Information Systems Journal*, *25*(3), 275–308. https://doi.org/10.1111/isj.12068

Majchrzak, A., Markus, M. L., & Wareham, J. (2016). Designing for Digital Transformation: Lessons for Information Systems Research from the Study of ICT and Societal Challenges. *MISQ (MIS Quarterly)*, *40*(2), 267–277.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336–359. https://doi.org/10.1057/ejis.2012.26

Pirkkalainen, H., & Salo, M. (2016). Two Decades of the Dark Side in the Information Systems Basket: Suggesting Five Areas for Future Research. In *European Conference on Information Systems*, Istanbul, Turkey.

Raphael, D. D. (2007). *The impartial spectator: Adam Smith's moral philosophy*. Oxford University Press. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10220188

Schirrmacher, N.-B., Ondrus, J., & Tan, F. T. C. (2018). Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack. In *Pacific Asia Conference on Information Systems*, Yokohama, Japan.

Soror, A. A., Hammer, B. I., Steelman, Z. R., Davis, F. D., & Limayem, M. M. (2015). Good habits gone bad: Explaining negative consequences associated with the use of mobile phones from a dual-systems perspective. *Information Systems Journal*, *25*(4), 403–427. https://doi.org/10.1111/isj.12065

Tams, S., Thatcher, J. B [Jason B.], & Grover, V. (2018). Concentration, Competence, Confidence, and Capture: An Experimental Study of Age, Interruption-based Technostress, and Task Performance. *Journal of the Association for Information Systems*, *19*(9), 857–908. https://doi.org/10.17705/1jais.00511

Tarafdar, M., D'Arcy, J., Turel, O., & Gupta, A. (2015). The Dark Side of Information Technology. *MITSloan Management Review*, *56*(2), 61–70.

Thapa, D., & Sein, M. K. (2018). Trajectory of Affordances: Insights from a case of telemedicine in Nepal. *Information Systems Journal*, *28*(5), 796–817. https://doi.org/10.1111/isj.12160

Thatcher, J. B [Jason Bennett], & Perrewé, P. L. (2002). An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy. *MISQ (MIS Quarterly)*, *26*(4), 391–396.

Tian, F., & Xu, S. X. (2015). How Do Enterprise Resource Planning Systems Affect Firm Risk? Post-Implementation Impact. *MISQ (MIS Quarterly)*, *39*(1), 39–60.

USA TODAY. (2015). *Google Photos labeled black people 'gorillas'*. https://eu.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465/

2.2 Illuminating the dark side: a multi-level taxonomy of the risks and side effects of digitalization

Abstract: Achieving a bright digital future requires managing the adverse effects of digitalization. While we are aware of many adverse effects of digitalization, we do not fully understand these multifaceted phenomena. This lack of understanding hinders proper management and, in turn, limits digitalization success. In an effort to alleviate this problem, we synthesis accumulated knowledge by identifying, structuring, and communicating the most adverse risks and side effects of the development, production, use, and disposal of digital technologies and media. The result is a comprehensive, multi-level taxonomy of the dark side of digitalization. The taxonomy comprises 11 abstract risks and side effects of digitalization and 39 more specific subtypes of these risks and side effects. We highlight specific manifestations and examples of these risks and side effects, traced back to affordances of digital technology and media. Further, we indicate the level they affect. The taxonomy embraces dark side phenomena previously studied in IS research and substantially broadens current perspectives by studying relevant effects that have, so far, been overlooked in our discipline. The taxonomy will serve as a repository and a vantage point for research on better understanding and managing the risks and side effects of digitalization. Further, it may help to predict and mitigate adverse effects in the design and management of digitally-enabled socio-technical systems.

Keywords: Dark side of IT, dark side of IS, digitalization, affordances, taxonomy

Authors: Fabian Schmied, Henner Gimpel

Status: This article is a working paper.

"Ultimately, we as a society should decide how some things should work and make sure our systems follow these rules."

— Sundar Pichai, CEO Google, 2019[8]

"We must also protect against the dangers of digital technologies, from the spread of hatred and misinformation to cyberattacks and the exploitation of our data."

— António Guterres, UN Secretary-General, 2021[9]

2.2.1 Introduction

The increasing use of digital technologies and media (DTM) is ambivalent. DTM not only represent the world; they are also shaping the world (Baskerville et al., 2020). Over the past 70 years, DTM have made our lives easier, safer, healthier, and longer (Leidner, 2019). Our organizations have become more productive, and our economies have grown (Hitt & Brynjolfsson, 1996; G. Lee et al., 2018). Digitalization has many positive aspects. However, as digital technologies and media become ever more intelligent, adaptive, interactive, iterative, stateful, contextual, and pervasive (J. K. Lee, 2015; McCarthy et al., 2020; Schuetz & Venkatesh, 2020; Tarafdar et al., 2015b), it is increasingly apparent that they can also have unexpected, unintended, and adverse effects.

Articles in top information systems (IS) journals focus almost exclusively on (typically positive) instrumental outcomes while failing to consider humanistic ends (Sarker et al., 2019). Yet, Sarker et al. (2019) warn us that IS scholars and practitioners may fail to adequately reflect on the consequences of DTM and, hence, may fail to critique and actively oppose dehumanization and dystopian DTM-based developments. Walsham (2012, p. 92) insists that, as IS scholars, we must ask ourselves, "are we making a better world with ICTs?" "The recognition that ICT can have both positive and negative effects, both intended and unintended, deepens our field's theorization of ICT" (Majchrzak et al., 2016, p. 273). Yet, this recognition also demands rigorous stocktaking and active management of the risks and side effects of the increasing use of digital systems (Tarafdar et al., 2015a). For digitalization to result in net benefits, we must ensure that the many positive aspects outweigh the related risks and side effects (McCarthy et al., 2020). To support this process, we provide a multi-level taxonomy

[8] https://m.faz.net/aktuell/wirtschaft/digitec/interview-with-google-ceo-sundar-pichai-do-we-have-to-be-afraid-of-google-16010193.html
[9] https://news.un.org/en/story/2021/05/1092052

that can contribute to a net benefit assessment of the effects digitalization has, or will have, on individuals, organizations, and societies.

Studying the "dark side of IT" is not new in academia, but it is important. The term has been described as relating to a "collection of 'negative' phenomena that are associated with the use of IT, and that have the potential to infringe the well-being of individuals, organizations and societies" (Tarafdar et al., 2015b, p. 161). Prior work focused on individual-level effects (Pirkkalainen & Salo, 2016), malicious use of the internet (Kim et al., 2011), and cybercrime (J. K. Lee, 2015). These are valuable starting points. However, the scope of the dark side of IT is broader.

This paper aims to identify, structure, and communicate the most severe *risks and side effects of digitalization* (RSEDs). The starting point is a recognition that the development, production, use, and disposal of DTM may have consequences beyond the immediate aim. We engage in a review and synthesis of previously published accounts of dark side phenomena to generate theoretical insights and implications regarding RSEDs. Specifically, we apply a taxonomy development methodology heavily relying on existing knowledge encapsulated in academic writing. Identifying and assessing RSEDs is difficult due to their ambivalence, complexity, and novelty. The task is further complicated by the inevitable biases of observers, including ourselves, other authors, and readers. To account for these complexities and triangulate the RSEDs, we complement the theory-generative literature synthesis by also examining journalistic reflections on digitalization. Partially, we are guided by insights offered by scholars from other disciplines, to enlighten our individual and disciplinary blind spots.

Our taxonomy will serve as a repository of accumulated knowledge and a vantage point for further theoretical and empirical research on identifying and managing RSEDs. As a "theory for analyzing" the taxonomy describes and classifies by summarizing the commonalities found in discrete observations (Gregor, 2006). Majchrzak et al. (2016), describe a taxonomy as a "theory of the problem" that aims to elucidate a specific challenge. Particularly relevant to our work is Majchrzak et al.'s (2016) assertion that researchers often have a pro-IT bias and subconsciously avoid acknowledging IT-related harms. They call for researchers to consider the unintended consequences of IT artifacts and IT use. Likewise, Turel et al. (2021, p. 128) suggest that while "research on the dark sides of the digitalization is still in its nascent scholarly stage, the prevalence and significance of its negative impacts for individuals, organizations, and societies beg more research in this area." Our taxonomy provides a research synthesis and structure that enables users to systematically respond to these calls.

From an ethical standpoint, the rapid evolution of digitalization creates normative uncertainty that calls for reflection on the ethical aspects of DTM's role. Our paper, and future works that build on it, will enrich the societal dialogue on whether RSEDs should be accepted and how they might be managed given the substantial (net) benefits of digitalization.

2.2.2 Methodology

We follow the iterative taxonomy development procedure suggested by Nickerson et al. (2013) to identify, structure, and communicate the most severe RSEDs. The taxonomy is primarily intended for use by IS scholars. The meta-characteristic is the types of risks and side effects associated with the actualization of affordances of DTM. The ending conditions are those suggested by Nickerson et al. (2013, Tables 2 and 3).

Our taxonomy development process uses four distinct sources in an empirical-to-conceptual approach (Nickerson et al., 2013) for identifying RSEDs and their common characteristics, as well as grouping and structuring RSEDs.

Firstly and primarily, extant academic IS literature: Following the cumulative principle of science, we build on IS literature published in journals and presented at conferences. This embeds our research in the discourse within the IS discipline. Specifically, we leverage the eight journals in the AIS Senior Scholars' Basket of Journals. A focus on the top outlets of our discipline supports the quality of the underlying research and the relevance of the topics. We also analyze articles in the *Communications of the Association for Information Systems (CAIS)*, a journal widely read in the IS community. A downside of academic journals might be a bias in terms of selection and timeliness. We have attempted to mitigate this potential for bias in our findings by including conference papers and journalistic coverage of digitalization. We studied papers from the leading IS conference, the International Conference on Information Systems (ICIS). Finally, for breadth of coverage, we searched the AIS eLibrary. Search strings, time restrictions, etc. for the different searches are detailed below.

Secondly, journalistic coverage of digitalization: We reviewed journalistic reflections on digitalization from leading print media. Journalistic articles are a valuable supplement to scientific contributions: Their lead-times for picking up news are shorter than those of academic outlets, and they are not restricted by specific disciplinary or community boundaries. And, although journalism doesn't necessarily follow scientific principles and or leverage academic peer-review for quality assurance, journalistic articles do shape public perceptions of, attitudes towards, and norms relating to DTM and RSED. There is no doubt it is important to recognize the different characteristics of academic and journalistic publications. Yet, when journalistic

articles in lead media discuss the adverse effects of digitalization—even if these discussions are based on anecdotes, opinions, or speculation—we consider it relevant for identifying the RSEDs.

Specifically, we reviewed all editions of the weekly magazines *TIME* and *DER SPIEGEL* for more than 3.5 years (details below). Both magazines provide global coverage of relevant topics. *TIME* primarily focuses on the US—the world's largest economy, while *DER SPIEGEL* focuses on Germany—the largest economy in Europe. We decided against including media from China—the largest Asian economy—due to Chinese limits on free speech.

Thirdly, expert interviews: Academic discourse traditionally centers around disciplines, rather than objects of investigation. Different disciplines develop and use different terminology and lexica to refer to related phenomena under study (Berente et al., 2019). Different disciplines also relate to different bodies of theory and use different theoretical lenses to study phenomena of interest. Thus, we used interviews to map our emerging perspective of RSEDs to the terminology, conceptualizations, theories, and lenses in different academic disciplines, specifically sociology, psychology, criminology, economics, history, computer science, IS, ethics, strategic foresight, and technology assessment. By interviewing scholars from these disciplines, we hoped to avoid overlooking essential perspectives already developed in the respective disciplines and gain valuable insights that would support our taxonomy development. We selected these disciplines because of their relation to (specific) RSEDs. For each discipline, we interviewed one senior scholar whose research focuses on digitalization. We selected senior scholars who could provide an overview of discourse in their domain.

Most interviews were conducted by one of the authors of this article. For practical reasons, some were conducted by external interviewers. In all cases, the interviews were semi-structured and focused on specific RSEDs, the conceptualization of RSEDs, and the theoretical lenses used to study RSEDs in the interviewees' disciplines. Interviews lasted between 41 and 82 minutes (total duration 9.8 hours), were recorded and transcribed (237 pages of transcript). The interview transcripts were then analyzed. Approaching RSEDs at various levels of abstraction, we followed a deductive approach, taking the taxonomy as it emerged from previous development steps, integrating the interviewees' insights, where possible, and revising the emerging taxonomy, where necessary. Approaching the conceptualization of RSEDs and theoretical lenses, we followed the inductive approach of identifying themes and integrating these into our thinking. When experts referred us to literature from their own disciplines, we followed their guidance.

Fourthly, feedback on preliminary versions of the taxonomy: We presented nascent versions of our taxonomy in two cycles of the iterative taxonomy development and obtained written and oral feedback. Specifically, we presented the taxonomy at two workshops involving scholars from law and ethics, and at three conferences: one on IS, one on management, and one on ethics. The rationale for the interdisciplinary discourse is the same as for the expert interviews, outlined above. Before the conferences, we obtained seven written peer reviews of a prior version of this paper. At the workshops and conferences, we engaged audiences in discussions and took field notes which we subsequently analyzed. Following Wunderlich et al. (2019), we approached fieldnotes as a legitimate data source that can be analyzed similarly to transcripts of recorded interviews.

Building on prior accounts of the dark side of IT use (see next section), we performed nine cycles of iterative taxonomy development, each cycle using one of the four sources listed above and building on the previous cycles. After each cycle, we decided which source appeared most promising for the next cycle. In this way, we purposefully mixed the four different sources. In totality, we gave primacy to synthesizing previously published academic literature and complemented this with additional sources to ensure a broad coverage of the phenomenon. As suggested by Nickerson et al. (2013), in each cycle, we identified examples and characteristics of RSEDs to develop a structured presentation that is concise, robust, comprehensive, extendible, and explanatory. Table 2.2-1 provides an overview of the cycles. After cycle 9, all ending conditions were fulfilled. Table 2.2-2 provides details on the interviews.

Cycle	Source	Specific approach	Key result
1	**Academic IS literature**	- Title and abstract search in the AIS eLibrary for "dark side" or "bright side" to get an initial understanding - "All fields" search in the AIS eLibrary for "dark side." Alongside the search results, the AIS eLibrary lists keywords of the retrieved articles that occur at least twice. We screened this keyword list for RSEDs	- An initial list of RSEDs
2	**Feedback on a preliminary version of the taxonomy**	- Two workshops with scholars from ethics and law to broaden the conceptualization of RSEDs	- Support for the relevance of topic, research gap (also in other disciplines), single RSEDs - Using affordance theory
3	**Journalistic coverage of digitalization**	- Analysis of all digitalization-related articles (manual selection by one of the authors of this article) in *TIME* magazine and *DER SPIEGEL* from June 2017 to July 2018 to grasp the journalistic coverage of RSEDs	- New RSEDs, subtypes, and manifestations
4	**Extant academic IS literature**	- Detailed search in all volumes of MIS Quarterly (MISQ) and the Journal of the AIS (JAIS) to reflect on the emerging RSEDs in selected top IS journals	- New RSEDs, subtypes, and manifestations - Alignment of terminology to discourse in IS

		- Search for “dark side” OR “downside” OR “risk” OR “adverse” OR “negative” OR "side effect" in title or abstract - Manual processing of the 166 results obtained	
5	**Expert interviews**	- Nine semi-structured expert interviews to broaden the understanding of RSEDs with their terminology, conceptualizations, and theories. - See Table 2.2-2 for a list of interviews - For practical reasons, some interviews were performed before, and some after, cycle 6. Thus, cycles 5 and 6 are almost conducted in parallel.	- Reconceptualization of RSEDs as now displayed in the section *Conceptualization* - New RSEDs, subtypes, and manifestations
6	**Feedback on a preliminary version of the taxonomy**	- Seven blind peer reviews and feedback from participants at three conferences to check for relevance, novelty, comprehensibility, and completeness of the emerging taxonomy	- Strengthen motivation by showing the prior taxonomies are not exhaustive - Strengthen discussion of implications - Expand presentation by more details on the methodology and by examples
7	**Academic IS literature**	- Detailed search in all volumes of seven journals (Information Systems Research, Journal of Management Information Systems, Journal of Strategic Information Systems, Information Systems Journal, European Journal of Information Systems, Journal of Information Technology, CAIS) using the same search string as in cycle 4 to fully cover the discourse on RSEDs in the basket journals and CAIS - Additional search for articles in MISQ and JAIS that were not published at the time of performing cycle 4, undertaken using the same search string as in cycle 4 - Manual processing of the 508 results obtained	- More abstract versions of some affordances - New RSED subtypes and manifestations - Elevation of former subtypes to RSEDs as the importance of the phenomena became clearer - Movement of subtypes to other more appropriate RSEDs
8	**Journalistic coverage of digitalization**	- Analysis of all digitalization-related articles (manual selection by one of the authors of this article) in *TIME* magazine and *DER SPIEGEL* from August 2018 to the end of 2020 to expand on cycle 3 and check for new occurrences of RSED	- No changes of RSED - One single new RSED subtype (“digital inequalities”) - Additional manifestations for RSED subtypes
9	**Extant academic IS literature**	- Detailed search in recent proceedings of the ICIS (2016-2020) as leading IS conference with the same search string as in cycle 4 and 7 to fully cover the academic discourse that has not yet been published in the leading IS journals - Manual processing of the 250 results obtained	- No changes of RSED - No changes of RSED subtypes - Additional manifestations for RSED subtypes

Table 2.2-1: Overview of taxonomy development cycles

Inter-viewee	Discipline	Duration in minutes	Select insights[10]
1	Sociology	62	RSEDs are a social construction, there is no technology determinism; DTM are reductionist and standardizing
3	Psychology	58	Assessments are subjective; majority votes do not suffice to determine adverse effects; the ambivalence of adversity needs to be accepted
2	Criminology	69	Damage to recognized legal interests (of natural persons, legal persons, collectively) is a criterion for adverse effects; adversity and illegality are different
4	Economic history	55	Societal transformation due to technological development is typical; one cannot accurately weigh positive and adverse effects, not even in historical retrospect
5	Computer science	76	Computer programming is always reductionist and thereby changes the world; if you don't take the side effects into account, they become the main effects
6	Information systems	41	The scope of socio-technical change across levels of analysis is substantial; the anticipated future change is even more substantial; values and ethics are important in IS design and use
7	Ethics	73	Culturally, processes of change have always been accompanied by rejection; lack of human control and autonomy are critical issues
8	Strategic foresight	82	We need a societal consensus (rather than domination by a select few cultures and companies) on the relevant outcome dimensions of developing and using DTM; a dual development track of technologies with a bright and a dark side is common also for other technology classes
9	Technology assessment	70	Historically, technological change and automation have always not only created winners but also losers; digitalization is means to an end, not an end in itself; humans are (unfortunately) very good at suppressing thoughts about adverse effects but this does not diminish the importance of such effects

Table 2.2-2: Overview of expert interviews

Conceptual-to-empirical iterations might be a fruitful addition to the taxonomy development process (Nickerson et al., 2013). One might argue that digitalization enhances the non-digital effects. Hence, one might use a list of all adverse effects and consider whether digitalization contributes to these. Furthermore, because each affordance of DTM may lead to RSEDs, one might use a list of all affordances of DTM to identify potential RSEDs. Unfortunately, neither of these lists exists. Hence, we focused on empirical-to-conceptual iterations.

The methodology we adopted has two key limitations: Firstly, "theories of the problem […] make explicit value judgments that the situation is problematic from the perspective of certain stakeholders" (Majchrzak et al., 2016, p. 271). From our (i.e., the authors') socialization, the media reviewed, and the interviewees, workshop participants, and conference participants, we tend to have a culturally biased Western perspective. This despite our knowledge that assessment of the valence of an effect depends on culture, and that DTM exert "a nonuniform effect

[10] In addition to the general perspectives listed in Table 2.2-2, each expert offered specific RSED subtypes, manifestations, and examples. This sharpened our understanding of the breadth of RSEDs and terminology. Knowing these RSEDs, we also detected them in academic or journalistic writing and, thus, refrain from quoting the experts as sources in presenting the RSEDs.

on societal transformations that varies with the stage of economic development“ (G. Lee et al., 2018, p. 234).

Secondly, we only integrate RSEDs mentioned in print, by experts during interviews or at workshops, or at conferences. This leads to a bias towards (but not an exclusive focus on) relatively short-term effects already observable at the current stage of digitalization and vague perceptions of potential risks emerging in the future. Thus, the specific RSEDs, their subtypes and manifestations, and the underlying affordances of DTM will likely evolve with the progression and maturity of digitalization.

After finalizing the RSED taxonomy, we evaluated and refined our assignment of RSED subtypes to affordances and primary levels affected with a focus group, i.e., “a small number of appropriate persons discussing the topics raised by a moderator who guides the interview process” (Rosemann & Vessey, 2008, p. 12). In our case, the two authors of this paper moderated the focus group, which consisted of six IS researchers (four postdoctoral researchers, one doctoral student, one affiliated researcher). The focus group had two sessions with a total duration of five hours. After an introduction to the taxonomy’s aim, the concept of affordances, the specific affordances identified by the authors in the taxonomy development process, and the levels affected, the participants discussed each RSED subtype. Each participant had the definition in front of her or him. Manifestations and examples and the delineation from other subtypes were discussed. Participants engaged in a discussion, suggesting different affordances or levels, and additions. At times, they questioned their suggestions which, after hearing and debating the arguments and examples, were either accepted or withdrawn. Some affordances were slightly adapted from the initial version suggested by the authors. Results were documented by a moderator in a spreadsheet that was visible to all participants. After each subtype had been discussed, one moderator asked whether the result displayed on the joint spreadsheet was a consensus or changes were required. The discussion continued until a consensus was reached.

2.2.3 Related work on the dark side of digitalization

IS research has a history of studying the dark side of IT and digitalization. All effects named in the following are included in our taxonomy.

2.2.3.1 A prior taxonomy, reviews, and a conceptualization

A taxonomy of the dark side of the internet includes seven technology-centric phenomena (spam, malware, hacking, denial of service attacks, phishing, click fraud, violation of digital

property rights) and eight non-technology-centric phenomena (online theft, online scams and frauds, physical harm, cyber bullying, spreading false or private information, illegal online gambling, aiding crime, other reprehensible behaviors) (Kim et al., 2011). Two findings are especially noteworthy here: Firstly, some dark side phenomena are technology-centric while others are not. Secondly, some of these dark side phenomena are illegal while others might be legal but unethical or reprehensible. Both is in line with our conceptualization.

A recent review of 282 IS papers on digital transformation, among other facets, identified negative impacts that arise from the use of DTM (Vial, 2019). The list of negative impacts is short; it merely lists security and privacy. The analysis of all research articles in the AIS Senior Scholars' Basket of Journals between 1995 and 2015 brings forth four key dark side phenomena: technostress, information overload, IT addiction, and IT anxiety (Pirkkalainen & Salo, 2016). Further topics from the review are loneliness and an increasing burden of work. Based on this, Pirkkalainen and Salo (2016) called for more research on the dark side of IT use at the individual level. We follow this call at the individual level and beyond.

S. Alter (2017) focuses on the simultaneous existence of IT's bright and dark sides. He points out that an intended bright side for some might go along with a possible or likely dark side for others. These are typically legitimate goal conflicts and trade-offs between the preferences of different stakeholders. As S. Alter (2017, p. 15) observes, the "evaluation of whether a specific use of IT is beneficial or detrimental is subjective and depends on the observer's personal concerns and interests". We agree with this view. Yet, our taxonomy development strives to identify general effects of DTM considered adverse by a large enough number of individuals that their existence should not be regarded as subjective. That is not to say that an RSED needs to be considered adverse by all people.

2.2.3.2 Special issues of IS journals

The *ISJ* published two issues on the dark side of IT use, featuring seven research papers and two editorials (Vol. 25, Issues 3 and 4, 2015). The editors describe "the 'dark side' of information technology (IT) use as a broad collection of 'negative' phenomena that are associated with the use of IT, and that have the potential to infringe the well-being of individuals, organisations and societies," and list several established and—at the time—relatively novel phenomena (Tarafdar et al., 2015b, p. 161). They propose four themes for characterizing dark side phenomena: the context of occurrence, negative outcomes, mitigation mechanisms, and level of analysis. Context involves aspects such as individuality, activity, location, time, and

relations. We have identified many manifestations of RSEDs deeply rooted in specific contexts. In the process of taxonomy development, we aggregate these manifestations to a level that is less dependent on context but retains the contextual perspective with respect to underlying affordances of DTM. Adverse outcomes are at the core of our taxonomy in the form of RSEDs and their subtypes. Our discussion of mitigation mechanisms is intentionally superficial as our focus is on identifying and structuring RSEDs. The level of analysis is, again, key for our taxonomy, as we relate RSEDs to the levels on which their effects are felt.

Much of the literature on the dark side of IT use has focused on the individual level, as do the papers in the special issue (Tarafdar et al., 2015b), which study the technostress, IT-based interruptions, excessive smartphone use, computer-mediated work control, computer abuse, and illegal music sharing. Six years later, the *International Journal on Electronic Commerce (IJEC)* published a special issue on the dark side of digitalization (Vol. 25, Issue 2, 2021) with two papers on technostress and two on excessive use, again, focusing on the individual level. The *ISJ* special issue editors posited that "the area of dark side outcomes at the societal level remains largely unexplored" and, thus, called for "attention to levels of analysis other than the individual and to cross-level effects" (Tarafdar et al., 2015b, pp. 165–166). The *IJEC* special issue editors compared the dark side to an iceberg, of which we can only so far see the tip, and called for future research to explore the entire iceberg (Turel et al., 2021). Our research responds to these calls.

2.2.3.3 Panels at IS conferences

At the *Americas' Conference on Information Systems (AMCIS) 2012*, a panel discussed the dark side of IT use in organizations, focusing on five phenomena: IT-usage-related stress, work overload, interruptions, addiction, and misuse of IT (D'Arcy et al., 2014). At *AMCIS 2016*, a panel discussed the "Dark Internet," starting with the effects presented by Kim et al. (2011) and Tarafdar et al. (2015b; 2015a). The panel focused on three topics from the "routinely dark side," namely deception, fraud, and phishing, and two topics from the "truly dark side," namely terrorism and the dark web. Unlike the *AMCIS 2016* panel, we refrain from assessing the level of darkness as our interviews with digitalization experts from other disciplines (cycle 5) suggested that we cannot sufficiently balance the numerous stakeholder perspectives and assessments drawing on different cultures. Yet, we agree with George et al. (2016) that the severity of phenomena differs. At a pre-workshop of the *ICIS 2018*, a panel discussed the dark side of digitalization, specifically at the individual level (Turel et al., 2019).

2.2.3.4 Practitioners' perspectives

Beyond the scholarly discourse, practitioners also reflect on ethical issues related to digitalization. The *Association of Computing Machinery (ACM)* published the *ACM Code of Ethics and Professional Conduct* (ACM, 2018). The code suggests that computing professionals "should reflect upon the wider impacts of their work, consistently supporting the public good" (ACM, 2018, p. 1). It lays out that "well-intended actions, including those that accomplish assigned duties, may lead to harm" such as "unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment" (ACM, 2018, p. 2). While these exemplary harms are included in our taxonomy, the ACM acknowledges that "this list is not exhaustive" (ACM, 2018, p. 2). The *Institute of Electrical and Electronics Engineers* (IEEE) goes in a similar direction. The *IEEE 7000-2021 standard* establishes processes by which organizations can consider ethical values during concept exploration and development. The *IEEE Code of Ethics* asks members of the *IEEE* "to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices and to disclose promptly factors that might endanger the public or the environment" (IEEE, 2020, Section 7.8). The code does not provide details on what these factors might be. We provide an exhaustive list of the most severe RSEDs. This list may support computing professionals, members of the *ACM*, and members of the *IEEE* in complying with their codes of ethics.

2.2.3.5 Summary

The emerging literature on the dark side of IT use suggests that many dark side phenomena exist, and current trends are making the field more diverse. Prior research indicates that the bright and dark sides of IT are two sides of a coin that go hand in hand. Trade-offs and net benefit calculations are necessary. The adverse effects are seldom determined by a technology or technological artifact per se but are rather by the specific context and type of use. In this, assessing the dark side is not the same as assessing the legality of IT use, but involves examining the intentions and consequences of IT use from multiple stakeholders' perspectives. Adverse effects can emerge at multiple levels, ranging from the individual to society, with most prior research focused on the individual level.

We are aware that there are multiple lists and frameworks structuring RSEDs. Yet, as none of these lists and frameworks is a superset of all others, we know that none of these lists and frameworks is exhaustive. Neither are these lists and frameworks collectively exhaustive. Is

it apparent, for example, that none include effects like a digital divide, discriminating algorithms, manipulation of democratic elections, and the climate impact of energy demand relating to DTM use (to be discussed in our taxonomy below). Thus, we move ahead with developing a conceptualization and taxonomy of RSEDs.

2.2.4 Conceptualization

The following subsections define and describe the primary constructs for our research.

2.2.4.1 Digitalization and digital technologies and media

Digitalization refers to the sociotechnical phenomena and processes of developing, adopting, and using digital technologies and media in individual, organizational, and societal contexts (Legner et al., 2017). Digital transformation is "a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies" (Vial, 2019, p. 121). In line with Legner et al. (2017), entities can be individuals, organizations, or societies at large.

Digital technologies and media (DTM) comprise all electronic devices (hardware) and applications (software) that use information in the form of numerical codes (usually binary codes), as well as all the media (i.e., means and channels of general communication in society) that are coded in formats that can be processed by these devices and applications.

2.2.4.2 Risks and side effects of digitalization

RSEDs are adverse secondary effects (side effects) or the possibility of such effects (risks) arising from digitalization. These are not effects of DTM themselves; they are the consequences of attitudes, decisions, and behavior related to DTM (Decker, 2013). According to common categorizations of technological consequences (Decker, 2013), RSEDs are (possible) secondary effects that are unwanted and unintended, but RSEDs are not the main effects. They may be certain or uncertain, expected or unexpected, result from individual thought or behavior, or emerge from the dynamics of collective behavior. They may be direct effects or mediated. Furthermore, they may moderate other effects outside the domain of digitalization.

DTM and digitalization are broad terms that involve IT and its development and use. RSEDs include the dark side of IT and go beyond it. Although digital phenomena are not identical with classical IT phenomena (e.g., Baskerville et al., 2020; Legner et al., 2017; Majchrzak et al., 2016; Vial, 2019), we conjecture that there is no benefit in aiming for a sharp boundary line between the closely interlinked dark sides of IT and digital.

RSEDs are adverse effects that cause harm. There is no objective criterion of adversity or harm spanning individuals, cultures, and ages. Judging adversity is not a matter of consensus or majority voting. Thus, we adopt the perspective of an impartial spectator assessing whether an effect is sufficiently adverse, sufficiently common, or likely to qualify as an RSED. The concept of an impartial spectator was first mentioned by Adam Smith in 1759 (Raphael, 2007). A perfectly impartial and well-informed spectator is an imaginary person that guides our decisions by virtually judging our actions according to common moral principles. To support our judgment about what the impartial spectator considers as adverse, we turned to the philosophy of law, which led us to define an effect as adverse if it negatively affects recognized interests in a sufficient manner. These interests might be the legal interests of natural persons (e.g., integrity of life, health, and freedom of action), legal interests of legal persons (e.g., physical, or intellectual property), or collective legal interests (e.g., payment of taxes). This does not imply that RSEDs are illegal. They have the same effect as socially harmful behavior but may also include, for example, self-harm and incidental harm. For example, social-media whitewashing and excessive exposure to images of presumably perfect bodies may lead to body image insecurity, eating disorders, and suicidal behavior, especially for (female) adolescents. Although there is nothing illegal in this, the individual legal rights of bodily integrity and right to health are curtailed, and we posit that an impartial spectator would consider this specific side effect of social media use to be adverse.

RSEDs can be analyzed at various levels of abstraction. In this paper, we consider four abstraction levels. **RSEDs** are rather broad, abstract effects. **RSED subtypes** are more specific effects. Each RSED subtype belongs to exactly one RSED. **Manifestations** of RSED subtypes, and—one level further down—specific **examples,** are even more specific, time-dependent, and context-dependent. Each manifestation relates to exactly one RSED subtype. The manifestations adversely affect individuals, groups, organizations, or society. Hence, making the world a better place requires inhibiting or reducing manifestations.

2.2.4.3 Affordances

Technology affordances arise from the relationship between an artefact and a goal-oriented actor or actors. Each DTM artefact has latent affordances that are action possibilities for at least one goal-oriented actor with the relevant action capabilities (Thapa & Sein, 2018). Affordances are potentialities; to have influence, they need to be actualized. How they are perceived and actualized is contextually influenced by cultural, social, and technical factors (Thapa & Sein, 2018). When an affordance is actualized, it may have the desired main effect

and it may have risks and side effects for the very actor actualizing the affordance (self-referring) or for others (externality).

We relate each RSED to at least one affordance of DTM (see exemplary mentions in the section *Taxonomy of RSEDs* and full overview in Table 2.2-5) to show that it is indeed a risk or side effect of digitalization and not, purely, of other causes. RSEDs are so complex that they have multiple simultaneous causes. However, to be classed an RSED, the requirement is that the actualization of a DTM affordance is a necessary precondition for having the RSEDs in the quality and/or extent that it exists. Focusing on affordances of DTM, rather than the DTM themselves, emphasizes that RSEDs depend on (i) how we humans design, build, manage, and use DTM and (ii) how digitalization affects our beliefs, attitudes, norms, and behavior.

Affordances exist at multiple layers. At a low technical level, DTM allow the digitization of analog signals, persistently store digital data, etc. Building on this, at a higher yet technical level, DTM afford encryption, big data handling, etc. At a higher sociotechnical level, they afford low transaction costs, automated decisions and actions, rapid innovation and diffusion, etc. In our study, this sociotechnical level is the main focus because it is more directly related to the RSED than the technical affordances, and because it outlasts individual DTM. Hence, for each RSED subtype, we identify at least one actualized high-level DTM affordance as a necessary precondition. This results in a list of high-level DTM affordances whose actualization produces the RSEDs. We do not claim that this is a comprehensive list of DTM affordances. Yet, we do claim that identifying and reporting the affordances serves two purposes: Firstly, it clarifies the link between RSEDs and digitalization. Secondly, it allows stakeholders who are primarily interested in a specific subset of affordances (e.g., arising from a technology they develop, manage, or use) to focus on the related RSEDs.

2.2.4.4 Affected level

The actualization of affordances can affect multiple levels, ranging from single individuals to society at large (J. Wang et al., 2015). Specifically, we consider five levels (see Table 2.2-3) that are similar to those in Costello et al. (2013) and based the ecological systems theory developed by Bronfenbrenner (1981). Effects can propagate from one level to another. For example, the effect of technostress caused by IT unreliability (personal level) might reduce individuals' socializing (interpersonal level) and work performance (organizational level).

Level		Description	Example of specific RSEDs
Individual	Nanosystem / personal	Adverse intrapersonal effects (behavioral, cognitive, bio-medical, etc.)	Negative psychological effects, such as IT anxiety or technostress.
	Microsystem / interpersonal	Adverse effects on the interaction and relationships in small groups, including the family, workgroup, and friendship networks	Personal attacks, such as cyberbullying or digital sex crimes
Organizational	Mesosystem / organizational	Adverse effects on individual social institutions that have organizational characteristics and are governed by formal (and informal) rules and regulations	IT operational risks, such as system malfunction
	Exosystem / inter-organizational	Adverse effects on interactions and relationships between organizations	Market power of quasi-monopolies suppressing other companies
Societal	Macrosystem / socio-economic	Adverse effects on society and economy at large as well as on nation-states and supranational relations	Unscrupulous public discourse, such as hate speech in social media or an "artificial intelligence singularity"

Table 2.2-3: Overview of the levels affected by risks and side effects of digitalization

For each RSED, we identify and report the level(s) with the strongest and most direct adverse effect. Other levels might be affected indirectly. Relating RSEDs to these levels serves two purposes: Firstly, an RSED will necessarily have an adverse effect on at least one level. Identifying and reporting this level clarifies the nature of the RSEDs. Secondly, reporting the level allows stakeholders interested in a certain level to focus on the related RSEDs.

In summary, human actors create and use DTM. Affordances arise from the relationships between actors and DTM. The actualization of some affordances has effects on multiple levels. RSEDs are the adverse, secondary effects. Figure 2.2-1 captures this in a stylized model.

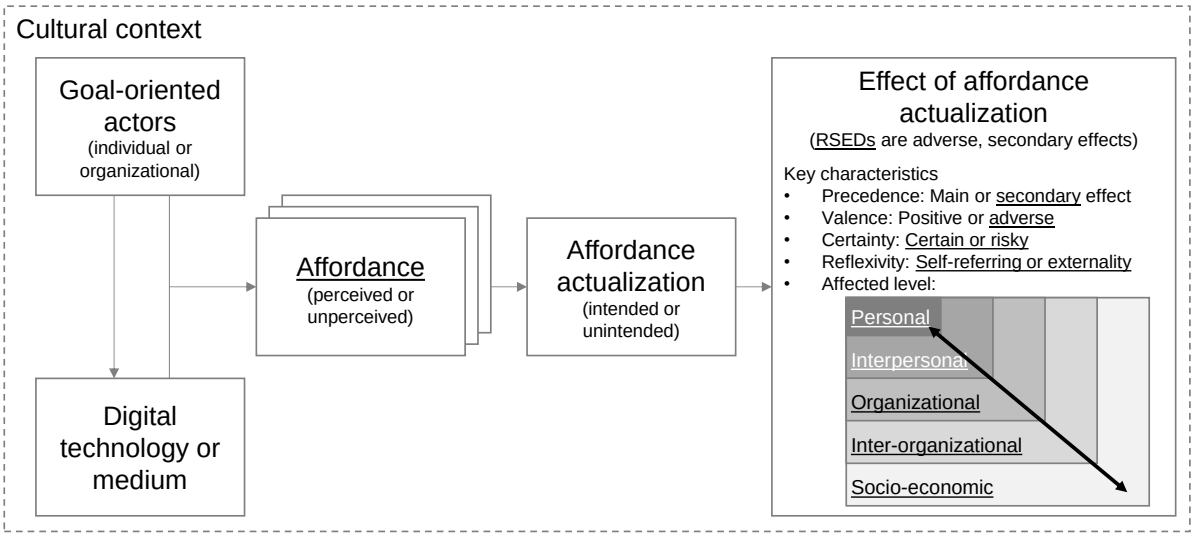


Figure 2.2-1: Stylized model of the emergence and types of effects of affordance actualization (underlining indicates the focus of the present paper)

2.2.5 Taxonomy of risks and side effects of digitalization

RSEDs and their subtypes are the core of the taxonomy. Table 2.2-4 defines all 11 RSEDs and 39 subtypes. To illustrate the abstract RSEDs and subtypes, we detail below some manifestations of the subtypes, as well as specific individual examples.[11] For clarity, RSEDs (level 1, highest level of abstraction) are written in ***italic bold font*** and subtypes of the RSEDs (level 2) in **plain bold font.** Manifestations of the subtypes (level 3) are highlighted in *italic font*. For brevity and because they are more transient than the higher levels, we do not formerly define the manifestations. Specific examples (level 4, lowest level of abstraction) are in plain font. Our framing of the RSEDs always includes the word "can" to highlight the potentiality of their occurrence. The subtypes foreground the adverse effects using definitive terms. This does not imply that the subtypes are universally relevant, either today or in the future. They might only apply under specific circumstances and reflect current perceptions of risk.

RSEDs	Subtypes of the RSEDs
Dissemination of problematic content: DTM can foster the public exchange of problematic information and socially harmful forms of public discourse.	**Distribution of inappropriate content:** Distribution of socially harmful content via DTM.
	Personal attacks: Harmful attacks among individuals via DTM.
Supporting delinquents: Digitalization can make it easier for malefactors to do harmful deeds and thereby promotes the occurrence of harmful deeds.	**Socially undesirable transactions:** DTM-enabled conclusion of (economic) transactions that are socially undesirable.
	Cybersecurity breaches: Harmful attacks on IT infrastructure, connected devices, or data, using DTM.
	Cybercrime: Criminal activities carried out, in part or wholly, via DTM.
	Aggravation of prosecution: Criminal prosecution by investigating authorities becoming more difficult due to DTM.
	Cyberterrorism and -warfare: The politically motivated use of DTM to cause severe disruption or widespread fear in society (cyberterrorism), and the use of DTM to disrupt the activities of a state or an organization, in particular, deliberate attacks on DTM used for strategic or military purposes (cyberwarfare).
Adverse socio-economic disruption: Digitalization can lead to social and economic disruption and, thus, may place some parties in a worse position than they would be without digitalization.	**Displacement of established structures:** DTM-enabled supplanting of established economic structures harms beneficiaries of such established structures.
	Digital inequalities: Separation between those who have access to DTM and those who do not.
	Superpowerful corporations: Extremely influential national and supra-national institutions and/or quasi-monopolies enabled by DTM create dependencies and suppress competition, innovation, and regulation.
	Loss of international competitiveness: Nation-states and regions lose competitiveness as economic location in global competition due to innovation in DTM along with regional agglomeration and network effects.
Shifting political control: Digitalization can shift political powers and dynamics and may facilitate political	**Trend towards extremism:** Extreme measures or views gain political influence due to DTM.
	Political regimes strengthening control: Autocrat regimes using DTM to strengthen and extend their political control.

[11] Although most of the manifestations are supported by different sources, we follow the manuscript guidelines of MISQ and limited in-text citations. By doing so, we prioritize academic sources over journalistic articles and (for ease of access of English text) articles published in *TIME* magazine over articles in *DER SPIEGEL*.

changes that are undesirable for a substantive majority of people.	**Lack of policy making:** Retarded enactment and revision of laws and policies regarding DTM-related progress leads to insufficient regulation.
	Manipulation of democratic elections: Manipulation of democratic election processes, or voters' information and opinions, via DTM.
Error-prone IT operations: Digitalization can worsen or stop organizational operations as critical DTM assets may not be available or work as expected.	**IT operational risks:** The risks of DTM-related losses resulting from inadequate or failed DTM-based systems or processes.
	IT project risks: Failure of IT projects leading to severe negative consequences for the entity conducting the project.
	Failure propagation: Failures propagate among DTM-based interconnected systems within organizations or across value networks.
Impairment of health: Digitalization can adversely affect individuals' health.	**Psychological health problems:** DTM-related development of mental illness.
	Addiction to DTM and resultant issues: Persistent, compulsive, and excessive use of DTM at an intensity that leads to individually harmful cognitive or behavioral adaptation. ***Note:*** *This subtype is a special form of psychological health problem. Its relevance and specificity justify its identification as a separate subtype.*
	Reduction of physical health: DTM-related infliction of bodily disease, illness, or malfunction.
Environmental deterioration: Resource requirements originating from digitalization can damage the natural environment.	**Climate impact of energy demand:** Negative climate change triggered by energy demand throughout the lifecycle of digital technologies.
	Consumption of material resources: Unsustainable levels of material resource use to manufacture digital technologies without proper recycling or reuse.
Loss of privacy: Digitalization can lead to an actual or perceived loss of freedom or dignity from inappropriate intrusion or disclosure.	**Privacy breaches:** Events of misuse of individuals' personal information.
	Ambivalent self-disclosure: Role conflict that arises from concurrent interaction with different social circles on social media.
	Digital surveillance: Surveillance of individuals by other individuals, organizations, or public authorities, via DTM.
Ambiguous decision environment: Digitalization can lead to decision-makers being exposed to untrustworthy or contradictory information on facts and agency.	**Uninformative information:** Assumed information becoming uninformative in DTM-based environments characterized by information overload, filtering, and questionable trustworthiness.
	Uncertain agency: Lack of transparency as to the nature and agency of technical or social actors in DTM-based systems.
	Loss of autonomy to act: Reduced individual freedom from external control or influence resulting from DTM use.
	Diffusion of responsibility: Lack of accountability for actions and their consequences in DTM-based decision environments.
Undesirable behavioral adaptation: Digitalization can facilitate socially undesirable changes to established competencies and behaviors.	**Technology-reliance along with increasing incompetence:** Increasing reliance on DTM leading to the loss of socially or individually desirable human competencies.
	Data fixation: Reliance on experience-based perception of the world declines thanks to an increasing reliance on data recorded and communicated by DTM.
	Poor time and workload management: Poor awareness and management of time, and an intertwining of different life spheres due to the ubiquity of DTM.
	Erosion of solidarity: DTM-triggered reduction of social and economic support commonly rooted in a sense of togetherness and advocacy for one another.
	Negative spillovers: Socially undesirable behavior in the offline world relating to interactions in the online world.
Rogue algorithms: Digitalization can enable complex and networked algorithms that are beyond proper human understanding and control.	**Lack of auditability:** Algorithms encoded in DTM not being available for methodical examination and review.
	Discriminating algorithms: Use of algorithms encoded in DTM leading to unjust or prejudicial treatment of different categories of people.
	Human-Technology role reversal: Complex technical systems and humans switching roles in their ability to shape each other.
	(Un)ethical programming: Reduction of ethical achievements and human values through explication and coding digital technologies.

Table 2.2-4: Overview and definitions of RSEDs and related subtypes

2.2.5.1 Dissemination of problematic content

Dissemination of problematic content describes the objectionable public exchange of information and socially harmful forms of public discourse via DTM. **Distribution of inappropriate content** as the first subtype of this RSED comprises *legal but socially detrimental hate speech* (McNamee, 2019), *negative word of mouth* (Beşer et al., 2016), *conspiracy theories* (Beuth, Groß, et al., 2020), and *spam mails* (Ilany-Tzur et al., 2016) spread by DTM as manifestations. Most of this content is disseminated by social media, which provides social media companies with unique, unregulated power over public discourse (Perrigo, 2018). Unlike traditional media, there are no journalists to act as mediating gatekeepers (Ressa, 2019). High visibility of posts containing strongly moralized, emotive content leads to polarization among users (Steinmetz, 2018c). This polarization is amplified by the dissemination of inappropriate content in isolated echo chambers of like-minded people (Huang et al., 2017). As most of the content shared on social media is free of charge, adolescents may access inappropriate content (e.g., material glorifying war or violence, pornographic material) (Rainer, 2019). The distribution of inappropriate content is fostered by the simplified broadcasting, low-cost anonymity, and low-cost interconnectedness afforded by DTM. These effects occur at the individual, organizational, and societal levels.

The second subtype, **personal attacks**, manifests in *cyber incivility*, i.e., computer-mediated interaction (e.g., via emails) which is perceived to be "aggressive, rude, inappropriate or disrespectful" (Lim et al., 2017, p. 2). Similar negative behavior, such as teasing and abusing, is also apparent in online communities (Carillo & Marsan, 2016). This subtype also comprises *violent cyber-attacks*, including cyberbullying (J. K. Lee, 2015), cybermobbing (Laurenz, 2018), cyberstalking (Jüttner, 2020), or hate pages (Steinmetz, 2019). For instance, cyberstalkers may spy on their victims with the help of special apps (so-called stalkerware) leading to severe consequences for their victims (Jüttner, 2020). Related, more specific manifestations are *digital sex attacks* such as revenge porn, nonconsensual porn, cyber-grooming, and sexting (C. Alter, 2017). Such violent crime in cyberspace is facilitated, inter alia, by DTM that affords low-cost anonymity or unverified pseudonyms in online media and simplified broadcasting via bulk e-mails, social media, and online communities (Amann & Rosenbach, 2019). **Personal attacks** occur at the individual level. They can cause great pain to those affected and may, hence, lead to a **reduction of psychological health** (cf. ***impairment of health***). This example illustrates that various RSEDs may be interrelated. Although RSEDs are distinct concepts that are independently relevant, they may also share antecedents or consequences with other RSEDs, or they may be antecedents or consequences of other RSEDs.

2.2.5.2 Supporting delinquents

Digitalization can make it easier for malefactors to cause harm and, thereby, promotes the occurrence of harmful deeds. The first subtype, **socially undesirable transactions**, comprises illegal transactions, as well as legal transactions that are perceived as socially harmful. Firstly, there is a *simplification of illegal transactions* involving pharmaceuticals, drugs, weapons, or assaults (M. U. Müller, 2018). Many of these exchanges run through the darknet. In a similar context, DTM may lead to a *reduction of control over trade*. For instance, prohibitions on the export or distribution of weapons may be bypassed via 3D printing. Further, DTM simplify the *financial exploitation of minors*. For example, minors are urged to pay for additional features in online games (Fröhlingsdorf, 2019), and young users of TikTok are encouraged by influencers to buy them expensive gifts (Böhm et al., 2019). Finally, DTM may lead to an *amplification of dubious business models*. For instance, the recruiting of multilevel marketing companies is simplified by social media (e.g., Instagram; Vesoulis & Dockterman, 2020). **Socially undesirable transactions** are enabled, inter alia, by DTM that allow for low-cost anonymity or unverified pseudonyms in online media and provide low transaction costs. Ultimately, **socially undesirable transactions** may harm individuals, and societies.

Cybersecurity breaches, as the second subtype of this RSED, have been extensively discussed by organizations and in research. Cybersecurity breaches occur when somebody gets *unauthorized access* to (sensitive) information, such as personal information or intellectual property (Lowry et al., 2015; Wallace et al., 2020). The access may be intentional or unintentional. Cybersecurity breaches often involve computer malware, such as viruses, worms, trojan horses, spyware, or ransomware. Further, there are growing concerns about *cyberattacks* on critical infrastructure (e.g., energy supply, hospitals, emergency alert systems), IoT devices (e.g., smart home applications), and AI-controlled systems (e.g., autonomous vehicles; Shim et al., 2020). Closely related are so-called (distributed) denial-of-service attacks which aim to make connected machines or network resources unavailable (Shim et al., 2020). *Cyberattacks* may lead to serious consequences, such as a **reduction of physical health** (cf. ***impairment of health***). For instance, *cyberattacks* may cause accidents of autonomous vehicles or interrupt pacemaker monitoring services, both of which may have lethal consequences (Shim et al., 2020). **Cybersecurity breaches** may harm individuals, and organizations and are facilitated, inter alia, by the low transaction costs, the low-cost anonymity, and the low-cost ubiquity provided by DTM.

The subtype **cybercrime** manifests in *cyber-enabled crime* (i.e., traditional crimes, such as fraud, theft, or sex trafficking, in forms that are facilitated by DTM), *cyber-dependent crime* (i.e., crimes that evolved after the emergence of specific DTM), or *platform crime* (i.e., crimes that are even more technology-focused and use, for example, the characteristics of botnets) (Schirrmacher et al., 2018). The manifold examples of **cybercrime** include identity theft, ransomware, fake shops, computer fraud (Riek et al., 2017), software piracy (Driouchi et al., 2015), unauthorized filesharing (Beekhuyzen et al., 2015), and concealment of data (Friedmann, 2019). Cybercriminal activities are facilitated by DTM that enable criminals to act anonymously, and provide a tremendously high level of interconnectedness, low-cost ubiquity, and an ever-increasing number of innovations and new possibilities. Cybercriminal activities may harm individuals and organizations, as was made apparent by, for example, the WannaCry attack in 2017 (Schirrmacher et al., 2018) which "turned into a serious global problem" (Riek et al., 2017, p. 2).

The **aggravation of prosecution** comprises the *technological and organizational backwardness of law enforcement authorities* that prevents, for example, the identification of anonymous perpetrators (C. Alter, 2017). For instance, prosecution is complicated by the use of encrypted messenger services (Diehl et al., 2019). Another manifestation is the *predictability of police actions* that are planned using algorithms (cf. predictive policing and predictive tax assessment) (Ashby & Tompson, 2017). A third manifestation is the *difficulty of prosecution beyond national borders* due to the supranationalism of DTM such as the World Wide Web (C. Alter, 2017). This effect is fostered, inter alia, by the low-cost anonymity provided by DTM and the rapid innovation and diffusion of DTM. As societies at large aim towards the prosecution of perpetrators, the **aggravation of prosecution** is an effect that impacts at the societal level.

Cyberterrorism and -warfare as a further subtype of this RSED manifest in *espionage*, *sabotage*, *propaganda*, *money laundry*, and *economic disruption* (Hay & LaFountain, 2017). Cyberwars are often waged by totalitarian states (Meyer, 2019). They are enabled by the low-cost ubiquity of DTM and the rapid innovation and diffusion of new technologies that may lend a strategic advantage over competitors and enemies. Compared to traditional weapons, cyberwarfare technologies are inexpensive and create new dangers (Stavridis, 2019). A comparatively new phenomenon is the live-streaming of assassinations on internet platforms, such as the Christchurch (New Zealand) terror attack on a mosque and the attack on a synagogue in Halle (Germany) in 2019 (Ratnesar, 2019). The threat of **cyberterrorism** is enlarged, inter

alia, by the fact that (critical) infrastructures, such as transportation, energy, and telecommunication, have become vulnerable due to their high levels of interconnectedness (J. K. Lee, 2015). The dissemination of terrorist propaganda is simplified by DTM such as social media or video platforms (Hay & LaFountain, 2017). As **cyberterrorism** affects infrastructures, this subtype impacts on a societal level.

2.2.5.3 Adverse socio-economic disruption

Digitalization causes ***adverse socio-economic disruption*** by changing current social and economic orders and thereby placing some parties in a worse position than they would be without digitalization. The **displacement of established structures** as the first subtype of the RSED manifests in the *replacement of traditional business models*. For instance, more traditional forms of exchange are replaced by electronic trading (Scott & Barrett, 2005), hotels are threatened by peer-to-peer rental platforms (M. Müller et al., 2020), and traditional taxi companies lose customers to ridesharing platforms (Ng et al., 2019). The business models of leading online retailers lead to *disintermediation*. Online retailers not only replace local brick-and-mortar stores but also manufacturers' brands by establishing ever more own-brands. Further, the use of online retailers' platforms by third-party merchants leads to a *loss of the customer interface*. Finally, the *establishment of virtual currencies* undermines the sovereignty of states and central banks (Bartz et al., 2019). Among others, the low transaction costs provided by DTM and the rapid innovation and diffusion of DTM lead to the **displacement of established structures**. The effects primarily occur at the organizational and the societal levels.

The subtype of **digital inequalities** manifests in the *digital divide,* which is extensively discussed in public discourse and research. The *digital divide* describes inequalities in access to DTM (Dewan & Riggins, 2005; Hsieh et al., 2008). There are first-order effects resulting from a divide between those who have access to DTM and those who do not. Second-order effects result from a divide between those who are able to use DTM and those who are not able to even if they have access to DTM (Dewan & Riggins, 2005). For instance, the online learning divide between students able or unable to participate in online classes (e.g., internet access, availability of home computers) became apparent during the COVID-19 pandemic (Reilly, 2020). Furthermore, the advancing digitalization leads to a *multiplication of inequalities* between the ultra-wealthy and the displaced workers (Lanchester, 2019). More precisely, the gig economy undermines social standards such as job security and pension insurance (e.g., online microtask labor markets, crowd work) and, thus, increases inequalities (Semuels, 2020a). The

increasing automation of job tasks by artificial intelligence (AI) or robots may lead to decreased incomes and job losses (Semuels, 2020b). These effects primarily occur at the individual and societal levels and are enabled, inter alia, by the rapid innovation and diffusion of DTM.

Adverse socio-economic disruption has also accompanied the growth of **superpowerful corporations**. Strongly DTM-focused companies, such as Google, Facebook, and Amazon, establish *almost indispensable international services*. The market power of such quasi-monopolies hinders competition, suppresses start-ups, and inhibits innovation (Shim et al., 2015). The international reach and economic power of these companies allow them to *evade national regulations and taxes* (Mingels, 2018). Further, there is a *unilateral definition of de-facto standards* (encapsulated in software and services) leading to the (global) dissemination of unilateral (politically shaped and normative) world views (Manzei, 2018). This prescribes certain views, norms, and behaviors while excluding others, particularly those that compete. Due to their market power, decisions by single companies may *harm whole industries* (e.g., Google Ads, Amazon Marketplace) or *restrict fundamental human rights* of billions of users (e.g., contact tracing via Android and Apple smartphones) (Rosenbach, 2019). Unlike other industries, internet companies usually *do not pay a price for the (social) harm they cause* (e.g., hate speech, manipulation of elections) (McNamee, 2020). The growth of these quasi-monopolies is enabled, inter alia, by low transaction costs and the ability to handle big data. The effects occur at the individual, organizational and societal levels.

Loss of international competitiveness describes the fact that investments in DTM may influence a country's economic development. For instance, AI may be seen as a new source of competitive advantage. While the cutting edge of technology has, for a long time, been dominated by the USA, China is now pioneering the development of many technologies (e.g., 5G) (Isaacson, 2019). Such changes mean that organizations based in former leading countries may incur a drop in sales or bankruptcy, and their employees may suffer decreasing incomes and job loss (Bremmer, 2017). These effects occur at the organizational and societal levels. Among other, they are related to the rapid innovation and diffusion of DTM and low transaction costs.

Adverse socio-economic disruption clearly highlights that RSEDs are not necessarily adverse for all stakeholders. The economic shifts may harm some stakeholders and benefit others. We do not aim for a utilitarian perspective evaluating the net benefit of the effects of digitalization, but, instead, consider effects as RSEDs when they have a substantial negative effect on a

significant number of stakeholders. It is not possible to meaningfully draw quantitative thresholds for the level of adversity or the number of people or organizations affected. Rather, we rely on assessments and reporting by fellow academics and professional journalists.

2.2.5.4 Shifting political control

Digitalization can shift political powers and may facilitate political changes that are undesirable for a significant number of people. The **trend towards extremism** as a first subtype of the RSED ***shifting political control*** manifests in ever more extremist (political) expressions on social media, leading to *political radicalization* (cf. ***dissemination of unscrupulous content***) (Bergengruen, 2020). A perceived loss of control (e.g., job insecurity) and bad prospects may lead to a call for simple (populistic) answers. Additionally, the vivid and omnipresent display of violence and crime (e.g., on social media) leads to *stronger perceived threats* and calls for *tougher regulation and enforcement*. These extremist opinions are enforced by *continuous affirmation by like-minded people* in online communities (cf. echo chambers). The **trend towards extremism** is afforded, inter alia, by the simplified broadcasting and low-cost interconnectedness provided by DTM that help to connect like-minded people who would never have met in person. These effects occur on a societal level.

Shifting political control is also apparent in **political regimes strengthening control** by using DTM to pursue their political agendas. For instance, social media is abused by totalitarian states to disseminate their political *propaganda* (Meyer, 2019). At the same time, *censorship of internet and social media content* takes place in some countries (e.g., China's great firewall, Russia's online iron curtain; Bremmer, 2018; Campbell, 2018). Sometimes, political regimes *cut off the internet* to avoid the dissemination of information and the organization of protests (Hincks, 2019). Finally, there is increasing *surveillance of citizens* which is discussed in detail with the RSED ***loss of privacy***. The manifestations of this subtype are enabled, inter alia, by simplified broadcasting, low-cost interconnectedness, and low-cost ubiquity provided by DTM and occur at the individual and the societal levels.

The **lack of policy-making** includes *tardy legislation* where the process of enacting and revising laws does not keep up with socio-technical progress, leading to unwanted harmful effects (e.g., hate speech, privacy breaches; Steinmetz, 2018b). Moreover, *national legislation is not suitable* to appropriately regulate cross-border use of DTM. There is a need for transnational legislation, as demonstrated by the European Union's (EU) General Data Protection Regulation (GDPR). Essentially, the design of DTM is left to an economic and technical sys-

tem logic and only slightly regulated by (cross-) national legislation. The **lack of policy making** is fostered by rapid diffusion and innovation and the low-cost interconnectedness and impacts on an organizational and a societal level.

As was widely discussed in the context of the US presidential election of 2016, DTM may be abused to **manipulate democratic elections**. Due to high levels of social interconnectedness, social media, in particular, are suitable for launching *misinformation campaigns* (e.g., by political parties or foreign countries) that may influence voters' decisions (Stengel, 2019). It was in this context that the phrase "weaponization of social media" was coined. Strongly emotional posts generate more attention and are spread more extensively on social media, leading to the *wide reach of populist parties* (cf. ***dissemination of unscrupulous content***). This phenomenon gives populist parties an advantage over their more moderate opponents. Unlike traditional media, the *regulation of electoral advertising does not apply in social media* (Zorthian, 2017), at least not yet (cf. **lack of policy making**). Hence, there is a lack of financial transparency and monitoring for veracity (Transparency International, 2021). The Cambridge Analytica scandal also showed that data generated on social media may be abused in electoral campaigns (e.g., *microtargeting*; cf. **privacy breaches**). Finally, democratic elections may be the target of *cyberattacks* (e.g., by attacking voting machines; cf. **cybersecurity breaches**; Ratnesar, 2019). The effects occur on a societal level and are enabled by simplified broadcasting and the massive amount of data generated and analyzed by DTM.

2.2.5.5 Error-prone IT operations

Regarding ***error-prone IT operations,*** digitalization can impair or halt organizational operations as critical DTM assets may not be available or work as expected. The first subtype of this RSED, **IT operational risks,** arises from the individual or organizational use of DTM and may be defined as "any threat that may lead to the improper modification, destruction, theft, or lack of availability of IT assets" (Goldstein et al., 2011, p. 610). *Data-related IT operational risks* refer to the confidentiality of data, while *function-related IT operational risks* refer to the availability or integrity of IT assets (Goldstein et al., 2011). Both may have severe consequences. For instance, plane crashes may result from erroneous sensor data, or accidents of autonomous vehicles may occur due to false perceptions of objects (Fitzpatrick, 2019). In the US, there have been several accidents involving Tesla's autonomous vehicles crashing into emergency vehicles with flashing blue lights (Book, 2021). Other examples include erroneous blockchain applications, erroneous AI-based recommendations or decisions,

and health apps leading to wrong diagnoses (Fitzpatrick, 2018). **IT operational risks** are further amplified by organizations' increasing dependency on information networks (P. Chen et al., 2011). A correlating failure of multiple nodes of a network may result in a greater loss of availability and a longer downtime (P. Chen et al., 2011). These effects occur on an individual and an organizational level and are fostered, inter alia, by the rapid innovation and diffusion of DTM, low-cost interconnectedness, and automated decisions and actions.

The second subtype of this RSED refers to **IT project risks**. Within organizations, the evaluation and implementation of new DTM are often organized as IT projects (Guggenmos et al., 2019). Due to their special characteristics, IT projects can be viewed as more complex than ordinary projects (Neumeier & Wolf, 2017). Many IT projects are challenging, exceed their budget, or fail completely (Flyvbjerg & Budzier, 2011; Guggenmos et al., 2019). This may lead to severe consequences for organizations, such as financial losses, loss of market value, or bankruptcy (Bharadwaj et al., 2009; Flyvbjerg & Budzier, 2011; Neumeier & Wolf, 2017). IT project risks occur on an organizational level and primarily result, inter alia, from the rapid innovation and diffusion of DTM and the interconnectedness of different IT assets.

Finally, we consider **failure propagation** as a third subtype. As IT assets are ever more connected, there is a *high risk of interrelated failures* that harm not only single IT assets but whole IT networks (P. Chen et al., 2011). For instance, in 2017 a simple typo by an Amazon programmer took several servers offline which caused losses of approximately $150 million among companies in the S&P 500 using Amazon Web Services (NPR, 2017). In 2013, cybercriminals identified vulnerable nodes of the U.S. emergency alert systems, gained access, and managed to send out false alerts in Michigan, Montana, and New Mexico (Green et al., 2020). A similar incident occurred in Hawaii where a state employee triggered an alert by clicking the wrong option from a computer menu (Hennigan, 2018). Both IT assets and IT projects may be intertwined in such a way that failures of one project can cause a cascade of failures in other projects leading to substantial financial losses (Beer et al., 2015; Guggenmos et al., 2019). Failure propagation occurs primarily on an organizational level and result, inter alia, from the low-cost interconnectedness and the low-cost ubiquity provided by DTM.

2.2.5.6 Impairment of health

Digitalization can adversely affect individuals' health. This RSED is of particular importance as the ***impairment of health*** can have major consequences for individuals (Anderson & Agarwal, 2011). The first subtype, **psychological health problems,** comprises the manifestation of *reduced mental health from excessive use of DTM*. Related effects that may occur

include sleep disorder, burnout, depression, and suicide (Kyung et al., 2017; Pirkkalainen & Salo, 2016). **Psychological health problems** may also manifest as *technostress* (i.e., stress resulting from the use of DTM; Galluch et al., 2015; Maier et al., 2015; Pirkkalainen & Salo, 2016; Srivastava et al., 2015; Tarafdar et al., 2007), *IT anxiety* (Heinssen et al., 1987; Thatcher & Perrewé, 2002), *body image insecurity* (e.g., social media images of thin models may foster insecurity and encourage eating disorders; Heid, 2017), *negative effects on personal wellbeing* (e.g., human degradation through social media; Sedera et al., 2017), and *social overload*, i.e., excessive social contact and self-disclosure (X. Chen & Wei, 2019). Heavy use of DTM may lead to a *feeling of social isolation* (Sedera et al., 2017) or *loneliness* (Matook et al., 2015). During the COVID-19 pandemic, in particular, this feeling was increased by DTM-enabled remote work that helped to limit the spread of the virus. Among others, the manifold manifestations of **psychological health problems** are closely related to the low-cost interconnectedness and the low-cost ubiquity of DTM. As with any health impairment, the effects cause harm on an individual level. **Psychological health problems** are already strongly covered in extant IS research, as has been reviewed by Pirkkalainen and Salo (2016).

Another more specific subtype of ***impairment of health*** is **addiction to DTM and resultant issues**. An addiction to DTM may result in serious mental or physical complaints, such as depression or obesity (Blech, 2019). *Excessive smartphone or internet use* is fostered by persuasive technologies based on business models that focus on eyeball time—that is, the time a visitor spends on a specific app or website (Soror et al., 2015). The *excessive use of computer games* allows users to escape from problems in other domains by experiencing feelings of power, achieving instant gratification, and being part of a community of gamers (Ledder, 2013). Such addictions may lead to a *worsening of human cognition* (e.g., less deep thinking, less nuanced ideas, worse memory), *reduction of emotional intelligence* (e.g., empathy) (Steinmetz, 2017-2018), *neglect of responsibilities* (e.g., at school, at work), *deterioration of adolescents' mood* (e.g., loneliness, envy, suicidal thoughts) (Pirkkalainen & Salo, 2016), and impaired development of self-image due to reduced interpersonal contact. Furthermore, frequent users of DTM may develop a *fear of missing out* (Ledder, 2013). Additionally, some research links *changes to children's brains* to media multitasking (Heid, 2017). The subtype **addiction to DTM and resultant issues** can be linked, inter alia, to the low-cost ubiquity of DTM and effects are felt primarily on an individual level.

Additionally, the ***impairment of health*** manifests as a **reduction of physical health** resulting *directly from excessive use of DTM*, with symptoms including short-sightedness, lack of ac-

tivity, and obesity (Goos, 2018). Furthermore, the use of DTM may indirectly lead to a reduction in physical health via effects such as the *spread of infectious diseases*. In the USA, for example, the introduction of Craigslist meant intimate encounters with strangers could be arranged with ease and led to an increased rate of HIV infections (Chan & Ghose, 2014). The **reduction of physical health** is primarily fostered by low transaction costs, low-cost interconnectedness, and the low-cost ubiquity of DTM. As with any health-related issues, the **reduction of physical health** impacts on an individual level.

The different subtypes of ***impairment of health*** are interrelated: Addiction is a specific form of psychological illness; psychological and physical illness may be mutually dependent. Three of the four dark side phenomena identified in the extensive literature review by Pirkkalainen and Salo (2016) belong to the RSED ***impairment of health***, namely *technostress*, *IT addiction*, and *IT anxiety*. Their fourth dark side phenomenon—*information overload*—belongs to the RSED ***ambiguous decision environment***.

2.2.5.7 Environmental deterioration

Resource requirements related to digitalization can lead to ***environmental deterioration.*** The first subtype refers to the **climate impact of energy demand**. Massive (and ever-increasing) amounts of energy are consumed by data centers and computing tasks (Graf et al., 2018; J. K. Lee, 2015). For instance, blockchain-based solutions require more energy than traditional centralized architectures (Sedlmeir et al., 2020). The energy consumption of blockchain-based cryptocurrencies (e.g., Bitcoin) is particularly high (Sedlmeir et al., 2020). The **climate impact of energy demand** is felt on a societal level and is, inter alia, a result of the low-cost ubiquity and rapid innovation and diffusion of DTM.

A second subtype we discuss is the increasing **consumption of material resources**. With the manufacturing of digital technologies (e.g., smartphones, computers) comes *massive raw-material requirements* (e.g., rare earths; Graf et al., 2018). Furthermore, as the lifecycle of digital technologies is comparatively short, there is a tremendous *generation of waste* (Graf et al., 2018). Electronics waste is the world's fastest-growing solid-waste stream (Semuels, 2019). As electronics waste can contain dangerous materials (e.g., mercury, beryllium), there are severe environmental risks (Semuels, 2019). The **consumption of material resources** is a concern that impacts on a societal level and is caused, primarily, by the ubiquity of DTM and their rapid innovation and diffusion.

2.2.5.8 Loss of privacy

Loss of privacy is the DTM-related actual or perceived loss of freedom from inappropriate intrusion by other individuals, organizations, or states. This RSED is broadly discussed in research and in society at large and can be seen as one of the most important ethical, legal, social, and political issues of the information age (Hong & Thong, 2013; Smith et al., 2011). The public debate on privacy draws ever more attention with the ongoing emergence of "increasingly ubiquitous technologies centered around the collection of consumer data" (Adjerid et al., 2018). As a first subtype of the RSED, we discuss **privacy breaches**, i.e., events involving the misuse of individuals' personal information (Acquisti et al., 2006). In this context, Smith et al. (1996) identified seven information privacy concerns, namely collection, unauthorized secondary use (internal), unauthorized secondary use (external), improper access, errors, reduced judgment, and combining data. One of the world's most notorious privacy breaches was the Cambridge Analytica scandal. During Donald Trump's 2016 presidential campaign, Cambridge Analytica used illegally obtained data from a Facebook quiz app to identify users' specific characteristics and target them with tailored political content (i.e., microtargeting) (Perrigo, 2018). When the Sony PlayStation Network was hacked in 2011, delinquents accessed personal and financial information from more than 77 million user accounts (Goode et al., 2017). Further, *privacy disasters* may also occur when an organization uses data to achieve a business advantage in a way that is legal "but violates public norms for acceptable use" (Culnan, 2019). For instance, personal algorithm-based recommendations may be appreciated by some people, but they may also be considered as an *intrusion into individuals' privacy* (Adjerid et al., 2018; Thiesse, 2007; Watson & Nations, 2019). Hence, there is a growing call for algorithmic transparency, i.e., organizations sharing information about how they use algorithms to analyze customer data (Watson & Nations, 2019). As **privacy breaches** concern individuals' personal information, these take effect on an individual level. However, privacy breaches also have a negative impact on the organizations involved. **Privacy breaches** are enabled by several affordances provided by DTM; inter alia, by low cost- interconnectedness and low-cost ubiquity.

Ambivalent self-disclosure as the second subtype relates, primarily, to the use of social media. As individuals' social connections on social media are very diverse (e.g., friends, relatives, co-workers), users may have *different role expectations* and *role conflicts* (Liu et al., 2019). For instance, private party pictures may negatively affect users' professional careers (Liu et al., 2019). As a consequence, users may feel obliged to show an image of themselves that does not correspond to their real personality (Pariser, 2019). Social media might also

undermine freedom of expression and the free flow of information, as users expressing socially unacceptable ideas can suffer from social sanctions (e.g., isolation, cyberbullying; Huang et al., 2017). The potential negative consequences of self-disclosure are reinforced by the fact that it is virtually impossible to erase information once it has been made public on the internet (C. Alter, 2017). The subtype **ambivalent self-disclosure** occurs on an individual level and is fostered, inter alia, by high levels of social interconnectedness and the ubiquity of DTM.

Finally, DTM tremendously simplifies surveillance. **Digital surveillance** of individuals may be undertaken by different players (e.g., employers, governments, companies). *Monitoring employee behavior and performance* becomes increasingly easy and fine-grained with the use of DTM (Manzei, 2018; Vieira da Cunha et al., 2015). For instance, monitoring employees' use of the internet may be carried out on the understanding that many employees use the internet for non-work-related purposes during working hours (i.e., cyberloafing; Jiang, 2019). Further, there might be *privacy intrusion by using mobile device management solutions* for employees' personal mobile devices (Degirmenci et al., 2019). The screening of applicants' social media accounts might be considered surveillance of (potential) employees (Schmoll & Bader, 2019). Many companies also create digital dossiers of their customers by *aggressively cultivating and harvesting data* (Hong & Thong, 2013; Son & Kim, 2008). For example, consumer location tracking, which is used for location-based advertising, might be perceived as a privacy intrusion (Bhagat & Kim, 2018; M Y et al., 2019). Smartphones, other IoT devices (e.g., Amazon Alexa, Google Echo), and ambient sensing and recording technology might also be considered intrusive (Edwards, 2018). DTM has played a part in enabling *privacy intrusion by governments or law enforcement authorities*. For instance, law enforcement authorities may use facial recognition technologies or body-worn cameras (J. Lee et al., 2016). Other examples of governments' digital surveillance include the Chinese Social Credit System and the surveillance of digital communications by agencies such as the U.S. National Security Agency (NSA) (Tanriverdi & Chen, 2018). Perceived privacy intrusions might also occur in the private sphere. For example, activity tracking apps (e.g., Runtastic, Strava) allow *constant surveillance by peers* (Rockmann & Gewald, 2017). Members of virtual neighborhood communities (e.g., Nextdoor) can *share surveillance videos* that show allegedly suspect incidents in their neighborhoods (Mingels, 2019), and social media users may be *spied out by fake profiles* (Baumgärtner & Höfner, 2020). **Digital surveillance** occurs primarily at the individual and societal levels and is enabled, inter alia, by the low-cost ubiquity of DTM and the handling of big data.

2.2.5.9 Ambiguous decision environment

Digitalization can put decision-makers in undesired ***ambiguous decision environments*** in which they are provided with untrustworthy or contradictory information on facts and agency. The first subtype, **uninformative information**, relates to the dissemination of vast amounts of unreliable information (e.g., *fake news*; Nasralah et al., 2018). Unreliable information may be presented in simple social media posts and comments, or manipulated media content such as images, or audio and video files (e.g., *deepfakes*; Rosenbach, 2018). The systematic dissemination of fake news occurs during electoral campaigns (cf. **manipulation of democratic elections**). A further specific example is the dissemination of health misinformation which "caused severely negative consequences to individuals' healthcare and public health" (Gu & Li, 2020; Islam et al., 2020). For instance, the widely spread misinformation that highly concentrated alcohol kills the COVID-19 virus has led to the deaths of approximately 800 people and the hospitalization of 6,000 (Gu & Li, 2020; Islam et al., 2020). A further example are *spam reviews* which serve to influence customers' purchase decisions (Wijnhoven & Pieper, 2018). The phenomenon of unreliable information is amplified by *algorithm-based information filtering* (i.e., filter bubbles) and a perceived *information overload* that occurs due to the ubiquity of DTM (X. Chen & Wei, 2019; D'Arcy et al., 2014). These effects occur at the individual, the organizational, and the societal levels and are fostered, inter alia, by simplified broadcasting and low-cost anonymity provided by DTM.

As the second subtype, we describe the phenomenon of **uncertain agency**. Social media is threatened by a high number of *fake accounts* and *automated bots* (Vick, 2019). In this way, delinquents pursue different goals. Firstly, fake accounts and automated bots may serve as disseminators of (political) propaganda and fake news. Secondly, fake accounts may be used to gain trust, obtain (personal) information, and commit fraud crimes (Baumgärtner & Höfner, 2020). Social media users may not know whether they are communicating with a real person or an automated bot (Rosenbach, 2018). Furthermore, the prevalence of *anonymous social media accounts* makes it difficult or impossible to hold people responsible for malicious social media use. Beyond social media bots, advances in AI allow more natural voice interaction (e.g., Google Duplex). Among others, the phenomenon of **uncertain agency** is enabled by the low-cost anonymity provided by DTM and may harm primarily individuals.

Another subtype, the **loss of autonomy to act,** results from omnipresent *recommendation engines* which ensure that one's own opinion is reinforced, creating a *manipulative choice architecture* (Zuboff, 1988). With the help of personalized recommendations, consumers are

continually pushed towards impulse buying in various online shops (Leidner, 2019). *Recommendation engines* are enabled by intelligent, ubiquitous *surveillance machines* (e.g., smartphones, smart home applications) that collect vast amounts of personal data (cf. **digital surveillance**; Jung et al., 2018). Further, personal data digitalization may be an affront to inherent human dignity in the form of constraining, coercing, or manipulating individual autonomy (Leidner & Tona, 2021). Often, users do not know which data are collected and analyzed when using DTM (Thimm, 2019). These developments are known as "surveillance capitalism" or "digital surveillance economy" (Leidner, 2019; Zuboff, 1988). The **loss of autonomy to act** occurs on an individual level. It is enabled, inter alia, by low transaction costs and the ubiquity of DTM.

Finally, we present the subtype **diffusion of responsibility,** which relates to the growing importance of automated decision-making. There are ever more autonomous technologies (e.g., self-driving cars, autonomous weapons) leading to unclear accountability regarding unforeseen incidents (Fritz et al., 2020). For example, people might be injured or killed in accidents involving self-driving cars (Geistfeld, 2018). The **diffusion of responsibility** occurs on a societal level and relates to the automated decisions and actions enabled by DTM and the ability to handle big data.

2.2.5.10 Undesirable behavioral adaptations

DTM causes ***undesirable behavioral adaptations*** when traditional competencies and behaviors change in a socially undesirable manner. **Technology-reliance along with increasing incompetence** is a specific subtype. As humans become increasingly reliant on DTM to complete their tasks, there is an increasing *loss of traditional human capabilities* (e.g., formal writing skills, craftmanship, learning; Wüst, 2018) and a *decrease of unique human knowledge* (Fügener et al., 2021). Permanent use of DTM may even negatively influence peoples' ability to read emotions (Cook, 2016). Additionally, there is an increasing *loss of ability to manually control complex technologies* when automatic control mechanisms fail (e.g., airplanes, self-driving cars; (Evers, 2019). For instance, pilots use the autopilot during large parts of a flight and might thus struggle with unforeseen technical issues (Evers, 2019). The subtype of **technology reliance, along with increasing incompetence** occurs on an individual and a societal level and is primarily related to automated decisions and actions enabled by DTM and its low-cost ubiquity.

Data fixation is the second subtype. Within the digital era, real events or entities are reduced to their representation in digital data which necessarily comes along with a *reductionist reflection of reality* (Manzei, 2018). Tacit knowledge (e.g., intuitions, personal knowledge) cannot be fully captured by data (Manzei, 2018). However, we can observe an increasing importance of scoring systems, performance measures, and popularity metrics both in business and society. For instance, the permanent measurement of employees' performance might lead to a *displacement of creative or innovative activities* (Jung, 2020). Further, the supposed transparency and competence of scoring systems lead to a lack of reflection and a potential misallocation of resources, for example, in terms of project budgets or investments in customers (Clarke, 2016). Additionally, companies harvest massive amounts of user data in their attempts to improve users experience and manipulate the attention of users (i.e., growth hacking; cf. **digital surveillance** and **loss of autonomy to act**; McNamee, 2019). In this context, users are increasingly considered as a metric, rather than as people (i.e., depersonalization; McNamee, 2019). Furthermore, **data fixation** also occurs in private life. Personal data digitalization may divert attention away from important areas for well-being and instead direct it to areas that are digitizable (Leidner & Tona, 2021). Users of social media are often particularly focused on popularity metrics, such as followers, views, or likes (Steinmetz, 2018c). This may have problematic consequences, such as a negative impact on one's self-worth (Steinmetz, 2018c). Moreover, people tend to miss experiences in real life because they are always busy taking and posting photos or videos of their activities, striving for recognition and likes on social media (Steinmetz, 2018a). Finally, self-quantification may have disempowering effects (Moya & Pallud, 2020). The phenomenon of **data fixation** occurs primarily at the individual level. It is enabled, inter alia, by the ubiquity of DTM and the capacity to handle big data.

Next, we consider the subtype of **poor time and workload management**. DTM lead to ubiquitous *technology-mediated interruptions* (i.e., interruption overload; Addas & Pinsonneault, 2015; A. Chen & Karahanna, 2018; Tams et al., 2018; Tams et al., 2020). Employees who are continuously interrupted by incoming emails or chat messages may struggle to focus on complex work tasks (Addas & Pinsonneault, 2018). The continuous flow of incoming messages or notifications leads to the phenomenon of *constant checking* or *compulsive smartphone use* (Gerlach & Cenfetelli, 2020; Sedera et al., 2017; C. Wang & Lee, 2020). For instance, the smartphone is "the first thing many users reach for when waking up in the morning" (C. Wang & Lee, 2020). Constant checking might distract from principal activities, such as taking care

of children (Weinert et al., 2016). Further, DTM enforce the occurrence of multitasking situations (D'Arcy et al., 2014). These phenomena lead to the perception of poor time management (Polites et al., 2018). Mobile devices increasingly blur work-nonwork boundaries and lead to an *intertwining of personal and work spheres* (i.e., work-life conflict; Benlian, 2020; Tams et al., 2020; Weinert et al., 2016). Often, the work sphere invades private life (e.g., constant availability), but private issues may also intrude into the work sphere, as when employees use the internet for non-work-related purposes during work time (i.e., *cyberloafing*; Jiang, 2019). The phenomenon of **poor time and workload management** occurs on an individual level and is enabled, primarily, by high levels of interconnectedness and the ubiquity of DTM.

We also consider the subtype **erosion of solidarity**. As companies harvest ever more personal data on their customers, there might occur a *gradual shift from personalization to desolidarization* (e.g., telematics tariffs of car insurances, self-tracking based health insurance pricing; Eling & Kraft, 2020; McFall, 2019; Wiegard et al., 2019). As another example, digital neighborhood communities (e.g., Nextdoor) may *reinforce the demarcation of homogenous neighborhoods*. Users of digital neighborhood communities who regularly report suspicious incidents in their neighborhoods often practice racial profiling (Mingels, 2019). The **erosion of solidarity** occurs on a societal level and is enabled, inter alia, by the increasing ability of big data handling and the ubiquity of DTM.

The subtype **negative spillovers** describes negative events in the offline world that are caused by previous interactions or activities online (Mikhaeil & Baskerville, 2017). For instance, mass instigation on social media might lead to racially motivated offenses in the offline world (cf. **trend towards extremism**; Baumgärtner et al., 2019). Further, there are ongoing discussions about whether the glorification of physical violence in computer games encourages physical violence in the real world (Ledder, 2013). **Negative spillovers** occur on a societal level and are enabled, inter alia, by simplified broadcasting and low-cost interconnectedness.

2.2.5.11 Rogue algorithms

Rogue algorithms refer to complex and networked algorithms that are beyond proper human understanding and control. As a first subtype, we discuss the **lack of auditability**. Due to the increasing complexity of algorithms, humans might *lose control over self-learning systems*. For instance, Microsoft launched an AI-based Twitter bot that soon disseminated extreme right-wing statements (The Telegraph, 2016). Unlike many other products, *digital technologies do not have to undergo standardized audits* before their market launch. Prior to their

release, we do not know whether such digital technologies will have a negative effect on society (Forbes, 2016). This applies even in the case of systems used by law enforcement agencies (e.g., predictive policing, recidivism prediction; Feuerriegel et al., 2020; Meijer & Wessels, 2019). Hence, unwanted or erroneous functions may remain invisible. For instance, an erroneous system in Boeing's 737 Max was only discovered after two planes had crashed (Hennigan, 2019), while Volkswagen's manipulation of emissions data remained undetected for years, likely because it was not directly visible in the software code as it would have been in a hardware system (BBC, 2015). Another example regarding the **lack of auditability** is the ongoing discussion as to whether Huawei's 5G technology might serve as a spying tool for China's government (cf. **cyberterrorism and -warfare**; Campbell, 2019a). The **lack of auditability** occurs at the individual, organizational, and societal levels and results, inter alia, from the rapid innovation and diffusion of DTM and its ability to undertake automated decisions and actions.

As a second subtype, we present **discriminating algorithms**. Self-learning systems learning from a given data set (i.e., training data) tend to perpetuate the status quo reflected in the given data set, which may lead to "unjustified discrimination for and against population segments" (Clarke, 2016, p. 86). Hence, such systems might embed *racism and sexism* in search results or recidivism scores (Buolamwini, 2019). *Biased algorithms* may negatively influence credit scores, hiring processes, or judicial decisions (Liel & Zalmanson, 2020). For example, AI-based facial-recognition technology used by law enforcement authorities may recognize some population groups (e.g., white men) more accurately than others (e.g., women of color) (Campbell, 2019b). As another example, an AI-based system that should support Amazon's hiring processes by evaluating application documents preferred men as it recognized that current positions were predominantly held by men (Fritz et al., 2020; Liel & Zalmanson, 2020). Such gender bias occurs regularly as many data have been collected predominantly on men (i.e., *gender data gap*; Perez, 2020). **Discriminating algorithms** impact on an individual and a societal level and results, inter alia, from automated decisions and actions enabled by DTM.

Human-technology role reversal is as another subtype of the RSED ***rogue algorithms.*** While technology is controllable at a microlevel, at a macrolevel of complex algorithmic systems and their interaction, we see emergent and systemic nonlinearity (Demetis & Lee, 2018). *Technology-shaped agency* is a manifestation where humans become artifacts shaped by unintended consequences of complex interactions of DTM artifacts with reduced agency in technologized decision-making (Demetis & Lee, 2018). The manifestation of an *AI singularity* describes the fear that a general artificial superintelligence might rapidly evolve and surpass

all human intelligence. This could represent a serious threat to humanity (Campbell, 2018). **Human-technology role reversal** occurs on a societal level and relates, inter alia, to low-cost interconnectedness and automated decisions and actions enabled by DTM.

Finally, we describe the subtype of **(un)ethical programming**. With the development of ever more AI-based systems that decide or act autonomously, new ethical issues will inevitably arise. In borderline situations, autonomous systems have to choose the lesser evil (e.g., accidents involving self-driving cars; Precht, 2018). Ethical evaluations of such situations can vary considerably. However, programmers need to incorporate rules for these incidents. The configuration of these rules may depend on the cultural background of the programmer. As some groups (e.g., women, people of color) are underrepresented among programmers, *autonomous systems may have a cultural bias* (Precht, 2018). As DTM are used globally, there is an implicit *establishment of global norms, values, and morals* (Jung et al., 2018). Usually, the *explication of rules remains incomplete*, as programmers are not able to consider all possibilities. For instance, blockchain-based self-driving cars that are operated by smart contracts may only carry the highest bidder even in the case of a humanitarian emergency. Furthermore, programmers need to define the *tolerance limit for false positives*. As autonomous systems may harm individuals' health and life, this might be a serious challenge (e.g., autonomous vehicles, autopilot, autonomous weapons; Oehmke, 2018). Another ethical issue occurs in the social media environment. Usually, *social media algorithms prefer radical and highly emotive posts* as these garner greater attention (e.g., views, click rate) and thus generate higher profits (Beuth, Mingels, & Nelles, 2020). However, this practice leads to the promotion of extremist groups and parties (cf. **manipulation of democratic elections** and **distribution of inappropriate content**). This subtype of **(un)ethical programing** occurs on a societal level and is driven, inter alia, by automated decisions and actions enabled by DTM.

2.2.6 Discussion

Overall, the development and use of DTM make our world a better place. Yet, they also have adverse, unexpected, and unintended effects. Understanding the dark side of digitalization is a necessary precondition for containment of this dark side. Our taxonomy of the RSEDs supports this understanding by providing an overview, structure, and terminology. Specifically, the taxonomy comprises 11 RSEDs and their 39 subtypes.

The phenomena previously studied under the label "dark side of IT" are primarily included in ***impairment of health***, ***ambiguous decision environment***, ***error-prone IT operations***, and ***supporting delinquents***. Our taxonomy further comprises additional phenomena studied in IS

but not under the label dark side. Examples include echo chambers and filter bubbles (***ambiguous decision environment***). Beyond that, our taxonomy covers perceptions of current adverse effects and potential future risks that have not, so far, been adequately addressed in IS research. These include **technology reliance along with increasing human incompetence** (included in ***undesirable behavioral adaptations***), **discriminating algorithms** (included in ***rogue algorithms***), and **cyberterrorism and -warfare** (included in ***supporting delinquents***).

For each RSED subtype, we indicated a selection of related DTM affordances and the levels at which effects play out. Table 2.2-5 provides an overall view of all related affordances and affected levels. Big data handling, automated decisions and actions, rapid innovation and diffusion, and the low-cost ubiquity of DTM appear to be the most influential affordances in the sense that they relate to more RSED subtypes than the other affordances. The overview of the affected levels shows that RSEDs occur predominantly on an individual and a societal level. Some of the RSEDs and their subtypes occur only on a specific level (e.g., ***impairment of health***), while others cause harm on every level (e.g., ***supporting delinquents***) and should, therefore, be subject to increased scrutiny. The fact that many RSEDs relate to more than one level is a key reason we believe a multi-level taxonomy to be beneficial. Only a simultaneous consideration of multiple levels allows one to see the full effect of the phenomena.

2.2.6.1 Contributions

Our paper contributes to IS literature in three ways: The first contribution is a generalized conceptualization of RSEDs. Discussions of the dark side of digitalization are already present in IS literature (e.g., Majchrzak et al., 2016; Pirkkalainen & Salo, 2016; Tarafdar et al., 2015b; Turel et al., 2021). We add to this stream by leveraging economic theory, philosophy of law, and philosophy of technology, and by conceptualizing RSEDs as adverse secondary effects, or the possibility of such effects, arising from digitalization (see section *Conceptualization*).

Our second contribution is the definition (see Table 2.2-4) and description of specific RSEDs and their subtypes. Some of these constructs are well-established in scholarly literature, while others are rather novel to the academic discourse. The labeling and definition of the constructs provide terminology and inspiration for future research exploring the RSEDs and their subtypes in detail. The descriptions include numerous manifestations and specific examples along with references to academic and journalistic articles. This anchors discussions about RSEDs in a cumulative body of knowledge and provides guidance for further reading.

RSEDs	RSED Subtypes	Affordances of DTM								Level		
		Low transaction costs	Simplified broadcasting	Low-cost anonymity	Low-cost interconnectedness	Low-cost ubiquity	Rapid innovation and diffusion	Automated decisions and actions	Big data handling	Individual	Organizational	Societal
Dissemination of unscrupulous content	Distribution of inappropriate content		x	x	x					x	x	x
	Personal attacks			x	x					x		
Supporting delinquents	Socially undesired transactions	x		x			x			x		x
	Cybersecurity breaches	x		x		x	x	x	x	x	x	
	Cybercrime			x	x	x	x			x	x	
	Aggravation of prosecution			x			x	x	x			x
	Cyberterrorism and -warfare	x	x	x			x	x	x			x
Adverse socio-economic shifts	Displacement of established structures	x					x	x	x		x	x
	Digital inequalities					x	x			x		x
	Superpowerful corporations	x	x		x	x	x		x	x	x	x
	Loss of international competitiveness	x					x		x		x	x
Shifting political control	Trends towards extremism		x		x			x				x
	Political regimes strengthening control		x		x	x		x	x	x		x
	Lack of policy making				x		x				x	x
	Manipulation of democratic elections		x					x	x			x
Error-prone IT operations	IT operational risks				x	x	x	x	x	x	x	
	IT project risks				x	x	x				x	
	Failure propagation				x	x		x	x		x	
Impairment of health	Reduction of psychological health	x	x		x	x	x	x		x		
	Addiction to DTM and resultant issues	x	x			x	x			x		
	Reduction of physical health	x			x	x				x		
Environmental deterioration	Climate impact of energy demand	x				x	x		x			x
	Consumption of material resources					x	x					x
Loss of privacy	Privacy breaches				x	x	x		x	x	x	
	Ambivalent self-disclosure		x		x	x				x		
	Digital surveillance				x	x	x		x	x		x
Ambiguous decision environment	Uninformative information		x	x	x			x	x	x	x	x
	Uncertain agency		x	x				x		x		
	Loss of autonomy to act	x				x		x	x	x		
	Diffusion of responsibility							x	x			x
Undesirable behavioral adaptation	Technology-reliance along with increasing incompetence					x		x		x		x
	Data fixation					x		x	x	x		
	Poor time and workload management	x			x	x				x		
	Erosion of solidarity					x		x	x			x
	Negative spillovers		x	x	x							x
Rogue algorithms	Lack of auditability						x	x	x	x	x	x
	Discriminating algorithms							x	x	x		x
	Human-technology role reversal				x		x	x	x			x
	(Un)ethical programming						x	x	x			x
	Number of occurrences:	12	12	10	18	21	21	21	22	23	13	24

Table 2.2-5: Overview of affordances and affected levels

Thirdly, we provide a taxonomy and embedding of the RSEDs. This contribution includes hierarchical relationships between RSEDs, their subtypes, manifestations, and examples. Furthermore, it relates RSED subtypes (and, indirectly, the RSED) to DTM affordances and the level affected (see section *Taxonomy of RSEDs* and summary in Table 2.2-5). Prior IS research on the dark side has been strongly focused on the individual level (Pirkkalainen & Salo, 2016; Tarafdar et al., 2015b; Turel et al., 2021). Our taxonomy clearly shows that the dark side also affects the organizational and societal levels.

Overall, these three contributions provide a holistic perspective that broadens the IS community's understanding of the dark side of digitalization and provides a repository for future research to draw on. With these contributions, this paper follows many calls for research in this direction (Majchrzak et al., 2016; Pirkkalainen & Salo, 2016; Tarafdar et al., 2015b; Turel, 2019; Turel et al., 2021) and reiterates these calls: We need substantially more research illuminating the dark side of digitalization.

2.2.6.2 Limitations and strengths

This study is limited to perceived rather than objective RSEDs. RSEDs are socially constructed. We, as authors and readers, cannot stand outside of our socio-linguistic constructs to view them objectively. However, by drawing on various sources and disciplines, the taxonomy is not limited to the authors' perceptions but rather a union of the perceptions of numerous scholars and journalists. Turel et al. (2021) made an analogy between an iceberg and the dark side of digitalization. To them, the bottom of the iceberg represents what is not in sight: people's subconscious, physiological, and automatic processes. This is different from the perception argument we present here. What is subconscious, physiological, or automatic for individual people might still be perceptible by scholars, journalists, or society at large. Hence, our taxonomy brings to light parts of Turel et al.'s (2021) iceberg.

Like the authors, the scholars and journalists whose work informed the taxonomy were focused on Europe and North America. Some sources, especially in the academic discourse, also reported on phenomena in other regions. Yet, there is a chance that our taxonomy has a cultural bias towards self-expression and secular values. A more intercultural approach would in no way cause RSEDs to disappear but could lead to the identification of additional RSEDs or subtypes. Thus, we call for future research aiming to extend our taxonomy.

Most RSEDs can be studied empirically. However, some risks that do not (yet) materialize defy immediate empirical observation. Risks such as an AI singularity might eventually manifest but cannot be studied empirically today. However, antecedents of this risk, the prevalence

of perceiving the risk, and judgements about its likelihood and severity can be studied. Increased knowledge of the risk might lead to circumstances that reduce the likelihood of the risk's manifestation. Thus, the fact that the AI singularity has not yet occurred does not mean that the risk has never existed or might not exist. The challenge this poses for empirical studies does not mean that our theoretical contribution defies empirical testing.

Inevitably, there will always be a trade-off between parsimony and the breadth of a theory (Weber, 2012). Our aim was to comprehensively map the dark side of digitalization, and our taxonomy might thus be perceived as lacking parsimony. Future research may develop more parsimonious theories of identified dark side phenomena relating to specific technologies, affordances, or contexts.

As DTM and their uses continuously evolve, the RSEDs will change over time. Hopefully, some of the RSEDs will disappear, while others will change and additional RSEDs will appear. Hence, our taxonomy should be seen as a snapshot of the current RSEDs. Having multiple layers of abstraction and focusing on affordances rather than individual technologies, we expect the top-level RSEDs to remain up-to-date for five or perhaps ten years. However, beyond this point, they will require periodic review and refinement.

Some readers of this paper might feel to some extent dissatisfied to see a vast number of adverse effects of digitalization but neither an in-depth analysis of any of these nor a strong proposition as to how they should be managed. To some degree, we as authors feel the same way. Each RSED subtype could be investigated in more depth and could be embedded in a nomological net of antecedents and consequences, along with detailed causal reasoning and first-hand empirical support beyond anecdotes or literature. In fact, this should happen. However, given the breadth and multifaceted nature of RSEDs, doing so for every RSED subtype is beyond the scope of a single paper. Yet, we believe that the IS community can play an important role in designing and evaluating approaches to RSED management. This paper steps in this direction by highlighting the breadth and manifold facets of RSEDs. Future research should embark on analyses of individual RSED subtypes and work towards countermeasures.

We see a strength in our original theoretical contributions (conceptualization of RSEDs in general, definition and description of constructs, arrangement and embedding of constructs) mapping an emerging, relevant, and understudied phenomenon. We see a further strength in the rigorous, extensive, iterative taxonomy development process leveraging a broad array of sources: academic journals, academic conferences, public media coverage of digitalization, interdisciplinary interviews and workshops, and written and oral feedback. Each of these

sources has distinct well-known weaknesses (e.g., relating to scientific rigor or timeliness). We believe that the iterative combination of these different sources enabled us to harness their respective advantages and, to some degree, compensate for their non-overlapping weaknesses. The result is an empirically grounded, multifaceted, comprehensive taxonomy of RSEDs.

A theory of analysis is "only" the lowest level of theory in the perspective put forward by Gregor (2006). Other theories explaining and/or predicting, and theories for design and action, are more advanced. In some ways, these other types of theories are more valuable. However, they require underlying theories of analysis. In this sense, our contribution may provide the foundation for future theories explaining and predicting RSEDs and suggesting design and actions with which they can be avoided.

2.2.6.3 Implications for theory and research

The intended users of our taxonomy of RSEDs are primarily IS scholars. The taxonomy provides a terminology and structure of RSEDs that may be observed in business and everyday life, but that has not yet been widely discussed in scientific literature. Due to the broad character of our taxonomy, we see various fields of application in IS research. However, the taxonomy may be adopted in other disciplines, such as criminology, psychology, economics, and political science that study digitalization from their own disciplinary perspectives. Hence, the taxonomy may be a starting point for interdisciplinary research projects examining the adverse, unintended effects of digitalization from a holistic perspective. (Interdisciplinary) research teams may further analyze antecedents, consequences, and boundary conditions of the 11 RSEDs and build new substantive theories of the identified dark side phenomena. Moreover, researchers may search for similarities in terms of affordances and levels affected between well-researched areas (e.g., technostress) and rather unknown adverse effects. This might help to develop more abstract, general theories of dark side phenomena.

In the development of new DTM-based systems, design science researchers may consider the affordances and use the taxonomy for the initial identification of potential RSEDs. Additionally, researchers may take a complementary perspective by systematically considering all levels affected, starting with the one they wish to improve but also considering potential externalities at other levels. At each level, the researcher should evaluate whether the related RSEDs may occur when using the new IT-based system.

In behavioral science, researchers may use our taxonomy as a basis for developing and responding to manifold research questions. For instance, the taxonomy may be helpful for ex-

amining perceptions of digitalization within groups from different cultures, ages, or professions. Furthermore, empirical research should evaluate the importance of single RSEDs for the different levels affected. Doing so will help to develop an order of priority for the identification, development, assessment, and ongoing monitoring of appropriate mitigation mechanisms to contain RSEDs (Kim et al., 2011; Nelson & Kletke, 1990; Tarafdar et al., 2015b). Researchers and policy makers need to consider how to identify and reduce features of DTM that are likely to cause harm without (excessively) limiting the benefits of digitalization (Nelson & Kletke, 1990; Tarafdar et al., 2015b). Seeing the breadth of dark side phenomena may spur the development of management approaches on an individual, organizational, and societal level. There may be specific management approaches addressing individual RSED subtypes or manifestations. Yet, even greater value lies in approaches that transcend different RSEDs. Tying these to affordances might be a good starting point.

2.2.6.4 Practical implications

Practitioners working on the analysis and design of DTM-based systems can use our taxonomy to identify potential RSEDs related to the use of specific systems.

The ability to identify RSEDs will help developers of DTM to produce DTM-based systems that minimize the effects of RSEDs, develop appropriate countermeasures, or – at the very least – remain informed about potential RSEDs. This will make it easier for computing professionals, members of *ACM*, and members of *IEEE* to comply with their codes of ethics.

Organizations can use the taxonomy and its embedding to identify RSEDs that put the organization at risk. For this, they should start with the RSEDs related to the organizational level. Further, they might identify RSEDs resulting from their own activities. For this, they should start from their use of DTM and related affordances to select the RSEDs most likely related to their activities. Regardless of the pathway, once they have identified RSEDs and recognize substantial relevance, they should develop mitigation or hedging strategies.

Policy experts can use the taxonomy to evaluate whether present legislation is sufficient to cover the effects of innovative DTM. For instance, our taxonomy sheds light on the adverse effects of DTM on individuals who need to be protected by legislation in a particular way. This may help to reduce the RSED subtype ***lack of policy making***. Possible policy mechanisms include regulation, prohibitions, and subsidies. For example, one might think about establishing an equivalent of the *U.S. Food & Drug Administration (FDA)* for technology to ensure the safety of new DTM (McNamee, 2019). The challenge will be to limit RSEDs without excessively curtailing the manifold benefits of digitalization.

2.2.7 Conclusion

IS scholars have called for the adoption of a "positive lens" in IS research (Agogo & Hess, 2017, p. 1). Yet, we believe that our discipline benefits from a detailed and comprehensive perspective on the dark side of digitalization. This is especially the case as IS scholars tend to have a pro-IT bias that they may need support to overcome (Majchrzak et al., 2016). Adverse effects of the increasing use of digital technologies and media are real. Their existence is increasingly present in public awareness. We, as IS scholars, need a sound understanding of these adverse effects to support the public debate and mitigate the RSEDs. We also need such an awareness if we are to meaningfully contribute to the net benefits of digitalization. We do not present the dark side in order to spread fear, but offer a package insert for digitalization that lists the risks and side effects in order to promote sensible decisions. Metaphorically speaking, IS scholars have to know the corners and angles of the dark side if they want to provide light. Our taxonomy maps these corners and angles. As theory of the problem and theory for analysis, it provides a basis for illuminating the dark side. Digitalization is made by us—we can shape it for maximum net benefit.

References

ACM. (2018). *The ACM Code of Ethics and Professional Conduct*. https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-and-professional-conduct.pdf

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. In *International Conference on Information Systems*, Milwaukee, Wisconsin, USA.

Addas, S., & Pinsonneault, A. (2015). The many faces of information technology interruptions: a taxonomy and preliminary investigation of their performance effects. *Information Systems Journal*, *25*(3), 231–273. https://doi.org/10.1111/isj.12064

Addas, S., & Pinsonneault, A. (2018). E-Mail Interruptions and Individual Performance: Is There a Silver Lining? *MIS Quarterly*, *42*(2), 381–405. https://doi.org/10.25300/MISQ/2018/13157

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. *MIS Quarterly*, *42*(2), 465–488. https://doi.org/10.25300/MISQ/2018/14316

Agogo, D., & Hess, T. J. (2017). "Yin and Yang": Integrating the Bright Side into Dark Side Research in IS. In *Americas Conference on Information Systems*, Boston, Massachusetts, USA.

Alter, C. (2017, July 10). The new scarlet letter. *TIME*, 190(2/3), pp. 60–65.

Alter, S. (2017). A Balanced Perspective on the Bright and Dark Sides of IT Based on a Systems Theory of IT Innovation, Adoption, and Adaptation. In *Annual Workshop of the Special Interest Group: Adoption and Diffusion of Information Technology (SIGADIT)*, Seoul, Korea.

Amann, M., & Rosenbach, M. (2019, May 18). Schäuble will Anonymität im Netz beenden. *DER SPIEGEL*(21), p. 12.

Anderson, C. L., & Agarwal, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Information Systems Research*, *22*(3), 469–490. https://doi.org/10.1287/isre.1100.0335

Ashby, M. P. J., & Tompson, L. (2017). Routine Activities and Proactive Police Activity: A Macro-scale Analysis of Police Searches in London and New York City. *Justice Quarterly*, *34*(1), 109–135.

Bartz, T., Mingels, G., & Rosenbach, M. (2019, June 22). König Zuckerbergs Dukaten. *DER SPIEGEL*(26), pp. 60–63.

Baskerville, R. L., Myers, M. D., & Yoo, Y. (2020). Digital First: The Ontological Reversal and New Challenges for Information Systems Research. *MIS Quarterly*, *44*(2), 509–523. https://doi.org/10.25300/MISQ/2020/14418

Baumgärtner, M., Becker, S., Bohr, F., Diehl, J., Gebauer, M., Gude, H., Heise, T., Höfner, R., Holscher, M., Knobbe, M., Lehberger, R., Lehmann, T., Meyer-Heuer, C., Müller, A.-B., Müller, A.-K., Neumann, H., Pouplier, R., Röbel, S., Rosenbach, M., . . . Wiegrefe, K. (2019, October 12). Stream läuft. *DER SPIEGEL*(42), pp. 12–17.

Baumgärtner, M., & Höfner, R. (2020, January 25). Falsche Freunde. *DER SPIEGEL*(5), pp. 26–31.

BBC. (2015). *Volkswagen: The scandal explained*. https://www.bbc.com/news/business-34324772

Beekhuyzen, J., Hellens, L. von, & Nielsen, S. (2015). Illuminating the underground: the reality of unauthorised file sharing. *Information Systems Journal*, *25*(3), 171–192. https://doi.org/10.1111/isj.12069

Beer, M., Wolf, T., & Zare Garizy, T. (2015). Systemic Risk in IT Portfolios - An Integrated Quantification Approach. In *International Conference on Information Systems*, Fort Worth, Texas, USA.

Benlian, A. (2020). A Daily Field Investigation of Technology-Driven Spillovers from Work to Home. *MIS Quarterly*, *44*(3), 1259–1300.

Berente, N., Seidel, S., & Safadi, H. (2019). Research Commentary—Data-Driven Computationally Intensive Theory Development. *Information Systems Research*, *30*(1), 50–64. https://doi.org/10.1287/isre.2018.0774

Bergengruen, V. (2020, August 7). The Wages of Hate. *TIME,* 196(9/10), pp. 58–61.

Beşer, A., Lackes, R., & Siepermann, M. (2016). The Quicker One is the Better One? - How to Fight Negative Word of Mouth. In *International Conference on Information Systems*, Dublin, Ireland.

Beuth, P., Groß, M., Hofmann, P., Hoppenstedt, M., Horchert, J., Kuntz, K., Rojkov, A., Sarovic, A., Scheuermann, C., & Schmidt, D. C. (2020, September 19). Unter Gläubigen. *DER SPIEGEL*(39), pp. 10–18.

Beuth, P., Mingels, G., & Nelles, R. (2020, October 17). Die Macht der Mythen. *DER SPIEGEL*(43), pp. 68–72.

Bhagat, S., & Kim, D. J. (2018). Why do People Geo-Tag themselves on Social Media? Role of Self-esteem, Need for Online Affiliation and Privcy Calculus. In *International Conference on Information Systems*, San Francisco, California, USA.

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, *18*(2), 66–79. https://doi.org/10.1016/j.jsis.2009.04.001

Blech, J. (2019, September 14). „Zocken, futtern, schwänzen“. *DER SPIEGEL*(38), p. 95.

Böhm, M., Mingels, G., & Rainer, A. (2019, December 28). Schwierige Pubertät. *DER SPIEGEL*(1), pp. 70–72.

Book, S. (2021). *Tesla auf Autopilot fährt gezielt in Highway-Streife*. https://www.spiegel.de/panorama/tesla-fahrzeug-auf-autopilot-faehrt-in-florida-gezielt-in-highway-streife-a-09054c62-4cc8-4423-ac26-14ef66cb13f5

Bremmer, I. (2017, November 13). Advantage China. *TIME*, 190(20), pp. 40–43.

Bremmer, I. (2018, May 14). The Strongman Era. *TIME*, 191(18), pp. 42–45.

Bronfenbrenner, U. (1981). *Die Ökologie der menschlichen Entwicklung: Natürliche und geplante Experimente*. Klett-Cotta.

Buolamwini, J. (2019, February 18). Because We Can Free Our Machines of Bias. *TIME*, 193(6/7), pp. 67–68.

Campbell, C. (2018, January 29). Baidu’s Brain. *TIME*, 191(3), pp. 42–45.

Campbell, C. (2019a, June 3). The Battle for 5G. *TIME*, 193(21/22), pp. 40–48.

Campbell, C. (2019b, December 2). The Fight for Our Faces. *TIME*, 194(24/25), pp. 52–55.

Carillo, K. D. A., & Marsan, J. (2016). “The Dose Makes the Poison” - Exploring the Toxicity Phenomenon in Online Communities. In *International Conference on Information Systems*, Dublin, Ireland.

Chan, J., & Ghose, A. (2014). Internet’s Dirty Secret: Assessing the Impact of Online Intermediaries in HIV Transmission. *MIS Quarterly*, *38*(4), 955–976.

Chen, A., & Karahanna, E. (2018). Life Interrupted: The Effects of Technology-Mediated Work Interruptions on Work and Nonwork Outcomes. *MIS Quarterly*, *42*(4), 1023–1042.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly*, *35*(2), 397–422.

Chen, X., & Wei, S. (2019). Enterprise social media use and overload: A curvilinear relationship. *Journal of Information Technology*, *34*(1), 22–38. https://doi.org/10.1177/0268396218802728

Clarke, R. (2016). Big data, big risks. *Information Systems Journal*, *26*(1), 77–90. https://doi.org/10.1111/isj.12088

Cook, J.-R. (2016). *Digital technology can be harmful to your health*. https://news-room.ucla.edu/stories/digital-technolgy-can-harm-your-health

Costello, G. J., Donnellan, B., & Curley, M. (2013). A Theoretical Framework to Develop a Research Agenda for Information Systems Innovation. *Communications of the Association for Information Systems*, *33*(1), Article 26, 433–462.

Culnan, M. J. (2019). Policy to Avoid a Privacy Disaster. *Journal of the Association for Information Systems*, *20*(6), 848–856. https://doi.org/10.17705/1jais.00554

D'Arcy, J., Gupta, A [Ashish], Tarafdar, M., & Turel, O. (2014). Reflecting on the "Dark Side" of Information Technology Use. *Communications of the Association for Information Systems*(35), Article 5, 109–118. https://doi.org/10.17705/1CAIS.03505

Decker, M. (2013). Technikfolgen. In A. Grunwald (Ed.), *Handbuch Technikethik* (pp. 33–38). Verlag J. B. Metzler. https://doi.org/10.1007/978-3-476-05333-6_6

Degirmenci, K., Shim, J. P., Breitner, M. H., Nolte, F., & Passlick, J. (2019). Future of Flexible Work in the Digital Age: Bring Your Own Device Challenges of Privacy Protection. In *International Conference on Information Systems,* Munich, Germany.

Demetis, D. S., & Lee, A. S. (2018). When Humans Using the IT Artifact Becomes IT Using the Human Artifact. *Journal of the Association for Information Systems*, *19*(10), 929–952. https://doi.org/10.17705/1jais.00514

Dewan, S., & Riggins, F. J. (2005). The Digital Divide: Current and Future Research Directions. *Journal of the Association for Information Systems*, *6*(12), 298–337.

Diehl, J., Knobbe, M., Rosenbach, M., & Wiedmann-Schmidt, W. (2019, May 25). Angriff auf WhatsApp. *DER SPIEGEL*(22), pp. 30–32.

Driouchi, A., Wang, M., & Driouchi, T. (2015). Determinants of software piracy under risk aversion: a model with empirical evidence. *European Journal of Information Systems*, *24*(5), 519–530. https://doi.org/10.1057/ejis.2014.14

Edwards, H. S. (2018, April 23). The Masters of Mind Control. *TIME,* 191(15), pp. 30–37.

Eling, M., & Kraft, M. (2020). The impact of telematics on the insurability of risks. *The Journal of Risk Finance*, *21*(2), 77–109. https://doi.org/10.1108/JRF-07-2019-0129

Evers, M. (2019, November 9). Bleiben Sie ruhig! *DER SPIEGEL*(46), p. 117.

Feuerriegel, S., Dolata, M., & Schwabe, G. (2020). Fair AI. *Business & Information Systems Engineering*, *62*(4), 379–384. https://doi.org/10.1007/s12599-020-00650-3

Fitzpatrick, A. (2018, December 17). Dr. Watch Will See You Now. *TIME,* 192(25/26), pp. 74–80.

Fitzpatrick, A. (2019, March 25). Boeing, the FAA and Newly Nervous Flyers. *TIME,* 193(11), pp. 7–8.

Flyvbjerg, B., & Budzier, A. (2011). Why Your IT Project May Be Riskier than You Think. *Harvard Business Review, 89*(9), 23–25. https://doi.org/10.2139/ssrn.2229735

Forbes. (2016). *The Darker Side of Digital*. https://www.forbes.com/sites/falgunidesai/2016/03/31/questioning-the-digital-shift/amp/

Friedmann, J. (2019, April 6). Längere Haft für Hacker. *DER SPIEGEL*(15), p. 22.

Fritz, A., Brandt, W., Gimpel, H., & Bayer, S. (2020). Moral agency without responsibility? Analysis of three ethical models of human-computer interaction in times of artificial intelligence (AI). *De Ethica, 6*(1), 3–22. https://doi.org/10.3384/de-ethica.2001-8819.20613

Fröhlingsdorf, M. (2019, December 28). „Wie ein Heroin-Junkie“. *DER SPIEGEL*(1), pp. 34–37.

Fügener, A., Grahl, J., Gupta, A [Alok], & Ketter, W. (2021). Will Humans-in-the-Loop Become Borgs? Merits and Pitfalls of Working with AI. *MIS Quarterly, 45*(3), 1527–1556. https://doi.org/10.25300/MISQ/2021/16553

Galluch, P., Grover, V., & Thatcher, J. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context. *Journal of the Association for Information Systems, 16*(1), 1–47. https://doi.org/10.17705/1jais.00387

Geistfeld, M. (2018, April 16). How Liable Should Driverless-Car Companies Be for Accidents? *TIME,* 191(14), p. 23.

George, J. F., Derrick, D., Harrison, A., Marett, K., & Thatcher, J. B [Jason B.] (2016). The Dark Internet: Without Darkness There is No Light. In *Americas Conference on Information Systems,* San Diego, California, USA.

Gerlach, J. P., & Cenfetelli, R. T. (2020). Constant Checking Is Not Addiction: A Grounded Theory of IT-Mediated State-Tracking. *MIS Quarterly, 44*(4), 1705–1732. https://doi.org/10.25300/MISQ/2020/15685

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems, 12*(9), 606–631.

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

Goos, H. (2018, October 6). Fest im Griff. *DER SPIEGEL*(41), pp. 46–54.

Graf, V [Valerie], Graf, V [Vanessa], Baumbach, S., & Schafranek, M. (2018). Individuals' Sustainable Behaviour along the Lifecycle of IT. In *European Conference on Information Systems*, Portsmouth, UK.

Green, A. W., Woszczynski, A. B., Dodson, K., & Easton, P. (2020). Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems. *Communications of the Association for Information Systems*(46), Article 8, 187–208. https://doi.org/10.17705/1CAIS.04608

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642.

Gu, R., & Li, M. X. (2020). Investigating the Psychological Mechanism of Individuals' Health Misinformation Dissemination on Social Media. In *International Conference on Information Systems*, Virtual Conference.

Guggenmos, F., Hofmann, P., & Fridgen, G. (2019). How ill is your IT Portfolio? - Measuring Criticality in IT Portfolios Using Epidemiology. In *International Conference on Information Systems*, Munich, Germany.

Hay, B., & LaFountain, S. (2017). CyberWarfare: Offensive and Defensive Software Technologies (Introduction). In *Hawaii International Conference on System Sciences*, Waikoloa Village, Hawaii, USA. http://aisel.aisnet.org/hicss-50/

Heid, M. (2017, November 6). We Need to Talk About Kids and Smartphones. *TIME*, 190(19), pp. 42–46.

Heinssen, R. K., Glass, C. R., & Knight, L. A. (1987). Assessing computer anxiety: Development and validation of the Computer Anxiety Rating Scale. *Computers in Human Behavior*, *3*(1), 49–59. https://doi.org/10.1016/0747-5632(87)90010-0

Hennigan, W. J. (2018, January 29). Panic Station: Hawaii's False Alert Exposes Weak U.S. Alert Systems. *TIME*, 191(3), pp. 7–9.

Hennigan, W. J. (2019, April 1). Second-Hand Safety. *TIME*, 193(12), pp. 42–45.

Hincks, J. (2019, December 2). Iran Goes Dark As Riots Surge Over a Gas-Price Hike. *TIME*, 194(24/25), p. 13.

Hitt, L. M., & Brynjolfsson, E. (1996). Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value. *MIS Quarterly*, *20*(2), 121–142.

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275–298.

Hsieh, J. J. P.-A., Rai, A., & Keil, M. (2008). Understanding Digital Inequality: Comparing Continued Use Behavioral Models of the Socio-Economically Advantaged and Disadvantaged. *MIS Quarterly*, *32*(1), 97–126. https://doi.org/10.2307/25148830

Huang, Y., Kuo, F.-Y. B., & Lin, C. s. (2017). Behavior Regulation in Social Media: A Neuroscientific Investigation. In *International Conference on Information Systems,* Seoul, South Korea.

IEEE. (2020). *IEEE POLICIES*. https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/whatis/ieee-policies.pdf

Ilany-Tzur, N., Zalmanson, L [Lior], & Oestreicher-Singer, G. (2016). The Dark Side of User Participation - The Effect of Calls to Action on Trust and Information Revelation. In *International Conference on Information Systems,* Dublin, Ireland.

Isaacson, W. (2019, January 14). How America Loses Its Edge. *TIME*, 193(1), pp. 17–19.

Islam, M. S., Sarkar, T., Khan, S. H., Mostofa Kamal, A.-H., Hasan, S. M. M., Kabir, A., Yeasmin, D., Islam, M. A., Amin Chowdhury, K. I., Anwar, K. S., Chughtai, A. A., & Seale, H. (2020). Covid-19-Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis. *The American Journal of Tropical Medicine and Hygiene*, *103*(4), 1621–1629. https://doi.org/10.4269/ajtmh.20-0812

Jiang, H. (2019). Understanding the Impact of Cyberloafing-Related Internet Monitoring on Employee Job Performance: A Field Experiment. In *International Conference on Information Systems,* Munich, Germany.

Jung, A. (2020, February 8). „Sklaven der Prozesse“. *DER SPIEGEL*(7), p. 67.

Jung, A., Nezik, A.-K., Rosenbach, M., & Schulz, T. (2018, November 10). Angstträume. *DER SPIEGEL*(46), pp. 66–71.

Jüttner, J. (2020, December 5). Der Feind in meinem Chat. *DER SPIEGEL*(50), pp. 52–53.

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. https://doi.org/10.1016/j.is.2010.11.003

Kyung, N., Lim, S., & Lee, B. (2017). A Depressing Internet Tale: Empirical Analysis of the Internet's Impact on Suicide. In *International Conference on Information Systems,* Seoul, South Korea.

Lanchester, J. (2019, February 4). Leveling the Playing Field. *TIME,* 193(4/5), pp. 75–77.

Laurenz, N. (2018). *Schüler montieren Gesichter ihrer Lehrer in Pornos*. http://www.spiegel.de/lebenundlernen/schule/heppenheim-schueler-montieren-gesichter-ihrer-lehrer-in-pornos-a-1240794.html

Ledder, S. (2013). Computerspiele. In A. Grunwald (Ed.), *Handbuch Technikethik* (pp. 258–263). Verlag J. B. Metzler.

Lee, G., Shao, B. B. M., & Vinze, A. (2018). The Role of ICT as a Double-Edged Sword in Fostering Societal Transformations. *Journal of the Association for Information Systems*, *19*(3), 209–246. https://doi.org/10.17705/1jais.00490

Lee, J. K. (2015). Research Framework for AIS Grand Vision of the Bright ICT Initiative. *MIS Quarterly*, *39*(2), iii–xii.

Lee, J., Wang, J., Cliff, G., & Rao, H. R. (2016). Management of Digital Evidence: Police Judgment about Ethical Use of Body Worn Camera. In *International Conference on Information Systems,* Dublin, Ireland.

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Business & Information Systems Engineering*, *59*(4), 301–308. https://doi.org/10.1007/s12599-017-0484-2

Leidner, D. E. (2019). No risk, no reward. *Journal of Information Technology*, *34*(1), 84–86. https://doi.org/10.1177/0268396218815565

Leidner, D. E., & Tona, O. (2021). The CARE Theory of Dignity Amid Personal Data Digitalization. *MIS Quarterly*, *45*(1), 343–370. https://doi.org/10.25300/MISQ/2021/15941

Liel, Y., & Zalmanson, L [Liar] (2020). What If an AI Told You That 2 + 2 Is 5? Conformity to Algorithmic Recommendations. In *International Conference on Information Systems,* Virtual Conference.

Lim, V. K., Teo, T. S., & Nishant, R. (2017). Cyber Incivility at the Workplace. In *International Conference on Information Systems,* Seoul, South Korea.

Liu, Z., Wang, X., Min, Q., & Li, W. (2019). The effect of role conflict on self-disclosure in social network sites: An integrated perspective of boundary regulation and dual process model. *Information Systems Journal*, *29*(2), 279–316. https://doi.org/10.1111/isj.12195

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273. https://doi.org/10.1111/isj.12063

M Y, M., Li, B., & Foutz, Y. N. Z. (2019). Geo-Targeting, Privacy, and the Rise of Consumer Location Trajectories. In *International Conference on Information Systems*, Munich, Germany.

Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. *Information Systems Journal*, *25*(3), 275–308. https://doi.org/10.1111/isj.12068

Majchrzak, A., Markus, M. L., & Wareham, J. (2016). Designing for Digital Transformation: Lessons for Information Systems Research from the Study of ICT and Societal Challenges. *MIS Quarterly*, *40*(2), 267–277.

Manzei, A. (2018). Sind Standards objektiv und neutral? In S. Klinke & M. Kadmon (Eds.), *Ärztliche Tätigkeit im 21. Jahrhundert - Profession oder Dienstleistung* (pp. 207–229). Springer.

Matook, S., Cummings, J., & Bala, H. (2015). Are You Feeling Lonely? The Impact of Relationship Characteristics and Online Social Network Features on Loneliness. *Journal of Management Information Systems*, *31*(4), 278–310. https://doi.org/10.1080/07421222.2014.1001282

McCarthy, S., Rowan, W., Lynch, L., & Fitzgerald, C. (2020). Blended Stakeholder Participation for Responsible Information Systems Research. *Communications of the Association for Information Systems*(47), Article 33, 716–742.

McFall, L. (2019). Personalizing solidarity? The role of self-tracking in health insurance pricing. *Economy and Society*, *48*(1), 52–76. https://doi.org/10.1080/03085147.2019.1570707

McNamee, R. (2019, January 28). How to Fix Social Media Before It's Too Late. An Early Investor on How Facebook Lost Its Way. *TIME*, 193(3), pp. 22–28.

McNamee, R. (2020, June 15). Facebook cannot fix itself. *TIME*, 195(22), pp. 20–21.

Meijer, A., & Wessels, M. (2019). Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration*, *42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664

Meyer, J. (2019, May 27). The New Saudi War on Dissent. *TIME*, 193(20), pp. 26–31.

Mikhaeil, C. A., & Baskerville, R. (2017). An Identity Driven Escalation of Commitment to Negative Spillovers. In *International Conference on Information Systems*, Seoul, South Korea.

Mingels, G. (2018, December 22). Alles im Fluss. *DER SPIEGEL*(52), pp. 68–70.

Mingels, G. (2019, July 13). Digitale Bürgerwehr. *DER SPIEGEL*(29), p. 75.

Moya, J.-F. de, & Pallud, J. (2020). From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices. *Information Systems Journal*, *30*(6), 940–976. https://doi.org/10.1111/isj.12284

Müller, M. U. (2018, November 10). Contergan bei Ebay(46), pp. 78–79.

Müller, M., Neumann, J., Gutt, D., & Kundisch, D. (2020). Toss a Coin to your Host - How Guests End up Paying for the Cost of Regulatory Policies. In *International Conference on Information Systems*, Virtual Conference.

Nasralah, T., Ahmed, A., Wahbeh, A., Alyami, H., & Ali, A. (2018). Negative Effects of Online Health Communities on User's Health: The Case of Online Health Forums. In *Midwest Association for Information Systems Conference*, Saint Louis, Missouri, USA.

Nelson, D. L., & Kletke, M. G. (1990). Individual adjustment during technological innovation: A research framework. *Behaviour & Information Technology*, *9*(4), 257–271. https://doi.org/10.1080/01449299008924242

Neumeier, A., & Wolf, T. (2017). Getting a Grip on IT Project Complexity - Concluding to Underlying Causes. In *International Conference on Information Systems*, Seoul, South Korea.

Ng, E., Tan, B., & Meng, T. (2019). The Dark Side of the Sharing Economy: The Negative Implications of Ridesharing for a Traditional Taxi Business. In *International Conference on Information Systems*, Munich, Germany.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336–359. https://doi.org/10.1057/ejis.2012.26

NPR. (2017). *Amazon And The $150 Million Typo*. https://www.npr.org/sections/thetwo-way/2017/03/03/518322734/amazon-and-the-150-million-typo

Oehmke, P. (2018, December 8). Tod durch Algorithmus. *DER SPIEGEL*(50), pp. 48–52.

Pariser, E. (2019, January 28). Restoring Dignity to Technology How to Design Tools to Set Right What Has Gone Wrong Online. *TIME,* 193(3), pp. 34–35.

Perez, C. C. (2020, February 3). Closing the Gender Data Gap. *TIME,* 195(3/4), pp. 80–81.

Perrigo, B. (2018, October 1). Whistle-Blower Christopher Wylie on Life After Taking Down Cambridge Analytica. *TIME,* 192(13), pp. 12–13.

Pirkkalainen, H., & Salo, M. (2016). Two Decades of the Dark Side in the Information Systems Basket: Suggesting Five Areas for Future Research. In *European Conference on Information Systems,* Istanbul, Turkey.

Polites, G. L., Serrano, C., Thatcher, J. B [Jason Bennett], & Matthews, K. (2018). Understanding social networking site (SNS) identity from a dual systems perspective: an investigation of the dark side of SNS use. *European Journal of Information Systems*, *27*(5), 600–621. https://doi.org/10.1080/0960085X.2018.1457194

Precht, R. D. (2018, November 24). Maschinen ohne Moral. *DER SPIEGEL*(48), pp. 78–79.

Rainer, A. (2019, November 9). Medienwächter gehen gegen Pornoseiten vor. *DER SPIEGEL*(46), p. 68.

Raphael, D. D. (2007). *The impartial spectator: Adam Smith's moral philosophy*. Oxford University Press. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10220188

Ratnesar, R. (2019, September 16). Trust us. *TIME,* 194(10), pp. 38–42.

Reilly, K. (2020, April 6). The Online Learning Divide. *TIME,* 195(12/13), pp. 38–41.

Ressa, M. (2019, January 28). Facebook Let My Government Target Me but the Social-Media Giant Could Yet Fulfill Its Original Promise. *TIME,* 193(3), pp. 30–31.

Riek, M., Abramova, S., & Böhme, R. (2017). Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior. In *International Conference on Information Systems,* Seoul, South Korea.

Rockmann, R., & Gewald, H. (2017). Is IT What You Make out of IT? On Affordances, Goals, and Positive and Negative Consequences in Activity Tracking. In *International Conference on Information Systems,* Seoul, South Korea.

Rosemann, M., & Vessey, I. (2008). Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks. *MIS Quarterly*, *32*(1), 1–22.

Rosenbach, M. (2018, December 22). „Regelrechte Datenhalden“. *DER SPIEGEL*(52), pp. 66–67.

Rosenbach, M. (2019, June 15). Dringender Hilferuf. *DER SPIEGEL*(25), p. 73.

Sarker, S [Suprateek], Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and its Continued Relevance. *MIS Quarterly*, *43*(3), 695–719. https://doi.org/10.25300/MISQ/2019/13747

Schirrmacher, N.-B., Ondrus, J., & Tan, F. T. C. (2018). Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack. In *Pacific Asia Conference on Information Systems,* Yokohama, Japan.

Schmoll, R., & Bader, V. (2019). Who or what screens which one of me? The differential effects of algorithmic social media screening on applicants' job pursuit intention. In *International Conference on Information Systems,* Munich, Germany.

Schuetz, S., & 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), 460–482. https://doi.org/10.17705/1jais.00608

Scott, S. V., & Barrett, M. I. (2005). Strategic risk positioning as sensemaking in crisis: the adoption of electronic trading at the London international financial futures and options exchange. *The Journal of Strategic Information Systems*, *14*(1), 45–68. https://doi.org/10.1016/j.jsis.2005.01.001

Sedera, D. D., Lokuge, S., & Chandrasekara, D. (2017). Human Degradation with the use of Social Media: A Theological Perspective. In *International Conference on Information Systems*, Seoul, South Korea.

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, *62*(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Semuels, A. (2019, June 3). The Coming Mountain of E-Waste. *TIME,* 193(21/22), pp. 48–49.

Semuels, A. (2020a, June 1). As the Gig Economy Grows, its Workers' Paychecks Shrink. *TIME,* 195(20/21), pp. 12–13.

Semuels, A. (2020b, August 17). Fewer Jobs, More Machines. *TIME,* 196(7/8), pp. 64–71.

Shim, J. P., French, A. M., Guo, C., & Jablonski, J. (2015). Big Data and Analytics: Issues, Solutions, and ROI. *Communications of the Association for Information Systems*(37), Article 39, 797–810. https://doi.org/10.17705/1CAIS.03739

Shim, J. P., Sharda, R., French, A. M., Syler, R. A., & Patten, K. P. (2020). The Internet of Things: Multi-faceted Research Perspectives. *Communications of the Association for Information Systems*(46), Article 21, 511–536. https://doi.org/10.17705/1CAIS.04621

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Son, J.-Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, *32*(3), 503–529.

Soror, A. A., Hammer, B. I., Steelman, Z. R., Davis, F. D., & Limayem, M. M. (2015). Good habits gone bad: Explaining negative consequences associated with the use of mobile phones from a dual-systems perspective. *Information Systems Journal*, *25*(4), 403–427. https://doi.org/10.1111/isj.12065

Srivastava, S. C., Chandra, S., & Shirish, A. (2015). Technostress creators and job outcomes: theorising the moderating influence of personality traits. *Information Systems Journal*, *25*(4), 355–401. https://doi.org/10.1111/isj.12067

Stavridis, A. J. (2019, October 7). America Needs a New Strategic Triad to Face the 21st Century. *TIME,* 194(14), p. 19.

Steinmetz, K. (2017, December 25-2018, January 1). Generation Z Finds the Upside to Growing Up Amid Total Disruption. *TIME,* 190(27/28), pp. 66–67.

Steinmetz, K. (2018a, April 2). A San Francisco Museum Tackles Art's Instagram Dilemma. *TIME,* 191(12), p. 12.

Steinmetz, K. (2018b, April 23). Can Congress Rein in Big Tech. *TIME,* 191(15), pp. 46–47.

Steinmetz, K. (2018c, October 8). Popularity on Social Media? Not cool. *TIME,* 192(14), p. 25.

Steinmetz, K. (2019, July 22). Instagram's Challenge. *TIME,* 194(3), pp. 46–51.

Stengel, R. (2019, October 7). The Global War on Truth. *TIME*, 194(14), pp. 36–39.

Tams, S., Ahuja, M., Thatcher, J., & Grover, V. (2020). Worker stress in the age of mobile technology: The combined effects of perceived interruption overload and worker control. *The Journal of Strategic Information Systems*, *29*(1), 1–17. https://doi.org/10.1016/j.jsis.2020.101595

Tams, S., Thatcher, J. B [Jason B.], & Grover, V. (2018). Concentration, Competence, Confidence, and Capture: An Experimental Study of Age, Interruption-based Technostress, and Task Performance. *Journal of the Association for Information Systems*, *19*(9), 857–908. https://doi.org/10.17705/1jais.00511

Tanriverdi, H., & Chen, H. (2018). Government's Digital Surveillance and Citizens' Self-Censorship of Technology Use. In *International Conference on Information Systems*, San Francisco, California, USA.

Tarafdar, M., Gupta, A [Ashish], & Turel, O. (2015a). Editorial: Introduction to the special issue on 'dark side of information technology use' - part two. *Information Systems Journal*, *25*(4), 315–317. https://doi.org/10.1111/isj.12076

Tarafdar, M., Gupta, A [Ashish], & Turel, O. (2015b). Editorial: Special issue on 'dark side of information technology use': an introduction and a framework for research. *Information Systems Journal*, *25*(3), 161–170. https://doi.org/10.1111/isj.12070

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems*, *24*(1), 301–328.

The Telegraph. (2016). *Microsoft deletes 'teen girl' AI after it became a Hitler-loving sex robot within 24 hours*. https://www.telegraph.co.uk/technology/2016/03/24/microsofts-teen-girl-ai-turns-into-a-hitler-loving-sex-robot-wit/

Thapa, D., & Sein, M. K. (2018). Trajectory of Affordances: Insights from a case of telemedicine in Nepal. *Information Systems Journal*, *28*(5), 796–817. https://doi.org/10.1111/isj.12160

Thatcher, J. B [Jason Bennett], & Perrewé, P. L. (2002). An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy. *MIS Quarterly*, *26*(4), 391–396.

Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems*, *16*(2), 214–232. https://doi.org/10.1016/j.jsis.2007.05.006

Thimm, K. (2019, June 15). „Unwissen macht uns manipulierbar". *DER SPIEGEL*(25), pp. 102–104.

Transparency International. (2021). *Regulate Online Political Ads for Greater Political Integrity*. https://www.transparency.org/en/news/regulate-online-political-ads-for-greater-political-integrity

Turel, O. (2019). Potential ‘dark sides’ of leisure technology use in youth. *Communications of the ACM*, *62*(3), 24–27. https://doi.org/10.1145/3306615

Turel, O., Matt, C., Trenz, M., Cheung, C. M., D’Arcy, J., Qahri-Saremi, H., & Tarafdar, M. (2019). Panel Report: The Dark Side of the Digitization of the Individual. *Internet Research*, *29*(2), 274–288. https://doi.org/10.1108/INTR-04-2019-541

Turel, O., Qahri-Saremi, H., & Vaghefi, I. (2021). Special Issue: Dark Sides of Digitalization. *International Journal of Electronic Commerce*, *25*(2), 127–135. https://www.ijec-web.org/past-issues/volume-25-number-2-2021/special-issue-dark-sides-of-digitalization/

Vesoulis, A., & Dockterman, E. (2020, July 20). Pandemic Schemes. *TIME*, 196(3/4), 84-91.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Vick, K. (2019, December 23). Guardians. *TIME*, 194(27/28), pp. 24–25.

Vieira da Cunha, J., Carugati, A., & Leclercq-Vandelannoitte, A. (2015). The dark side of computer-mediated control. *Information Systems Journal*, *25*(4), 319–354. https://doi.org/10.1111/isj.12066

Wallace, S. A., Green, K. Y., Johnson, C. M., Cooper, J. T., & Gilstrap, C. M. (2020). An Extended TOE Framework for Cybersecurity-adoption Decisions. *Communications of the Association for Information Systems*(47), Article 16, 338–363.

Walsham, G. (2012). Are We Making a Better World with Icts? Reflections on a Future Agenda for the IS Field. *Journal of Information Technology*, *27*(2), 87–93.

Wang, C., & Lee, M. K. O. (2020). Why We Cannot Resist Our Smartphones: Investigating Compulsive Use of Mobile SNS from a Stimulus-Response-Reinforcement Perspective. *Journal of the Association for Information Systems*, *21*(1), 175–200. https://doi.org/10.17705/1jais.00596

Wang, J., Xiao, N., & Rao, H. R. (2015). Research Note—An Exploration of Risk Characteristics of Information Security Threats and Related Public Information Search Behavior. *Information Systems Research*, *26*(3), 619–633. https://doi.org/10.1287/isre.2015.0581

Watson, H. J., & Nations, C. (2019). Addressing the Growing Need for Algorithmic Transparency. *Communications of the Association for Information Systems*(45), Article 26, 488–510. https://doi.org/10.17705/1CAIS.04526

Weber, R. (2012). Evaluating and Developing Theories in the Information Systems Discipline. *Journal of the Association for Information Systems*, *13*(1), 1–30. https://doi.org/10.17705/1jais.00284

Weinert, C., Laumer, S., Maier, C., & Weitzel, T. (2016). Is Information Technology Solely to Blame? The Influence of Work-home Conflict Dimensions on Work Exhaustion. In *International Conference on Information Systems,* Dublin, Ireland.

Wiegard, R., Guhr, N., Krylow, S., & Breitner, M. H. (2019). Analysis of wearable technologies' usage for pay-as-you-live tariffs: recommendations for insurance companies. *Zeitschrift Für Die Gesamte Versicherungswissenschaft*, *108*(1), 63–88. https://doi.org/10.1007/s12297-019-00431-2

Wijnhoven, F., & Pieper, A. T. (2018). Review spam criteria for enhancing a review spam detector. In *International Conference on Information Systems,* San Francisco, California, USA.

Wunderlich, P., Veit, D. J., & Sarker, S [Saonee] (2019). Adoption of Sustainable Technologies: A Mixed-Methods Study of German Households. *MIS Quarterly*, *43*(2), 673–691. https://doi.org/10.25300/MISQ/2019/12112

Wüst, C. (2018, November 3). Gut im Wischen. *DER SPIEGEL*(45), p. 112.

Zorthian, J. (2017, November 6). Should Tech Companies Have to Disclose Who Pays for Online Election Ads. *TIME*, 190(19), p. 19.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. Basic Books.

3 Antecedents of digitalization's negative consequences

3.1 Fear of algorithms: a synopsis of concerns about automated decision-making

Abstract: Automated decision-making (ADM) is making its impact in all areas of modern life. Decisions previously made by humans are increasingly supported or replaced by algorithms. Many people harbor reservations about ADM, and yet, there is no exhaustive study that structures these concerns. The objective of our research is to outline a comprehensive framework of concerns about ADM. Based on a structured review of the literature and a qualitative content analysis of semi-structured interviews, we identified ten major concerns regarding the underlying technology, data, or the decision itself. Furthermore, we identified 14 concerns about the potential consequences of using ADM. Our framework is intended to guide future research on concerns about ADM, while also serving as a touchstone for anyone developing ADM-related offers and services that account for the potential reservations of the intended user group.

Keywords: Algorithm, automated decision-making, algorithmic decision-making, concerns

Authors: Sarah Bayer, Fabian Schmied, Daniela Waldmann

Status: This article is a working paper.

3.1.1 Introduction

Algorithms are "a sequence of computational steps that transform inputs into outputs, and range from simple if-then statements to artificial intelligence (AI), machine learning, and neural networks" (Martin, 2019). Nowadays, algorithms are involved in all areas of life, for instance by producing news articles based on structured data, by supporting recruitment processes, by detecting fraud in sports betting, by deciding which physicians see which patient, and by defining dynamic prices in many application areas, such as e-commerce (e.g., Amazon), tourism (e.g., Airbnb), and transportation (e.g., Uber) (Diakopoulos, 2016; Martin, 2019; van den Broek et al., 2019). In some of these areas, we see "complex and networked algorithms that are beyond proper human understanding and control" (Gimpel & Schmied, 2019, p. 8). This comes with certain adverse, unexpected, and unintended effects (Gimpel & Schmied, 2019; Majchrzak et al., 2016), and these effects – positive as well as negative – are extending their reach into all aspects of modern life (Diakopoulos, 2016). Decision-making processes previously made by humans are increasingly supported (augmented by technology) or even replaced by algorithms (fully automated) (Martin, 2019; Wachter et al., 2017).

In the future, algorithms are expected to gain even more influence due to an ever-increasing degree of automation in decision-making processes as well as the expansion of application areas of ADM. This is affecting individuals, organizations, and society at large. On the one hand, organizations and public authorities may benefit from the accuracy, scale, speed, simplicity, and cost-efficiency of automated decisions (Diakopoulos, 2016). There are those who argue that algorithmic decisions foster objectivity and fairness (van den Broek et al., 2019). Others predict that algorithms may have significant negative consequences for individuals affected by automated decisions. Two prime examples are when potentially biased algorithms support policing (known as predictive policing) or assist judicial decision-making in court (Angwin et al., 2016; Binns et al., 2018; Corbett-Davies et al., 2016; Dressel & Farid, 2018; Martin, 2019). Algorithmic decisions are further criticized for facilitating other ethical violations such as sexism or privacy invasions (van den Broek et al., 2019). In this paper, we focus on reservations that individuals harbor about ADM.

Prior literature has already investigated potential risks and side effects of ADM for individuals, such as discrimination, lack of data protection, unfairness, or wider ethical issues. Most research articles discussed these issues in highly specific (and primarily future-oriented) use cases. However, there is no comprehensive overview of the chief concerns held by individuals when dealing with ADM, which is a necessary foundation to improve ADM adoption. What

is missing, therefore, is a synopsis of these concerns about ADM derived from literature (focused mainly on specific single use cases) and complemented with a survey of multiple ADM cases. To fill this gap in the research and to provide a starting point for further, detailed research about these concerns, we aim to answer the following question:

Which concerns do individuals have about the use of automated decision-making?

The overview we have generated in reply to this question may serve as a foundation upon which others can develop responsible and transparent ADM-related offers and services with full regard for the fears and reservations of those affected (Diakopoulos, 2016). Furthermore, we intend to summarize as well as extend existing research to offer a basis for future research.

The paper is structured as follows: The following section provides the theoretical background for algorithmic decision-making and concerns. Then, we describe the methodological approach of our structured literature search and the qualitative content analysis of our semi-structured interviews, followed by the presentation of results. After the result section, or discussion includes practical and theoretical implications, and an outlook towards future research, followed from the conclusion.

3.1.2 Theoretical background

To understand concerns about ADM one must first dive deeper into the negative aspects of IT. Although there is an apparent pro-IT bias in information systems (IS) research, there is also research on the "dark side of IT." The *Information Systems Journal* published two consecutive special issues on the dark side of information technology use (Tarafdar et al., 2015a, 2015b). These special issues comprise articles that focus on one negative aspect of IT use at a time, such as technostress, IT interruptions, computer abuse, IT-mediated control, or unauthorized file sharing (Tarafdar et al., 2015a, 2015b). Further, Pirkkalainen and Salo (2016) review 37 articles in the AIS Senior Scholars' Basket of Journals and detect four types of dark side phenomena: information overload, IT addiction, and IT anxiety. Kim et al. (2011) provide a taxonomy of the dark side of the internet and focus on attacks, costs, and appropriate responses. They identify technology-centric dark side effects like spam, malware, hacking, and digital property rights violations. Additionally, they identify non-technology-centric dark side effects such as online theft, cyberbullying, and the aiding and abetting of crime. Gimpel and Schmied (2019) aim to provide a broad overview of dark side phenomena by developing a taxonomy of the most severe risks and side effects of digitalization, such as adverse exchange, adverse economic shifts, impairment of health, undesirable behavioral adaptation, or losing control over algorithms. Some of those dark sides of IT also relate to the use of algorithms.

ADM takes place when a result, e.g., a recommendation or a purchase, is achieved without human intervention (Allen & Masters, 2019). Thus, ADM is either supported by modern information and communication technologies (ICTs) or the decision is entirely made by the application of specific algorithms (Allen & Masters, 2019). This is why ADM is also called algorithmic decision-making. Another way to achieve ADM, however, may be to use complex artificial intelligence (AI) supported and trained by machine learning (ML) (Allen & Masters, 2019). Within AI, the different analytical techniques, such as descriptive, predictive, or prescriptive analytics, facilitate ever greater intelligence and business efficiency. Whereas descriptive and predictive analytics require a human manager to interpret the results, prescriptive analytics enables ADM (Vahn, 2014). In other words, it goes beyond predicting future results by anticipating what will happen, when it will happen, and why it will happen. What is more, it gives recommendations that benefit from those predictions (Kumar, 2015; Shankararaman & Gottipati, 2015). Consequently, prescriptive analytics answers the question "How can we make it happen?" (Shankararaman & Gottipati, 2015).

The impact of ADM on the lives of individuals triggers certain concerns about ADM. According to Lowry et al. (2011), we define concerns in use cases of ADM as the extent to which a person worries about possible risks and consequences associated with ADM use. The existing literature has already discussed the concerns some individuals have about ADM, e.g., discrimination (Strobel, 2019), or data privacy (Newell & Marabelli, 2015). It has also discussed factors that inhibit ADM adoption, e.g., control (Dietvorst et al., 2018) or trust (Castelo et al., 2019). It has further discussed a variety of use cases for ADM, e.g., automated travel planning (Cho & Han, 2019), autonomous driving (Dietrich & Weisswange, 2019), or automated purchases (Ringe et al., 2019), and the literature has also already discussed the implementation of ADM in business use cases (Dwivedi et al., 2021). However, these discussions have typically been grouped around single concerns, and most of the studies have focused on a specific context. A comprehensive overview of concerns that might inhibit ADM adoption does not yet exist. In this paper, we argue for the need of a better understanding of how individuals perceive the impact of using ADM in daily life. This is necessary if we are to gain a deeper insight into the relationship between the perception of ADM's use, the perception of the consequences of ADM's use, and actual behavior, because organizations need to know which consequences individuals fear and how to address those negative perceptions (Karwatzki et al., 2017).

Further areas of academic research, such as data privacy, has indicated that individual concerns can be manifold (Hauff et al., 2015; Smith et al., 1996). Smith et al. (1996) have identified seven major data privacy concerns of customers (including data collection, secondary use, or improper access). Hauff et al. (2015) have investigated how perceived privacy-invasive data collection and usage can affect individuals. Their research has shown that, for some individuals, there are concerns at different levels. Meanwhile, Karwatzki et al. (2017) have developed a categorization of how individuals perceive the consequences of access to their personal information. This categorization spans seven types of consequences: psychological, social, career-related, physical, resource-related, prosecution-related, and freedom-related. Nevertheless, this research has merely discussed data privacy concerns (e.g., regarding unauthorized access to individuals' information), which we believe to be only one type of concern about ADM. As such, the existing research does not provide a comprehensive overview of potential concerns.

3.1.3 Research methodology and approach

To answer our research question, we take a two-step approach by way of a structured literature search and a qualitative content analysis of semi-structured interviews. First, we reviewed the existing (IS) literature to identify concerns about ADM. In so doing, we also identified current use cases for ADM, which served as a basis for the semi-structured interviews conducted in the second step. We used a search string, combining "automated decision" with the most common synonym used in the literature ("algorithmic decision"), as well as the term "prescriptive analytics," which is used primarily in the research area of statistics. Furthermore, we linked those expressions with "concern" and synonyms for concern commonly used in the literature, which yielded the following search terms: *("automated decision" OR "algorithmic decision" OR "prescriptive analytics") AND ("concern" OR "risk" OR "attitude" OR "danger" OR "aversion")*. As advised by Webster and Watson (2002), we did not restrict our literature search to databases with a focus on the IS discipline (covered by the databases ACM Digital Library and AIS Electronic Library). Instead, we expanded our search to general databases so as to cover a wide range of different research areas with our main focus directed at the domain of electronic commerce and computer science, engineering, law, marketing, logistics, and beyond (covered by the databases Science direct, EBSCOhost, JSTOR Library, SpringerLink, ProQuest). Since ADM is frequently embedded in highly topical discussions about AI, we included news from associations and academic journals. The structured literature search resulted in 175 articles. After the initial screening of titles and abstracts, the full texts of the remaining 30 articles were examined, whereupon 18 articles were classified as relevant. An

article was considered relevant if the following two conditions were met: (1) the article dealt with ADM in general or in a specific use case and (2) the article named or explained concerns or adverse effects of ADM for a specific use case or in general terms. With regard to those 18 articles, we highlighted words or phrases expressing concerns about ADM (e.g., "discrimination" (Strobel, 2019), "computer implementation may be incorrect" (Brauneis & Goodman, 2018)) and use cases for ADM (e.g., "recommender systems" (Borràs et al., 2014), "loan application" (Strobel, 2019)).

This also proved to be highly useful in preparing the semi-structured interviews, which we then conducted to identify further concerns about ADM. We chose interviewees with diverse backgrounds to cover a broad cross-section of the population in terms of age and gender as well as educational and professional backgrounds. We met the interviewees in person or spoke to them on video calls, and in each case we recorded the interview. In total, we conducted 13 interviews, as shown in Table 3.1-1.

ID	Age	Gender	Highest educational level	Profession / Occupation
1	25	male	University degree	Student
2	60	female	High school diploma	Secretary
3	28	male	University degree	Doctoral candidate
4	34	male	Secondary school	IT administrator
5	33	female	University degree	Doctoral candidate
6	29	male	University degree	Technical employee
7	26	female	Secondary school	Nurse
8	28	male	University degree	Student
9	27	male	University degree	Doctoral candidate
10	57	male	Secondary school	Civil servant
11	57	female	University degree	Civil servant
12	22	male	High school diploma	Student
13	28	female	University degree	Doctoral candidate

Table 3.1-1: Demographic overview of interviewees

After 11 interviews, the 12th did not reveal further insights of any relevance. We conducted a 13th interview anyway, but this, too, revealed nothing new. Reassured that we had reached saturation point, we determined that we had gathered enough data via interviews. The duration of each ranged from 15 to 45 minutes and comprised four steps: (1) present a definition of ADM ("decisions that are made or at least supported by algorithms") and ensure a common understanding of ADM, (2) ask open questions about prior experiences with ADM and any associated concerns, (3) present five use cases to discuss concerns with regard to each use case, (4) present and discuss the results of our literature search.

We presented five ADM use cases (automated lending (Brauneis & Goodman, 2018), intelligent travel bots (Cho & Han, 2019), automated evaluation of applicants (Faliagka et al., 2012), autonomous driving (Dietrich & Weisswange, 2019), and automated purchases (Ringe et al., 2019)). We chose those use cases because they are current in both mainstream media and academic research, and because they cover a broad spectrum of modern life, ranging from consumption, travel and locomotion, to the professional environment. Furthermore, we attached importance to the fact that the cases represent current progress as well as future scenarios. We provided the interviewees with images and a short description of these use cases. We transcribed all interviews verbatim in order to conduct a qualitative content analysis in line with the eight steps proposed by Schreier (2013). These eight steps bring together the best of various approaches to a thorough qualitative content analysis (Boyatzis, 1988; Hsie & Shannon, 2005; Mayring, 2010; Rustemeyer, 1992). We used the software MAXQDA to code the interviews, and each step of this methodology is outlined in detail below.

(1) Deciding on a research question: Our research question was defined ahead of the interviews (cf. Section 1).

(2) Selecting material: We conducted semi-structured interviews, each of which was fully transcribed. As our interview sample includes two different types of stakeholders (students and doctoral candidates involved in ADM research as well as individuals without professional experience in ADM), we chose two interviews from each group in order to set up the coding frame.

(3) Building a coding frame: To build main categories ("structuring") and generate the subcategories ("generating"), we combined a concept- and data-driven approach. Since our ultimate aim is to analyze concerns about ADM, the main category of the coding frame is *concerns about ADM*. In the following, where we only use one main category, we also refer to categories on the second level as main categories, while categories on the third level are called sub-categories. The results of our literature research were used to generate certain main- and sub-categories in a concept-driven way (e.g., technology, data and societal as main categories, as opposed to privacy incidents, discrimination and job loss as sub-categories). Furthermore, we adopted the strategy of subsumption as proposed by Mayring (2010) for data-driven categories: We reviewed the interview transcripts until we encountered a relevant aspect, then checked whether this aspect is already covered by a category and either attributed the aspect to the existing category or created a new category (e.g., organizational for main categories, as opposed to lack of enjoyment and lack of spontaneity for subcategories).

As advised by Schreier (2013), our coding frame meets the requirements of unidimensionality (our main categories are unidimensional), mutual exclusiveness (sub-categories within one main category are mutually exclusive), and exhaustiveness (all relevant aspects of the material are covered by a category). After the definition of the coding frame, we defined each category (Schreier, 2013). Subsequently, we examined the bigger picture of the coding frame, then merged and split a few categories, and refined our definitions.

(4) Segmentation: As suggested by Schreier (2013), we divided our material into segments. Since the use cases of ADM mentioned in the interviews are suitable to specify the start and the end of a unit, we chose the use cases as a thematic criterion for segmentation.

(5) Trial coding: In the next step, we applied the coding frame to further interview transcripts. We split the material among the researchers and each researcher coded the material twice within two weeks.

(6) Evaluating and modifying the coding frame: We evaluated consistency and validity. Less than 10% of codes were assigned to different categories in two coding rounds. We discussed the respective categories and revised each definition. As we did not have any leftover categories but managed to assign each code to a proper category, we determined our coding frame to be valid.

(7) Main analysis: We coded the rest of the interviews, and due to the high validity and consistency, there was no need to double-code the rest of the material (Schreier, 2013).

(8) Presenting and interpreting the findings: Below, we present our framework in visual terms alongside explanations of the categories of concerns in Table 3.1-3 and Table 3.1-4. Additionally, we explain each category, illustrated by quotes in the following section.

3.1.4 Results

With the help of our structured literature search and semi-structured interviews, we identified 24 concerns. 13 concerns resulted from the structured literature search, 22 from the semi-structured interviews, which is to say that eleven emerged from both sources. Figure 3.1-1 structures the 24 concerns. We divided the framework into two categories of concerns: On the left-hand side of the chart, we identify concerns inherent to technology, data, or decisions. Those concerns do not necessarily have a direct impact but can develop into graver concerns about the consequences on the right-hand side.

Since applied technology, such as an algorithm, needs data to make automated decisions for the user, the concerns on the left-hand side of the framework are divided into three categories:

technology, data, and decision. These concerns about technology, data, and decision can lead to further concerns in different categories adapted from Karwatzki et al. (2017) and described in Table 3.1-2.

Category	Definition
Physical	Loss of physical safety due to the application of ADM
Social	Change in social status due to the application of ADM
Resource-related	Loss of resources due to the application of ADM
Psychological	Negative impact on one's peace of mind due to the application of ADM
Prosecution-related	Legal actions taken against an individual due to the application of ADM
Career-related	Negative impacts on one's career due to the application of ADM
Freedom-related	Loss of freedom of opinion and behavior due to the application of ADM

Table 3.1-2: Categories of concerns about consequences that individuals have due to the use of ADM adapted from Karwatzki et al. (2017)

A concern on the left-hand side can give rise to more than one concern on the right-hand side. For example, *"poor decision quality"* can lead to various specific concerns at different levels on the right-hand side of the framework, e.g., *"negative financial impact"* if the algorithm opts for more expensive consumer goods, *"negative physical impact"* if the autonomous driving car gets involved in an accident, or *"discrimination"* if the algorithm discriminates females for job offers. With the icons in Figure 3.1-1, we indicate whether a concern originates from semi-structured interviews (microphone) and/or from the literature review (book).

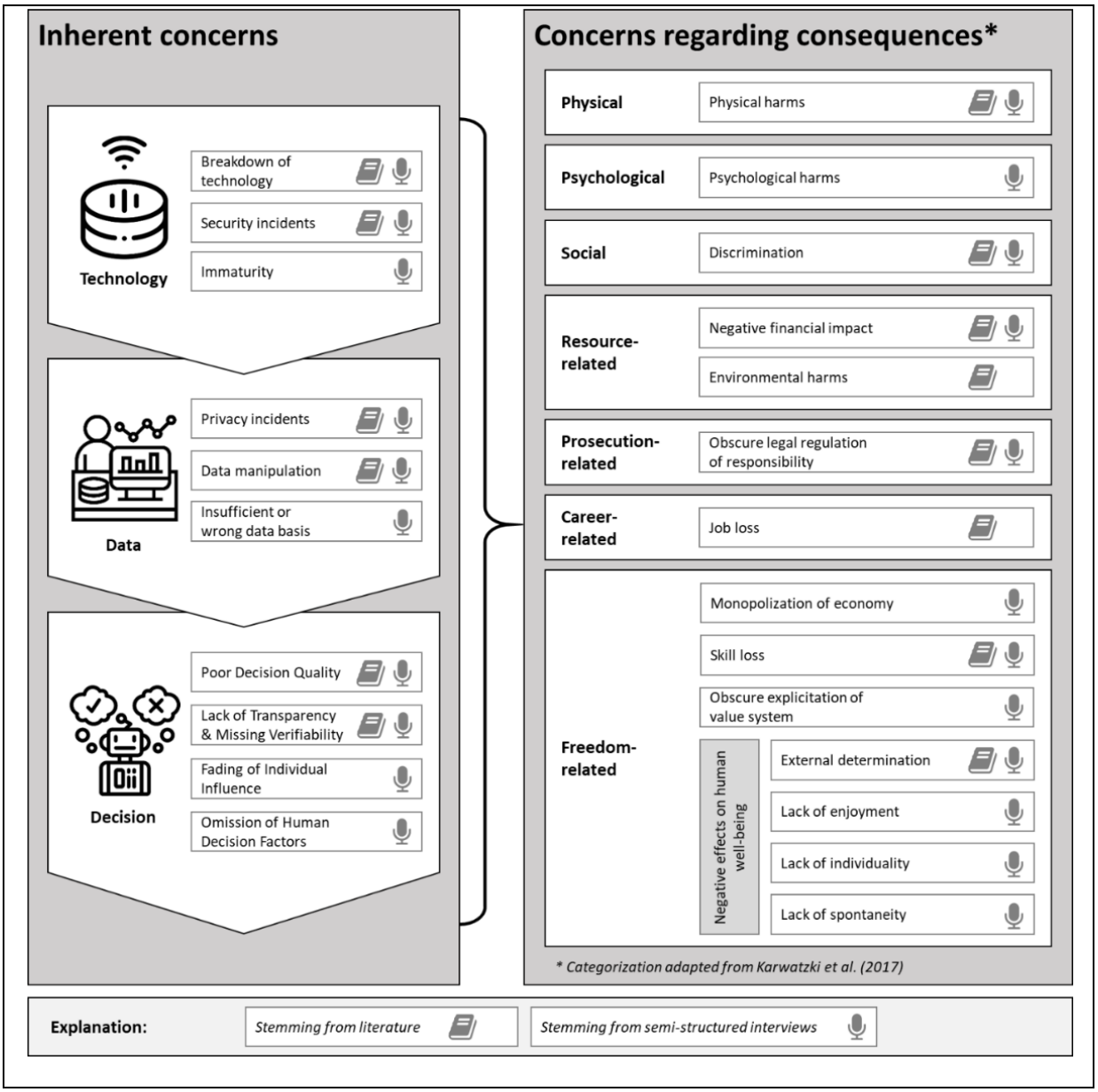


Figure 3.1-1: Framework of concerns about the use of ADM

Job loss and *environmental harms* are the only two aspects that did not occur in any interview but solely in the literature. All other 13 concerns that we found in the literature were confirmed in the interviews. Furthermore, our interviews added four concerns to the framework's left-hand side and seven concerns to the right-hand side. Table 3.1-3 presents the inherent concerns (left-hand side of Figure 3.1-1). Table 3.1-4 presents the concerns about consequences (right-hand side of Figure 3.1-1). For each concern, an explanation is provided, and literature sources as well as the IDs of the respective interviewees are shown to identify the origin of each concern.

Concerns	Description	Literature sources	Interviews
Technology			
Breakdown of technology	*Concerns about failures in technology or single features of technology*	Winters, 2017; Woldeamanuel & Nguyen, 2018	5, 10
Security incidents	*Concerns about security incidents via technology or enabled by technology, such as misuse of related IT systems*	Winters, 2017; Woldeamanuel & Nguyen, 2018	4, 5, 13
Immaturity	*Concerns that technology is not yet fully mature and does not meet functional expectations*	-	2, 6, 7, 8
Data			
Privacy incidents	*Concerns about data privacy, in particular the use of and access to personal data (privacy invasion), disclosure of personal data to third parties (e.g., employers and health insurance companies), misuse of personal data for other purposes, and loss of control over the usage of personal data*	Alawadhi & Hussain, 2019; Coudert, 2010; Duarte, 2017; Newell & Marabelli, 2015; Strobel, 2019; Winters, 2017; Woldeamanuel & Nguyen, 2018	1, 6, 7, 8, 9, 10, 11, 12, 13
Data manipulation	*Concerns that manipulated data underlying the algorithm may lead to biased results of ADM*	Winters, 2017; Yang et al., 2018	1, 5, 9
Insufficient or wrong data basis	*Concerns that the data basis is insufficient, or that the data provided cannot be explained adequately*	-	3, 4, 6, 9, 10, 13
Decision			
Poor decision quality	*Concerns about the poor decision-making quality of a given system, leading to mistakes or decisions that do not match the fears, wishes, and preferences of individuals*	Bahner et al., 2008; Brauneis & Goodman, 2018; Strobel, 2019; Uhl, 1980; Westin et al., 2016; Winters, 2017; Woldeamanuel & Nguyen, 2018	1, 2, 3, 4, 7, 8, 11, 12, 13
Lack of transparency and missing verifiability	*Concerns about the lack of traceability of decisions by ADM, as decision-making takes place in the background ("black box") and is thus not comprehensible for individuals*	Brauneis & Goodman, 2018; Strobel, 2019; Westin et al., 2016; Yang et al., 2018	1, 3, 8, 9, 13
Fading of individual influence	*Concerns about losing the ability to influence the decision-making process due to loss of personal bargaining power, as opposed to traditional decision-making*	-	1, 2, 3, 6, 7, 11
Omission of human decision factors	*Concerns about the lack of human elements (empathic capacity) in ADM's decision-making, i.e., soft aspects and special cases are no longer taken into account*	-	1, 2, 5, 8, 9, 10, 12, 13

Table 3.1-3: Individuals' inherent concerns about ADM

The first category, *technology*, describes concerns about the technology used for ADM. *Breakdown of technology* is primarily seen as dangerous because "humans are highly dependent on technology" (Interviewee 10) and because technology could create "accidents involving humans" (Winters, 2017). The literature also shows that individuals are concerned about

disruption to infrastructure (Winters, 2017) or potential system failure (Woldeamanuel & Nguyen, 2018). *Security incidents* refer to security concerns about system as a whole, and especially to the underlying data. Woldeamanuel and Nguyen (2018) indicate that the majority of individuals has security concerns, be they clear-cut security incidents or more general concerns about incidents associated with technology, e.g., the fear that someone may know when you are not home and then "burgle the house" (Interviewee 5, 13). Doubts that the system "will ever be mature enough to work 100%" (Interviewee 7) are summarized in the category *immaturity*.

The category *data* comprises concerns that individuals expressed about data used for ADM. *Privacy incidents* facilitated by "complete transparency of individuals" (Interviewee 1) are widely discussed in the literature (Alawadhi & Hussain, 2019; Coudert, 2010; Duarte, 2017; Newell & Marabelli, 2015; Strobel, 2019; Winters, 2017), and indeed in our interviews. The statements of Interviewee 12 ("the idea that one is completely predictable is daunting"), Interviewee 13 (who expressed concern about "having no control at all" over personal data), or Interviewee 11 (who said "data collected will be used for any other purpose") confirm the relevance of this issue. Concerns about manipulation of "the input that the algorithm receives" (Interviewee 9), e.g., via "false statements" (Interviewee 1), "paid advertisement that influences the algorithm" (Interviewee 1, 5), or that "small changes in the input data […] may lead to drastic changes in the output, making the result uninformative and easy to manipulate" (Yang et al., 2018) are summarized in *data manipulation*. *Insufficient or wrong data basis* includes, e.g., concerns about "weak points in the entered data, where you know they can be misinterpreted without further explanation" (Interviewee 3) or that data quality "depends on how well I maintain my personal data, e.g., how I answer the questions" (Interviewee 13), related to the thought that "an algorithm needs all data from my wife and me, and so it is not capable of booking a holiday for us, as it will never know how many and which compromises are possible and which are not" (Interviewee 10).

The category *decision* presents concerns that individuals have about the automated decision itself. Individuals are concerned about *poor decision quality*. They are convinced that "implementation will never be 100% correct" (Interviewee 1) and think that the algorithm cannot respond with sufficient sensitivity to highly individual needs. The topic of poor decision quality is also discussed in the literature as the fear individuals have, for example, about incorrect decisions (Strobel, 2019) or false recommendations. Furthermore, individuals are concerned about a *lack of transparency and missing verifiability* of decisions made by ADM, i.e., they cannot verify whether the decision really is the best one or "if it is only the third-best offer"

(Interviewee 1), because they "don't know about the decision basis in the background" (Interviewee 1). Intransparency is another relevant topic in the literature, as individuals do not fully understand the opacity of a system (Westin et al., 2016). Meanwhile, *fading of individual influence* is discussed in the interviews with regard to "loss of bargaining space" (Interviewee 1) or a sense that there is no "possibility for a personal introduction, where my abilities might be recognized" (Interviewee 11) due to a lack of human involvement. O*mission of human decision factors* refers to "missing empathy" (Interviewee 9), "complete reduction to numbers" (Interviewee 5), and the thought that a "human can be better assessed by other humans than by algorithm" (Interviewee 12), especially in "exception cases" (Interviewee 12).

Having illustrated the inherent concerns, Table 3.1-4 shows concerns about consequences of ADM.

Concerns	Description	Literature sources	Interviews
Physical			
Physical harms	*Concerns that use of ADM may result in physical harm, such as accidents involving individuals*	Brauneis & Goodman, 2018	6, 7, 13
Psychological			
Psychological harms	*Concerns that the feeling of being at the mercy of ADM systems has negative consequences on individuals' mental health*	-	13
Social			
Discrimination	*Concerns that existing discrimination in human decision-making is being systematized through ADM, leading to structural biases and unfairness in decisions*	Albarghouthi & Vinitsky, 2019; Binns et al., 2018; Brauneis & Goodman, 2018; Dietrich & Weisswange, 2019; Kullmann, 2018; Persson & Kavathatzopoulos, 2017; Strobel, 2019; Veale & Edwards, 2018; Woldeamanuel & Nguyen, 2018; Yang et al., 2018	1, 2, 3, 4, 6, 7, 8, 11, 13
Resource-related			
Negative financial impact	*Concerns about ADM making decisions that are financially unfavorable for individuals*	-	6, 8, 13
Environmental harms	*Concerns about negative impacts on environment through the spread of ADM*	Winters, 2017; Woldeamanuel & Nguyen, 2018	-
Prosecution-related			
Obscure legal regulation of responsibility	*Concerns about missing or unclear legal accountability for the decisions taken by algorithms*	Binns et al., 2018; Persson & Kavathatzopoulos, 2017; Woldeamanuel & Nguyen, 2018	2, 3
Career-related			
Job loss	*Concerns about becoming unemployed due to widespread use of ADM*	Winters, 2017	-

Freedom-related			
Monopolization of economy	*Concerns about monopolization on a limited number of platforms which gain disproportionate power from data, leading to a centralized and unbalanced market*	-	1, 8, 11
Skill loss	*Concerns about individuals losing abilities or skills because they are no longer used to performing certain tasks*	Winters, 2017	2, 7, 8, 10, 12
Obscure explicitation of value system	*Concerns about a lack of morality in ADM or a mismatch between the moral values of the system and personal values*	-	1, 2, 4, 8, 12, 13
Negative effects on human well-being			
External determination	*Concerns that individuals give up more control over their lives to ADM systems (and organizations operating those systems)*	Newell & Marabelli, 2015; Woldeamanuel & Nguyen, 2018	3, 4, 6, 8, 9, 11, 12
Lack of enjoyment	*Concerns that ADM decreases sensual and joyful moments, as the decision-making process itself is an enjoyable part of life that is no longer experienced by humans*	-	2, 6, 8, 9, 10, 13
Lack of individuality	*Concerns that ADM is not capable of reaching a level of individuality close to that of highly individual human decision-making*	-	1, 2, 8, 9, 12, 13
Lack of spontaneity	*Concerns that rigid patterns of ADM curtail the human value of spontaneity in daily life*	-	1, 4, 7, 13

Table 3.1-4: Individuals' concerns about consequences of ADM

Physical harms refer, for the most part, to accidents caused by ADM, e.g., via self-driving cars and other health hazards due to the increasing use of ADM technologies. In contrast, *psychological harms* denote "emotional damage" (Interviewee 13) through ADM. In the literature, Brauneis and Goodman (2018) also mention the concern that data can be used to hurt individuals.

Discrimination is among the most frequently discussed topics in the literature on ADM. Perhaps the most common form this takes is gender discrimination against individuals or protected groups (Kullmann, 2018; Persson & Kavathatzopoulos, 2017; Yang et al., 2018). Our interviews confirm this, as many interviewees fear biased decisions due to the "discrimination between men and women" (Interviewee 8) and "exclusion of people who cannot afford or use technologies that get more and more sophisticated and therefore expensive" (Interviewee 11). Often, discriminatory decisions made by automated systems result from biased training data sets (Interviewee 1).

Furthermore, individuals are concerned about ADM having a *negative financial impact*, primarily caused by *data manipulation*, e.g., when an algorithm orders a product at "a disadvantageous price" due to a paid advertisement (Interviewee 8) or a faulty product that will not be used (Interviewee 6). The category *environmental harms* comprises aspects such as increasing air pollution or greenhouse gas emission (Winters, 2017; Woldeamanuel & Nguyen, 2018).

The following concern *obscure legal regulation of responsibility* is prosecution-related. Individuals fear that it is unclear "who bears responsibility if something happens" (Interviewee 3). One such concern relates to the use case of autonomous driving, as stated by Interviewee 2: "In case somebody dies, or gets injured or anything else, who is responsible?"

Individuals also have career-related concerns. Winters (2017) states that individuals fear losing their jobs (*job loss*) due to ADM.

The first concern in the category of freedom-related concerns is the *monopolization of economy*, meaning that "the market becomes more unbalanced" (Interviewee 1). *Skill loss* refers to the concern that with an increasing number of automated decisions and thus a diminishing proportion of human-made decisions, individuals lose human abilities, such as "empathy" (Interviewee 10) and decision-making skills (Interviewee 12). *Skill loss* also includes a concern about "humans becoming lazy or less industrious" and "losing certain abilities or skills" (Winters, 2017). In *obscure explicitation of value system*, individuals fear a lack of morality in ADM or a mismatch between the moral values of the system and personal values. For instance, this may result from distinct cultural backgrounds of an algorithm's programmer and its users.

The subcategory of negative effects on human well-being comprises four concerns. Individuals prefer non-binding "recommender systems" (Interviewee 2, 8) in contrast to a completely automated decision in order to avoid *external determination*. The literature confirms these views, as concerns about dependence and loss of control have already been investigated (Newell & Marabelli, 2015; Woldeamanuel & Nguyen, 2018). *Lack of enjoyment* includes statements that ADM in private life is associated with having less fun. For example, decisions about food or traveling are perceived as "fun" (Interviewee 6, 9), and to some the decision-making process itself constitutes an "experience" (Interviewee 13), which is why some do not want to give up decision-making. Meanwhile, *lack of individuality* denotes concerns about the inability of ADM to reach a sufficiently high level of individuality in decision-making: "No matter how complex the algorithm, it will never offer a highly individual trip for me" (Interviewee 8). Another interviewee raised the question: "Where is the individuality?" (Interviewee 2). The *omission of human decision factors* is seen as the chief reason why ADM will

not achieve sufficiently high individuality. Moreover, individuals are concerned about a *lack of spontaneity* through the use of ADM in their daily lives, as they feel that the algorithm cannot respond unprompted to changes, which is why there will no longer be any room for spontaneity (Interviewee 1). Incidentally, according to some individuals it is simply "nice if not everything is planned, but you just happen to stumble over something" (Interviewee 8).

3.1.5 Discussion

The interviewees confirmed concerns that were identified by the structured literature search. Only two concerns originating from the literature could not be confirmed by our qualitative content analysis (*job loss, environmental harms*). This might be due to the abstract nature of these two long-term consequences of ADM, which is to say that our interviewees may well have thought of those aspects as being too far in the future to be caused by single automated decisions. Yet these two aspects aside, the concerns discussed in the literature were supplemented by eleven further concerns that were first identified in our qualitative content analysis. To break down those numbers, four concerns were added to the literature on the left-hand side of the framework (immaturity, insufficient or wrong data basis, fading of individual influence, omission of human decision factors).

A closer look at the inherent concerns in Table 3.1-3 shows that only concerns in the category *decision* are unique to ADM. Conversely, *technology* and *data* concerns can also be transferred to other new technologies, such as the Internet of Things (IoT) or Blockchain. For example, *security* and *privacy incidents* have already been discussed in depth in the existing IoT literature (Leloglu, 2017; Naeini et al., 2005). Further concerns, such as *immaturity*, also pertain to other new technologies and are, therefore, not specific to ADM (Lepekhin et al., 2019). Concerns arising from these two categories – *technology* and *data* – can lead to concerns about consequences for individuals, organizations, or society, and these concerns can be held regardless of whether a specific automated decision is executed. For example, a *security incident* where personal data is stolen, which causes a *privacy incident*, might lead to discrimination in another context, one that is quite distinct from the original decision-making process during which the data was collected and therefore not governed nor indeed controlled by the initial decision.

As explained above, our framework contains eleven concerns that emerged solely from our interviews and have not been addressed in previous research. Within all categories, the interviews revealed new inherent concerns as well as concerns about consequences that lend them-

selves to further examination in future research (see Figure 3.1-1), which is strongly recommended in order to reduce individuals' skepticism about ADM and improve its acceptance among users. Some of the associated concerns worthy of further research are as follows: first, interviewees mentioned several aspects that mitigate their concerns about ADM, chief among them the fact that for many there is no perceived difference between ADM and a human decision-making process. For instance, interviewees often do not see a notable difference whether they provide their personal data to a human or to an algorithm. Furthermore, they tend to think that nowadays many organizational processes are already automated to a high degree, even though a human employee is involved. Another crucial aspect that would seem to attenuate many concerns is transparency. If individuals think they understand the decision-making process, which is to say that if they understand how and why the algorithm comes to its decision, many concerns are mitigated. A research area that focuses on this phenomenon is called explainable AI (XAI). XAI research analyses the black-box problem, i.e., that AI is becoming ever more complex. Hence, it becomes more difficult for the user to truly understand how the system works, and this diminishes the transparency of the user system (Bahdanau et al., 2017). This, in turn, brings us to trust, the third mitigating aspect mentioned in our interviews. Individuals state that their concerns about a specific ADM system significantly decrease when they trust the system, for instance, if they have had good experiences with the same system in the past.

In addition to those attenuating aspects, interviewees mentioned potential positive aspects of ADM, as opposed to human-made decisions. These include time savings, less effort for individuals, less subjectivity and more fairness in decisions, variety and positive surprises through ADM, and lower error rate in decisions. Future research could be of interest to examine the relationship between those attenuating and positive aspects of ADM on the one hand and the afore-mentioned concerns on the other. It might be very helpful for the development of ADM systems to know which concerns could be addressed by which attenuating aspects and under which circumstance, or for instance in which use case a user will focus more on positive aspects and less on concerns.

To develop these findings into a coherent theory, we follow in the footsteps of Urquhart et al. (2010): "Theoretical integration means relating the theory to other theories in the same or similar field." Since there is, at the time of writing this, no relevant theory to draw on with regard to ADM, we employ a related theory from the field of information privacy research. Specifically, we compare our framework with Karwatzki et al. (2017), who investigate ad-

verse consequences of access to individuals' information. What makes this comparison especially apt is that Karwatzki et al. (2017) examine individuals' technology-related concerns and develop a comprehensive conceptualization and categorization in terms of physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related adverse consequences. In our own research, we transfer this categorization to the field of ADM and use it to structure individuals' concerns about consequences, i.e., the right-hand side of our framework (see Table 3.1-4). What is more, we identify inherent concerns about technology, data or decisions, i.e., the left-hand side of our framework (see Table 3.1-3). Karwatzki et al. (2017) present very detailed manifestations in each category, i.e., concrete concerns (e.g., kidnapping and imprisonment, slander and bullying, stalking), and these also apply to ADM. For instance, the manifestation "financial loss (direct or indirect)" is very similar to our concern *negative financial impact* (Karwatzki et al., 2017). Another example is the manifestation "being fired". This relates to our concern *job loss* (Karwatzki et al., 2017). However, Karwatzki et al. (2017) identified other manifestations, such as "time loss", which do not apply to ADM as they are mentioned neither in the literature nor in our interviews.

Moreover, we expect our framework to provide several meaningful insights for individuals and organizations using ADM, and it is our express hope that our work in this area will lead to further research. ADM is a current topic of great interest and potential, but so far researchers have focused either on the possibilities of using and implementing ADM or on dealing with its technical consequences and ethical issues, while the concerns of individuals have only been considered selectively or disregarded entirely. None of the papers to date have focused on any reasons for reluctance from an individual's point of view. Our primary theoretical contribution is, therefore, the understanding and structuring of concerns that prevent individuals from using ADM applications. Our framework can be used – either ex-ante or ex-post – to anticipate and evaluate problems associated with the introduction of ADM applications. We believe that our framework provides an interesting new perspective on this issue and will guide future research. Furthermore, it contributes to the extensive literature on the dark side of IS since it contains individuals' concerns and fears about using a specific technology, i.e., ADM.

Our results also offer practical benefits. A thorough consideration of concerns is essential as it can determine whether or not ADM applications are successfully disseminated. Our findings clearly show that some of the concerns are subjective feelings. Companies that implement or think about implementing ADM use cases should consider these concerns when developing ADM applications. They can use the framework to address these concerns, offer their pro-

spective users targeted information, and strengthen trust in process outcomes based on automated decisions. Furthermore, our framework allows individuals to systematically gather information about ADM's potential risks for themselves and thus balance their concerns about ADM applications with facts. Many interviewees did not raise many concerns at the beginning of our interview but instead required concrete use cases to articulate their concerns.

Nevertheless, our research does not yet go far enough. Whereas the findings from the literature review are based on studies from different regions and countries, the interviews were all conducted in Germany. Expecting interesting cultural differences, the framework may be improved by extending the scope of the interviews to different countries (Belanger & Crossler, 2011). Even though we included open questions regarding concerns about ADM at the beginning of each interview, future research may strive for more generalizability or test concerns for a specific use case. Moreover, future research may clarify the relationship between the concerns by collecting quantitative data and evaluating it, e.g., with factor analysis. Such future research may also contribute to the current discussion by developing appropriate countermeasures that address individuals' concerns about ADM.

3.1.6 Conclusion

The aim of this paper was to provide an overview of concerns about ADM and thus show the need for further research in this area. To date, the literature in the field has neglected the individual human side. Therefore, it has failed to account for the importance of individuals' concerns as limiting factors in the adoption of ADM. Based on a thorough structured literature search and semi-structured interviews, we identified the concerns already addressed in the literature as well as those it has so far neglected. In total, we identified 24 concerns associated with integrating automated decisions into a person's life. We structured these concerns in a framework divided into different categories: technology, data, decision for inherent concerns, and concerns adapted from the categories of Karwatzki et al. (2017). It is our belief that this framework will help in summarizing and communicating concerns about ADM with a view to increasing confidence in automated decisions. As a result, this framework shall also support the adoption of ADM applications and enable individuals to be better informed about potential risks.

References

Alawadhi, R., & Hussain, T. (2019). A method toward privacy protection in context-aware environment. *Procedia Computer Science*, *151*, 659–666. https://doi.org/10.1016/j.procs.2019.04.088

Albarghouthi, A., & Vinitsky, S. (2019). Fairness-Aware Programming. In *Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency,* Atlanta, GA, USA.

Allen, R., & Masters, D. (2019). Artificial Intelligence: the right to protection from discrimination caused by algorithms, machine learning and automated decision-making. *ERA Forum.* Advance online publication. https://doi.org/10.1007/s12027-019-00582-w

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks.* ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bahdanau, D., Cho, K., & Bengio, Y. (2017). Neural Machine Translation by Jointly Learning to Align and Translate. *IJCAI-17 Workshop on Explainable AI (XAI)*, *8*(1).

Bahner, J. E., Hüper, A.-D., & Manzey, D. (2008). Misuse of automated decision aids: Complacency, automation bias and the impact of training experience. *International Journal of Human-Computer Studies*, *66*(9), 688–699. https://doi.org/10.1016/j.ijhcs.2008.06.001

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041.

Binns, R., van Kleek, M., Veale, M., Lyngs, U., Zhao, J., & Shadbolt, N. (2018). It's Reducing a Human Being to a Percentage. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems,* Montreal QC, Canada.

Borràs, J., Moreno, A., & Valls, A. (2014). Intelligent tourism recommender systems: A survey. *Expert Systems with Applications*, *41*(16), 7370–7389. https://doi.org/10.1016/j.eswa.2014.06.007

Boyatzis, R. E. (1988). *Transforming Qualitative Information: Thematic Analysis and Code Development*. SAGE Publications.

Brauneis, R., & Goodman, E. P. (2018). Algorithmic transparency for the smart city. *Yale Journal of Law and Technology*, *20*(1).

Castelo, N., Bos, M. W., & Lehmann, D. R. (2019). Task-Dependent Algorithm Aversion. *Journal of Marketing Research*, *56*(5), 809–825. https://doi.org/10.1177/0022243719851788

Cho, E., & Han, M. (2019). AI Powered Book Recommendation System. In D. Lo (Ed.), *Proceedings of the 2019 ACM Southeast Conference on ZZZ - ACM SE '19* (pp. 230–232). ACM Press. https://doi.org/10.1145/3299815.3314465

Corbett-Davies, S., Pierson, E., Feller, A., & Goel, S. (2016). *A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear.* https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/

Coudert, F. (2010). When video cameras watch and screen: Privacy implications of pattern recognition technologies. *Computer Law & Security Review*, *26*(4), 377–384. https://doi.org/10.1016/j.clsr.2010.03.007

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM*, *59*(2), 56–62. https://doi.org/10.1145/2844110

Dietrich, M., & Weisswange, T. H. (2019). Distributive justice as an ethical principle for autonomous vehicle behavior beyond hazard scenarios. *Ethics and Information Technology*, *21*, 227–239. https://doi.org/10.1007/s10676-019-09504-3

Dietvorst, B. J., Simmons, J. P., & Massey, C. (2018). Overcoming Algorithm Aversion: People Will Use Imperfect Algorithms If They Can (Even Slightly) Modify Them. *Management Science*, *64*(3), 1155–1170. https://doi.org/10.1287/mnsc.2016.2643

Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, *4*(1), 1-5. https://doi.org/10.1126/sciadv.aao5580

Duarte, N. (2017). Building Ethical Algorithms. *Scitech Lawyer*, *14*(1), 32–37.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., . . . Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Faliagka, E., Tsakalidis, A., & Tzimas, G. (2012). An integrated e-recruitment system for automated personality mining and applicant ranking. *Internet Research*, *22*(5), 551–568. https://doi.org/10.1108/10662241211271545

Gimpel, H., & Schmied, F. (2019). Risks and Side Effects of Digitalization: A Multi-Level Taxonomy of the Adverse Effects of Using Digital Technologies and Media. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden.

Hauff, S., Veit, D., & Tuunainen, V. K. (2015). Towards a taxonomy of perceived consequences of privacy-invasive practices. In *Proceedings of the 23rd European Conference on Information Systems (ECIS)*, Münster, Germany.

Hsie, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*, 1277–1288.

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, *26*(6), 688–715. https://doi.org/10.1057/s41303-017-0064-z

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. https://doi.org/10.1016/j.is.2010.11.003

Kullmann, M. (2018). Platform work, algorithmic decision-making, and EU gender equality law. *International Journal of Comparative Labour Law and Industrial Relations*, *34*(1), 1–21.

Kumar, B. (2015). An encyclopedic overview of big data analytics. *International Journal of Applied Engineering Research*, *10*(3), 5681–5705.

Leloglu, E. (2017). A review of security concerns in internet of things. *Journal of Computer and Communications*, *5*(1), 121–136. https://doi.org/10.4236/jcc.2017.51010

Lepekhin, A., Borremans, A., Ilin, I., & Jantunen, S. (2019). A Systematic Mapping Study on Internet of Things Challenges. In (pp. 9–16). IEEE. https://doi.org/10.1109/SERP4IoT.2019.00009

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163–200.

Majchrzak, A., Markus, M. L., & Wareham, J. (2016). Designing for digital transformation: Lessons for information systems research from the study of ICT and societal challenges. *MIS Quarterly*, *40*(2), 267–277.

Martin, K. (2019). Designing ethical algorithms. *MIS Quarterly Executive*, *18*(2), 129–142. https://doi.org/10.17705/2msqe.00012

Mayring, P. (2010). Qualitative Inhaltsanalyse. In G. Mey & K. Mruck (Eds.), *Handbuch qualitative Forschung in der Psychologie* (pp. 601–613). VS Verlag für Sozialwissenschaften.

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L., & Sadeh, N. (2005). Privacy Expectations and Preferences in an IoT World. In *4th USENIX Conference on File and Storage Technologies,* San Francisco, CA, USA.

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. *The Journal of Strategic Information Systems, 24*(1), 3–14. https://doi.org/10.1016/j.jsis.2015.02.001

Persson, A., & Kavathatzopoulos, I. (2017). How to make decisions with algorithms: Ethical decision-making using algorithms within predictive analytics. *ACM Computers & Society*, *47*(4).

Pirkkalainen, H., & Salo, M. (2016). Two Decades of the Dark Side in the Information Systems Basket: Suggesting five Areas for Future Research. In *Proceedings of the 24th European Conference on Information Systems (ECIS),* Istanbul, Turkey.

Ringe, A., Dalavi, M., Kabugade, S., & Mane, P. P. (2019). IoT based smart refrigerator using Raspberry Pi. *International Journal of Research and Analytical Reviews*, 154–158.

Rustemeyer, R. (1992). *Praktisch-methodische Schritte der Inhaltsanalyse*. Aschendorff.

Schreier, M. (2013). Qualitative Content Analysis. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Analysis.* SAGE Publications Ltd.

Shankararaman, V., & Gottipati, S. (2015). A Framework for Embedding Analytics in a Business Process. In D. Aveiro & A. Caetano (Eds.), *2015 IEEE 17th Conference on Business Informatics (CBI)* (pp. 49–54). IEEE. https://doi.org/10.1109/CBI.2015.10

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196.

Strobel, M. (2019). Aspects of Transparency in Machine Learning: Doctoral Consortium. In *Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019),* Montreal.

Tarafdar, M., Gupta, A., & Turel, O. (2015a). Introduction to the special issue on 'dark side of information technology use' - part two. *Information Systems Journal*, *25*(4), 315–317. https://doi.org/10.1111/isj.12076

Tarafdar, M., Gupta, A., & Turel, O. (2015b). Special issue on 'dark side of information technology use': An introduction and a framework for research. *Information Systems Journal*, *25*(3), 161–170. https://doi.org/10.1111/isj.12070

Uhl, F. S. (1980). Automated capital investment decisions. *Management Accounting*, *61*(10).

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems. *Information Systems Journal*, *20*(4), 357–381. https://doi.org/10.1111/j.1365-2575.2009.00328.x

Vahn, G.-Y. (2014). Business analytics in the age of big data. *Business Strategy Review*, *25*(3), 8–9. https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-8616.2014.01083.x

van den Broek, E., Sergeeva, A., & Huysman, M. (2019). Hiring Algorithms: An Ethnography of Fairness in Practice. In *Proceedings of the 40th International Conference on Information Systems (ICIS)*, Munich, Germany.

Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, *34*(2), 398–404. https://doi.org/10.1016/j.clsr.2017.12.002

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), 13–23.

Westin, C., Borst, C., & Hilburn, B. (2016). Automation transparency and personalized decision support: Air traffic controller interaction with a resolution advisory system. *IFACPapersOnLine*, *49*(19), 201–206.

Winters, J. (2017). By the numbers: How much do we trust AI? *Mechanical Engineering*, *139*(1), 26–27.

Woldeamanuel, M., & Nguyen, D. (2018). Perceived benefits and concerns of autonomous vehicles: An exploratory study of millennials' sentiments of an emerging market. *Research in Transportation Economics*, *71*, 44–53. https://doi.org/10.1016/j.retrec.2018.06.006

Yang, K., Stoyanovich, J., Asudeh, A., Howe, B., Jagadish, H. V., & Miklau, G. (2018). A Nutritional Label for Rankings. In G. Das, C. Jermaine, & P. Bernstein (Chairs), *Proceedings of the 2018 International Conference on Management of Data,* Houston, TX, USA.

3.2 Understanding the evaluation of mHealth app features based on a cross-country Kano analysis

Abstract: While mobile health (mHealth) apps are playing an increasingly important role for digitalized healthcare, little is known regarding the effects of specific mHealth app features on user satisfaction across different healthcare system contexts. Using personal health record (PHR) apps as example, this study identifies how potential users in Germany and Denmark evaluate a set of 26 app features, and whether evaluation differences can be explained by differences in four pertinent user characteristics, namely privacy concerns, mHealth literacy, mHealth self-efficacy, and adult playfulness. Based on survey data from both countries, we employed the Kano method for the evaluation of PHR features and applied a quartile-based sample split approach to unravel the underlying relationships between users' characteristics and their perceptions of features. Our results not only show significant differences in 14 of the features between Germans and Danes, they also demonstrate which of the user characteristics explain each of these differences best. Our two key contributions are, therefore, first to shed light on the evaluation of specific PHR app features on user satisfaction in two different healthcare contexts and second to demonstrate how to extend the Kano method with a perspective for explaining subgroup differences through user characteristic antecedents. Implications for app providers and policy makers are discussed.

Keywords: Personal health record, Kano model, privacy concerns, mHealth literacy, mHealth self-efficacy, adult playfulness

Authors: Henner Gimpel, Tobias Manner-Romberg, Fabian Schmied, Till Winkler

Status: This article is published in Electronic Markets, Volume 31, Issue 4, pp. 765-794 (2021).

3.2.1 Introduction

Mobile health applications (mHealth apps) play an increasingly important role in the digitalization of nationwide healthcare services for better health outcomes due to the ubiquity of smartphones in society (Ali et al., 2016; Bhavnani et al., 2016; Birkhoff & Moriarty, 2020; Messner et al., 2019; Stoyanov et al., 2015; Xu & Liu, 2015). In 2017, the number of available mHealth apps was estimated at approximately 300,000 and will grow by about 25% every year (Benjumea et al., 2020; Larson, 2018). Frequent examples of mHealth apps are disease-specific apps (e.g., for diabetes), apps for strengthening health competence or adherence (e.g., medication reminders and diet and nutrition tracking), and apps for the storage and exchange of health-related data (e.g., personal health records (PHRs)) (Aitken et al., 2017; Jimenez et al., 2019; Knöppler et al., 2016). The usage of mHealth apps promises excellent opportunities, including improvement in user self-management and user empowerment (Wickramasinghe et al., 2012; Zapata et al., 2015). For example, throughout the COVID-19 pandemic, tracking apps have been used for contact tracing and monitoring infected individuals (Salathé et al., 2020). Moreover, PHR apps are promoted as a digital solution toward greater patient empowerment by integrating health data in one spot (Helmer et al., 2011; Sachverständigenrat Gesundheitswesen, 2020; Schneider et al., 2016). Although literature agrees on the considerable potential of mHealth apps, the current adoption of mHealth apps is still low (Lusignan et al., 2013; Ozok et al., 2017; Thies et al., 2017). Furthermore, the retention rate of actual mHealth app users is comparatively low (Vaghefi & Tulu, 2019; Zhou, Bao, Watzlaf, & Parmanto, 2019). Due to the plethora of available mHealth apps (Benjumea et al., 2020; Larson, 2018), there is a wide variability in quality and key features of the apps (Jimenez et al., 2019). Because of this abundance, users struggle to identify appropriate, secure, and trustworthy mHealth apps that fulfill their specific needs (Jimenez et al., 2019; van Haasteren et al., 2020). To overcome this challenge, several authors suggest to better involve relevant stakeholders to the app development process (Jimenez et al., 2019; Marent et al., 2018). Within our paper, we focus on mHealth app users as a relevant stakeholder group to better understand their needs and preferences and to contribute to the development of more appropriate apps.

Specific mHealth app features' relative attractiveness to user groups in different countries is not yet well understood. Despite country-dependent conditions, such as the technological infrastructure and cultural attitudes (Wickramasinghe & Schaffer, 2010), the preponderance of mHealth research has addressed user acceptance of mHealth only on the app level (e.g., Abd-Alrazaq et al., 2019; Bin Azhar & Dhillon, 2016; Dehzad et al., 2014; Stoyanov et al., 2015; Vaghefi & Tulu, 2019). While providing important insight into the factors influencing the

general attractiveness of mHealth apps, the app-level approach obscures differences in the feature evaluation of the specific mHealth app, which typically consists of a bundle of privacy-related (Kharrazi et al., 2012), data-related (Maloney & Wright, 2010), functionality-related (e.g., Cabitza et al., 2015), and other possible features, such as gamification (e.g., Mendiola et al., 2015). Furthermore, most prior mHealth research has evaluated mHealth apps in a single geography (e.g., La Torre Díez et al., 2017; R. A. Lee & Jung, 2018) and thus has implicitly ignored the potential influences of technological, legal, and cultural variations across countries on the attitudes of the user groups. Feature-specific knowledge about mHealth apps that is sensitive to the potential influence of the country context is valuable to mHealth app providers (e.g., governmental agencies, health insurances, and startups) to provide apps that satisfy the specific user needs and thus to enhance the so-far underwhelming adoption rates of most mHealth apps.

To address the gap in our knowledge on the feature-specific and context-sensitive evaluation of mHealth apps, we focus on the case of the PHR app and the potential users in two countries representing distinct healthcare system contexts in Europe: Germany and Denmark. The PHR apps are a suitable representative of mHealth apps because they cover various features relevant to a broad segment of society (Roehrs et al., 2017). Our focus on German and Danish[12] users provides an adequate basis for comparative analysis within the European Union. Both countries have a joint background in European regulation and similar Western values, whereas they differ concerning critical aspects of digital health care. While the Danish *Beveridge* health system is often thought of as a digital leader, Germany's *Bismarck* health system is frequently considered to be at the slower end of the innovation curve (Bertelsmann Stiftung, 2018; Kierkegaard, 2013; Nohl-Deryk et al., 2018; Stroetmann et al., 2011). For example, Denmark launched a nationwide PHR (sundhed.dk) in 2003 (Gherardi et al., 2014), whereas PHR solutions in Germany are still fragmented and not widely adopted (Fitte et al., 2019). Consequently, the two countries represent two different predominant healthcare system types in Europe with different innovation positions. To understand potential differences in the evaluation of PHR features across the two countries, we focus on four pertinent user characteristics that have either been discussed in prior literature as factors influencing mHealth app adoption (privacy concerns, mHealth literacy, and mHealth-self-efficacy) or have been proposed to influence user satisfaction with mHealth apps more generally (adult playfulness).

Thus, we raise the following two research questions:

[12] We define country affiliation by the country in which the study participants have spent most of their life.

RQ1: *How do potential users in Germany and Denmark evaluate a broad set of specific PHR features?*

RQ2: *Do user characteristics (specifically privacy concerns, mHealth literacy, mHealth self-efficacy, and adult playfulness) explain the differences in the evaluation of PHR features by potential users in Germany and Denmark?*

To answer the research questions, we identified 26 potential PHR app features from the prior literature. We designed a cross-national survey using the Kano method (for evaluating these features) and assessing user characteristics. The Kano method (N Kano et al., 1984) is widely applied in information systems as a suitable method to understand user preferences regarding the specific attributes of a product or service (i.e., the features) as one out of four main categories (attractive, one-dimensional, must-be, or indifferent quality) (Gimpel et al., 2018; Hejaili et al., 2009). To identify possible explanations for evaluation differences between Germans and Danes, we apply a quartile-based sample split on each of the user characteristics and compare the resulting categorizations in the upper and lower quartiles with the categorization differences between Germans and Danes.

Our results from a survey of 274 participants (215 Germans and 59 Danes) demonstrate significant and meaningful differences in the evaluation of features and the evaluation between Germans and Danes. Moreover, given the empirical results that demonstrate significant group differences between Germans and Danes on the four user characteristics, we demonstrate that user characteristics help explain the evaluation differences for 14 of the 26 features. Generally, the findings indicate that users with lower privacy concerns, higher mHealth literacy, higher mHealth self-efficacy, and higher playfulness (such as Danish users) tend to evaluate more PHR features as attractive. In contrast, users with higher privacy concerns, lower mHealth literacy, lower mHealth self-efficacy, and lower playfulness (such as German users) tend to evaluate more PHR features as indifferent. We argue that our study not only explains the evaluation of a broad range of PHR app features across two representative countries but also demonstrates how to methodologically augment the Kano model with an analytical method for explaining emerging subgroup differences using antecedent user characteristics.

In the following sections, we set the theoretical foundations and develop the research hypotheses (Section 3.2.2). We also explain the research method (Section 3.2.3) and provide empirical results (Section 3.2.4). Moreover, we discuss the implications, limitations, and future research (Section 3.2.5) and conclude the work (Section 3.2.6).

3.2.2 Theoretical foundations and hypothesis development

This section reviews the theory behind the Kano model. This section also introduces PHRs and their features and develops the research hypotheses regarding the influence of the four user characteristics.

3.2.2.1 Kano theory of user satisfaction

The *user satisfaction*[13] construct is of high relevance in both research and practice due to its influence on consumer behavior (Oliver, 2014). For instance, user satisfaction has a positive impact on user loyalty (Gronholdt et al., 2000) and the overall company value (Stahl et al., 2000). Initially, user satisfaction has often been considered a one-dimensional construct: the higher the perceived product or service quality, the higher the user satisfaction, and vice versa (Yi, 1990). However, solely fulfilling user expectations to a great extent does not necessarily imply a high level of user satisfaction; it is also the type of expectation that defines the perceived quality and thus the user satisfaction (Matzler et al., 1996). Consequently, several contemporary studies have provided method-independent empirical evidence for the assumption of a multi-factorial structure of the user satisfaction construct (see Hölzing (2008) for a discussion of different approaches).

Due to the construct's importance, literature provides several methods to measure user satisfaction. A cross-sectoral applied approach to measure user expectations and perceptions of service attributes is SERVQUAL (Ladhari, 2009; Parasuraman et al., 1985), which is also applied in the healthcare domain (Akter et al., 2010; Suki et al., 2011). In addition, there are various methods that aim to capture mHealth app users' perceptions and the resulting evaluation of such apps. For instance, Stoyanov et al. (2015) developed the MARS, a new tool for assessing the quality of mHealth apps. Hereby, the application areas of the MARS range from mindfulness-based apps (Mani et al., 2015) to psychoeducational apps for military members (C. Jones et al., 2020). Korte et al. (2018) applied a mixed-method qualitative study based on individual interviews and focus groups, to evaluate a mHealth app in the working context. Finally, Melin et al. (2020) presents the development of a 12-item based questionnaire for assessing user satisfaction with mHealth apps. However, even though the different author teams focus on the evaluation of mHealth apps and the construct user satisfaction, none of the mentioned approaches intend a link of the surveyed user satisfaction to specific features.

[13] Market research usually refers to *customer satisfaction*. Because this work examines an mHealth app, we use the term *user satisfaction*.

Bartikowski and Llosa (2004) provide an analysis of further methods that capture user satisfaction with regard to specific product or service attributes, namely Dual Importance Mapping, Penalty Reward Contrast Analysis, Correspondence Analysis, and the Kano theory of user satisfaction (Kano model). The Kano model which was developed by N Kano et al. (1984) has been discussed and applied in several theoretical and empirical research projects (Füller & Matzler, 2008; Löfgren & Witell, 2008). We decided to use the Kano model, since it provides a comprehensive method to analyze the influence of product or service attributes (i.e., features) on user satisfaction.

According to the Kano model, there are four major categories, as listed in Table 3.2-1 and illustrated in Figure 3.2-1. These categories depend on actual user expectations and the implementation/nonimplementation of attributes (in our study: features of a PHR) and differ regarding their influence on overall user satisfaction (Berger et al., 1993; Gimpel et al., 2018; N Kano et al., 1984; Matzler et al., 1996). The relationship between the performance and importance of attractive and must-be qualities is nonlinear and asymmetric. For instance, some features might perform well but may not be evaluated as very important by users (Matzler et al., 2004).

Category	User expectations	Effect on user satisfaction	
		if implemented	if not implemented
Attractive quality (delighter)	Users do not expect the implementation of a feature	positive	none
One-dimensional quality (performance need)	Users explicitly demand the implementation of a feature	positive	negative
Must-be quality (basic need)	Users implicitly demand the implementation of a feature	none	negative
Indifferent quality	Users are indifferent to the implementation of a feature	none	none

Table 3.2-1: List of Kano model categories applied to the personal health record context

Furthermore, it is possible to identify the features that have the greatest influence on user satisfaction (Bailom et al., 1996). Thus, the Kano categories lead to a hierarchy of the features that a product (e.g., the PHR app) should contain: providers should fulfill all basic needs, be competitive in terms of performance needs, and offer selected attractive qualities that delight the user to differentiate themselves from competitors, (Berger et al., 1993).

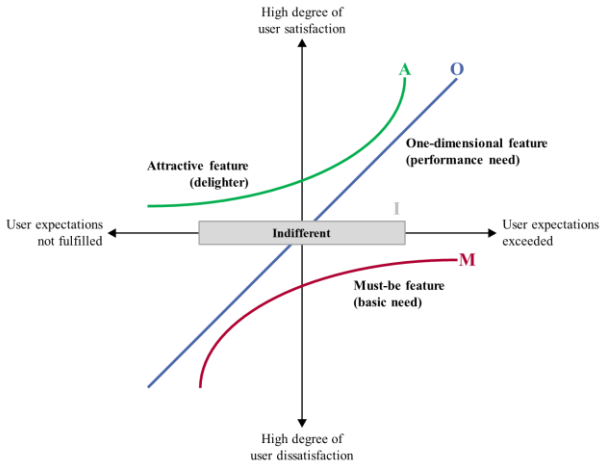


Figure 3.2-1: Illustration of the Kano model categories derived from Matzler et al. (1996) and applied to the personal health record context

According to Noriaki Kano (2001), the categories usually follow a specific lifecycle and change over time depending on the experiences or changes in user expectations (from indifferent to attractive to one-dimensional to must-be). New or unknown features should be classified as either indifferent or attractive because users could hardly form distinct expectation levels without substantial usage experience. After gaining more experience, features become part of the user expectations (i.e., one-dimensional) and are eventually recognized as must-be features (Noriaki Kano, 2001).

3.2.2.2 Features of personal health records influencing user satisfaction

Since the late 1990s, PHRs have concerned the research community (e.g., Iakovidis, 1998). They have received increased interest in recent years due to widespread technical capabilities, such as those enabled by smartphones, and their inherent promise to improve health outcomes (Cabitza et al., 2015; Dameff et al., 2019; Wickramasinghe, 2019). The literature has provided various PHR definitions (Roehrs et al., 2017; Tang et al., 2006; Zhou, Bao, Setiawan, et al., 2019). At its core, a PHR "can potentially store all the medical records for one patient across multiple health care networks and even countries" (Kao & Liebovitz, 2017, p. 112). The technical implementation can vary considerably, from USB sticks (Kim and Johnson 2002) and electronic health insurance cards (Pagliari et al., 2007) to web-based portals (Nazi et al., 2010) and smartphone apps (Kharrazi et al., 2012). Within this work, we relate PHRs solely to smartphone apps and follow the definition by D. A. Jones et al. (2010):

> "[PHRs are] a private, secure application through which an individual may access, manage, and share his or her health information. The PHR can include information

> that is entered by the consumer and/or data from other sources such as pharmacies, labs, and health care providers."

Previous PHR research can be grouped into different research streams, inter alia, PHR function evaluation, PHR adoption and attitudes, PHR privacy and security, and PHR architecture (Kaelber et al., 2008). Although Kaelber et al. (2008) emphasized the importance of PHR function evaluation, researchers have primarily focused on PHR adoption and attitudes (Abd-Alrazaq et al., 2019). However, the functions and data elements (i.e., features), are key components of a PHR (Kharrazi et al., 2012). Moreover, PHRs comprise several such features. Within this work, we focus on understanding the PHR feature evaluation.

To identify a comprehensive list of PHR features, we conducted a literature review covering five journals recommended by the Association for Information Systems Special Interest Group Information Technology in Healthcare due to their high relevance in the respective research domain (*Journal of the American Medical Informatics Association*, *International Journal of Medical Informatics*, *Journal of Medical Internet Research*, *Health Systems, and BMC Medical Informatics and Decision Making*). We decided to search specifically for the keywords *PHR Features* and identified 150 publications. Analyzing the titles and abstracts, we narrowed the list to a total of seven publications. Besides, we manually added three publications (Cabitza et al., 2015; Mendiola et al., 2015; Nazi et al., 2010) known to us from our prior research. Extracting the features mentioned in these ten publications resulted in a list of 109 features. Because all these features were derived from detailed feature overviews with large thematic overlaps, we decided not to expand the search string, as the expected knowledge gain would be marginal.

To consolidate the 109 features, we performed an interpretative categorizing analysis using the connecting strategy, which is commonly applied to process healthcare literature (Kerpedzhiev et al., 2019). The connecting strategy is used to identify homogeneous groups of objects and thus is beneficial in the case of several terms with similar meanings (Atkinson, 1992; Maxwell, 2009). Consequently, we merged identical features and pooled features covering similar aspects, and we removed features that were too specific (e.g., Mac-compatible). Subsequently, we refined the feature descriptions in various iterations until the author team reached a consensus.

During this process, it became clear that the feature description of *gamification* by Mendiola et al. (2015) is limited to rewards and does not cover the comparatively new phenomenon in its complexity (Deterding et al., 2011). Therefore, we decided to extend our first literature

review by explicitly searching for gamification features in the PHR context. As a result, we manually added three further gamification features (F24 to F26 in Table 2), covering other gamification aspects in PHRs (see Sardi et al., 2017). The resulting 26 PHR features are presented in Table 3.2-2.

Because the 26 features in this study cover various aspects of PHRs and because we further expect significant differences between potential users in Germany and Denmark, we hypothesize the following:

> **Hypothesis 1:** The effect of PHR features on the satisfaction of potential users follows a multi-categorial structure with features being categorized as basic needs (M), performance needs (O), delighters (A), indifferent (I), or reverse (R).

#	Name and description	References
F1	**Protected personal access.** The app is password protected and requires two-factor authentication (e.g., a code sent to the user's phone via a text message) for login.	Kharrazi et al. (2012); M. I. Kim and Johnson (2002); Maloney and Wright (2010)
F2	**Direct emergency access.** In case of emergency, authorized first aid providers can bypass security features to access medical data (e.g., a user's current medical condition and history).	Kharrazi et al. (2012); M. I. Kim and Johnson (2002); Maloney and Wright (2010)
F3	**Data encryption.** The app stores all data on the phone and servers in encrypted formats.	Halamka et al. (2008)
F4	**Health record.** The app can record personal (e.g., name and insurance number) and medical data (e.g., diagnoses, medications, and immunizations).	Archer et al. (2011); Cabitza et al. (2015); Davis et al. (2017); Dexheimer et al. (2019); Halamka et al. (2008); Kharrazi et al. (2012); M. I. Kim and Johnson (2002); Maloney and Wright (2010); Mendiola et al. (2015); Nazi et al. (2010)
F5	**Integration of other health-related records.** The app automatically integrates other health-related records, which allows the user to access his/her complete medical data (e.g., laboratory results, past and current treatments, and medications).	Archer et al. (2011); Cabitza et al. (2015); Davis et al. (2017); Dexheimer et al. (2019); Halamka et al. (2008); Kharrazi et al. (2012); M. I. Kim and Johnson (2002); Maloney and Wright (2010); Mendiola et al. (2015); Nazi et al. (2010)
F6	**Integration of trackers.** The user can integrate information from health and physical activity trackers (e.g., Apple Health, Fitbit, and Google Fit) for self-monitoring user-defined indicators (e.g., physical activity, calories, and weight).	Davis et al. (2017); Maloney and Wright (2010); Mendiola et al. (2015)
F7	**Manual upload.** The user can manually upload medical documentation (e.g., test results from private lab facilities), medical reports from specialists (e.g., dentists), and other documents regarding his/her health.	Archer et al. (2011); Cabitza et al. (2015); Davis et al. (2017); Kharrazi et al. (2012); Maloney and Wright (2010)
F8	**Consideration of health predispositions.** The user can import family-related data (e.g., genetic predispositions) from providers of such information (e.g., 23andMe and FamilyTreeDNA).	Archer et al. (2011); Dexheimer et al. (2019); Kharrazi et al. (2012); Nazi et al. (2010)
F9	**Health check/health diary.** The app can regularly query lifestyle-related user data (e.g., smoking and food calories or general wellbeing) and record this information for self-monitoring.	Archer et al. (2011); Dexheimer et al. (2019); Nazi et al. (2010)

#	Name and description	References
F10	**Sharing data with doctors.** The user can authorize doctors to access his/her data (e.g., to get a second opinion, to be referred, or to change to a new family physician more easily).	Cabitza et al. (2015); Davis et al. (2017); Dexheimer et al. (2019); Halamka et al. (2008); Maloney and Wright (2010); Mendiola et al. (2015)
F11	**Sharing data with peers.** The user can share his/her data with relatives and friends (e.g., to ask them for informal advice or to share information that could help them for their own health).	Cabitza et al. (2015); Davis et al. (2017); Dexheimer et al. (2019); Halamka et al. (2008); Maloney and Wright (2010); Mendiola et al. (2015)
F12	**Sharing data with organizations.** The user can authorize his/her insurance and other health-related organizations to access user data (e.g., for bill payment or to speed up reimbursement procedures).	Cabitza et al. (2015); Davis et al. (2017); Dexheimer et al. (2019); Maloney and Wright (2010); Mendiola et al. (2015); Nazi et al. (2010)
F13	**Communication with caregivers.** The app provides an integrated messaging system that enables direct interaction with caregivers (e.g., doctors).	Cabitza et al. (2015); Davis et al. (2017); Halamka et al. (2008); Nazi et al. (2010)
F14	**Community forum.** The app includes a forum that allows the user to ask health-related questions, share experiences, and read responses from other users with similar issues or caregivers.	Davis et al. (2017); Mendiola et al. (2015)
F15	**Social media.** The user can connect the app to social media platforms (e.g., Facebook and Twitter), allowing the user to communicate important health information and events with others.	Davis et al. (2017); Mendiola et al. (2015)
F16	**Health provider registry.** The app provides a searchable health provider registry to let the user know what caregivers and pharmacies are close geographically (e.g., based on geolocation services, such as Google maps).	Kharrazi et al. (2012); Nazi et al. (2010)
F17	**Booking appointments.** The user can book appointments through the app (e.g., ambulatory visits and hospital admissions).	Cabitza et al. (2015); Halamka et al. (2008)
F18	**Reminders.** The app offers automatic reminders and predetermined alerts (e.g., reminders for the ingestion of medicine or upcoming medical appointments).	Cabitza et al. (2015); Davis et al. (2017); Mendiola et al. (2015); Nazi et al. (2010)
F19	**Medication support.** The app offers automated medication support (e.g., by providing guidance regarding drug intolerances and known drug interactions).	Davis et al. (2017); Kharrazi et al. (2012); Mendiola et al. (2015); Nazi et al. (2010)
F20	**Care plan.** The app can provide the user with individual plans of action for reaching target goals, including specific, executable steps to guide the process (e.g., personal aftercare plan after a hospital stay).	Davis et al. (2017); Mendiola et al. (2015)
F21	**General education.** The app provides basic educational material about a disease or condition, including prevention through vaccines, causes, treatment, or management.	Davis et al. (2017); Mendiola et al. (2015); Nazi et al. (2010)
F22	**Virtual assistant.** The app includes a virtual assistant (e.g., an artificial intelligence-based chatbot), which provides personalized health information and guidance regarding preventive health recommendations and symptom analysis.	Archer et al. (2011); Davis et al. (2017); Dexheimer et al. (2019); Maloney and Wright (2010); Mendiola et al. (2015)
F23	**Health rewards.** The app rewards the user with points and badges as health objectives are achieved (e.g., for the undergoing of annual dental prophylaxis).	Mendiola et al. (2015)

#	Name and description	References
F24	**Motivational messages.** The app provides motivational messages (e.g., about the importance of preventive medical check-ups) to seek needed care.	Hors-Fraile et al. (2018); Kerns et al. (2013)
F25	**Challenges and quests.** The app provides health-related challenges and quests (e.g., to engage participation and thus address health topics more), which take place among users in a collaborative or single mode.	AlMarshedi et al. (2015); Hutchison et al. (2014); Lister et al. (2014); A. S. Miller et al. (2016)
F26	**Personalized avatars.** The app provides personalized avatars that represent the user and his/her current health status (e.g., to help the user visualize and better take charge of their health).	Borghese et al. (2013); Lentelink et al. (2013); Miloff et al. (2015)

Table 3.2-2: Features of personal health record apps

3.2.2.3 User characteristics influencing personal health record feature evaluation

Figure 3.2-2 displays the research model and hypotheses addressing the two research questions of this study. Next, we introduce the four user characteristics and hypothesize their influence on the PHR feature evaluation.

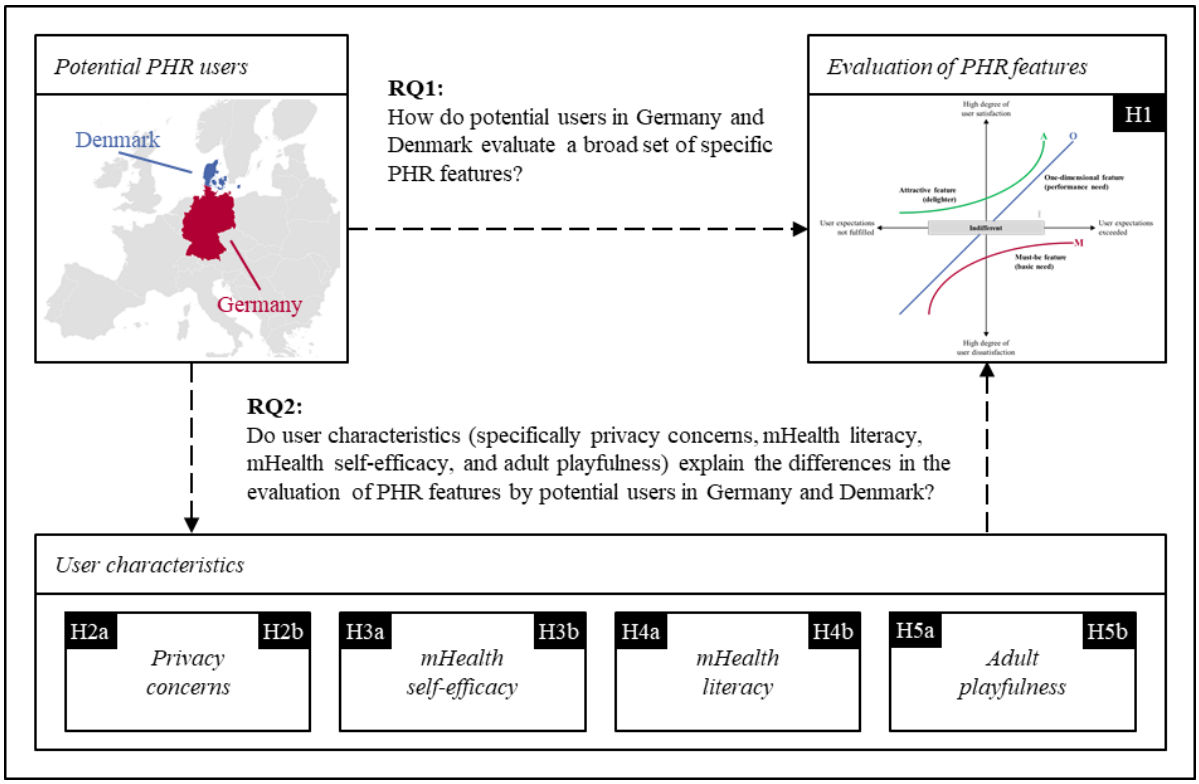


Figure 3.2-2: Research model

3.2.2.3.1 Privacy concerns

Privacy typically connotes something positive (Warren & Laslett, 1977) that must be protected or preserved (Margulis, 2003). This especially holds for personal medical data in a

digitalized world, as it is particularly sensitive and exposed to privacy incidents (J. G. Anderson, 2007; Appari & Johnson, 2010). Numerous publications have dealt with the role of privacy in digital health (e.g., C. L. Anderson & Agarwal, 2011; Angst & Agarwal, 2009; Winston et al., 2016).

Because privacy is a latent construct and thus cannot be measured directly, research often employs the concept of *privacy concerns* as a proxy for privacy (Y. Li, 2011; H. J. Smith et al., 1996; J. H. Smith et al., 2011). Privacy concerns are "the extent to which individuals are disturbed about the information collection practices of others [e.g., organizations] and how the acquired information will be used" (Angst & Agarwal, 2009, p. 342). Several studies have shown that Germans have higher privacy concerns than citizens in most other countries (e.g., Bellman et al., 2004; IBM, 1999; R. A. Miller, 2017). Most authors attribute this to German's historical legacy: in the 20th century, two regimes in Germany heavily surveilled their citizens to retain power (Whitman, 2004). Privacy concerns have become deeply engraved in the Germans' collective memory (Flaherty, 2014). Accordingly, we pose the following hypothesis:

Hypothesis 2a: Germans tend to have higher privacy concerns than Danes.

In healthcare digitalization, privacy concerns are one of the major barriers for individuals to accept and use healthcare technologies (J. G. Anderson, 2007). This applies especially to PHRs because they constitute a new way that personal health data are stored, shared, and processed by the multiple parties involved in the healthcare system (T. Li & Slee, 2014). Furthermore, previous research has suggested that safeguarding privacy increases individuals' satisfaction (e.g., George & Kumar, 2014; Khalaf Ahmad & Ali Al-Zu'bi, 2011; Nayeri & Aghajani, 2010). Because several PHR features are privacy-related (e.g., F1 or F3 in Table 3.2-2), require sensitive personal medical data (e.g., F8 or F19), or involve interfaces with other services (e.g., F6 or F12 in Table 3.2-2), we argue that privacy concerns affect user satisfaction regarding PHR features. Thus, we hypothesize the following:

Hypothesis 2b: Privacy concerns influence the evaluation of some PHR features.

3.2.2.3.2 mHealth literacy

Researchers have a growing interest in *mHealth literacy* due to the increasing use and acceptance of smartphones in health care (Birkhoff & Moriarty, 2020; Lin & Bautista, 2017; Messner et al., 2019). Although thematic overlaps exist between health literacy, eHealth literacy, and the comparatively new construct of mHealth literacy, researchers have argued that the constructs should be distinguished (Ahmed, 2017; Lin & Bautista, 2017; van der Vaart &

Drossaert, 2017). Following Lin and Bautista (2017), we define mHealth literacy as "the ability to use mobile devices to search, find, understand, appraise, and apply health information to address or solve a health problem" (p. 347).

Individuals mHealth literacy is context-dependent (Ćwiklicki et al., 2020; Messner et al., 2019) and can vary across countries (Okan et al., 2019). Researchers often underline the high digitalization level of health care in Denmark (e.g., Bertelsmann Stiftung, 2018; Kierkegaard, 2013) and the slow adoption of digital healthcare solutions in Germany (Nohl-Deryk et al., 2018). The overall level of mHealth literacy must align with digitalization because being literate about mHealth apps is one prerequisite for using them adequately (Kreps, 2017). Therefore, in line with previous research results (European Commission, 2014), we argue that Danes have a higher level of mHealth literacy than Germans. Conversely, we posit the following:

Hypothesis 3a: Germans tend to have lower mHealth literacy than Danes.

Inadequate literacy in health care (e.g., insufficient self-management skills and limited medication adherence) is associated with lower patient satisfaction (Altin & Stock, 2016; MacLeod et al., 2017). In contrast, Zhang et al. (2018) found that mHealth literacy significantly increases the satisfaction of mHealth apps users and attributes this relation to a better match of user expectations and experience. Most PHR features require a certain level of mHealth literacy to provide added value to users (e.g., F9, F18 in Table 3.2-2). Hence, a higher level of mHealth literacy may also lead to a higher level of user satisfaction and, thus, to a different evaluation of some of the PHR features. We pose the following hypothesis:

Hypothesis 3b: mHealth literacy influences the evaluation of some PHR features.

3.2.2.3.3 mHealth self-efficacy

Self-efficacy refers to individuals' confidence or belief in their ability to complete a task (Bandura, 1986). Furthermore, self-efficacy has a well-established, positive influence on the health status and health behavior of individuals of all ages (Grembowski et al., 1993). We follow Fox and Connolly (2018) and define mHealth self-efficacy as the "individuals' perceived ability to use m-health to manage their health" (p. 999).

Contrary to *literacy*, the efficacy judgment can over- or underestimate true ability. Thus, although self-efficacy usually correlates with literacy, it does not necessarily reflect actual literacy (Cheema & Skultety, 2017). Previous research has reported significant positive correlations between mHealth literacy and self-efficacy (e.g., Berens et al., 2018). Based on the close link between literacy and self-efficacy and based on prior work that found a lower level of

mHealth literacy for Germans compared to Danes (European Commission, 2014), we hypothesize the following:

Hypothesis 4a: Germans tend to have a lower mHealth self-efficacy than Danes.

Furthermore, empirical studies suggest a significant positive relationship between self-efficacy and satisfaction because self-efficacy improves task performance and increases users' perceived service value (e.g., Machmud, 2018; McKee et al., 2006). We assume that this relation also applies to mHealth self-efficacy and mHealth user satisfaction. Our list of PHR features contains several features (e.g., F7, F13, F17 in Table 3.2-2) for which users should demonstrate a certain level of mHealth self-efficacy to use them effectively. Accordingly, we posit the following hypothesis:

Hypothesis 4b: mHealth self-efficacy influences the evaluation of some PHR features.

3.2.2.3.4 Adult playfulness

Using gamification in mHealth apps is a relatively young and emerging trend (Schmidt-Kraepelin et al., 2020) that has the potential to promote behavioral health changes (A. S. Miller et al., 2016), to improve user self-management (Charlier et al., 2016), and to overcome a loss of interest and user engagement over time (Schmidt-Kraepelin et al., 2020). Several contemporary studies have applied various "game design elements in non-game contexts" (Deterding et al., 2011, p. 10), for example, in chronic disease rehabilitation (AlMarshedi et al., 2015) and mental health (Miloff et al., 2015). By analyzing 143 apps from the Apple App Store and the Google Play Store, Schmidt-Kraepelin et al. (2020) identify eight archetypes of gamification that are applied in mHealth apps (e.g., competition and collaboration, episodical compliance tracking, internal rewards for self-set goals). Previous research has shown that gamification can increase user satisfaction by fulfilling psychological needs, such as social relatedness (Sailer et al., 2017) and by increasing motivation or improving users' emotional experiences (Sardi et al., 2017).

Researchers frequently use *adult playfulness* to measure individuals' receptiveness to gamification elements (e.g., Codish & Ravid, 2015; Müller-Stewens et al., 2017; Poncin et al., 2017). According to Glynn and Webster (1992), adult playfulness is "an individual trait, a propensity to define (or redefine) an activity in an imaginative, nonserious or metaphoric manner so as to enhance intrinsic enjoyment, involvement, and satisfaction" (p. 85).

In the only available cross-country study on adult playfulness, Pang and Proyer (2018) concluded that societal rules and cultural factors might affect playfulness in a society. Anecdotal

evidence suggests the Danish culture is more liberal and progressive than many other cultures, including the German culture (Allen, 2012; Hoefler & Vejlgaard, 2011; Jensen, 2017). Cultural surveys reflect these libertarian values with comparably low values of power distance and high values of gender egalitarianism for Denmark and other Scandinavian countries (Hofstede Insights, 2020; House et al., 2011). Libertarian values may go along with higher playfulness among adults because liberal and progressive settings encourage play to a greater extent than conservative settings. Hence, despite limited prior evidence, we pose the following hypothesis:

Hypothesis 5a: Germans tend to have a lower adult playfulness than Danes.

Adult playfulness may influence the evaluation of PHR features. For example, our list of PHR features contains several gamification elements that can fulfill social relatedness (e.g., F14, F15) or increase user motivation (e.g., F24, F25 in Table 3.2-2). Gamification elements in mHealth apps may appeal more to those with higher adult playfulness and less to those with lower adult playfulness leading them to have greater preferences for these features. To conclude, we propose the following:

Hypothesis 5b: Adult playfulness influences the evaluation of some PHR features.

3.2.3 Research method

To address our research objective of evaluating PHR features by potential users from Germany and Denmark, we decided to use the Kano method[14], due to its ability to account for individual preferences regarding each PHR feature. We operationalized the four user characteristics (Figure 3.2-2) as factors based on the existing literature and conducted an online survey to test the theoretical hypotheses.

3.2.3.1 Kano method

The PHR features are classified depending on the users' answers to both a functional and a dysfunctional question (Berger et al., 1993; Gimpel et al., 2018; N Kano et al., 1984; Matzler et al., 1996). The functional question refers to the user's reaction if the respective feature is present, whereas the dysfunctional question refers to the reaction if the feature is not present. Each question has five possible answers (Figure 3.2-3). The combination of answers to these question pairs can be interpreted individually for each feature and leads to a specific category,

[14] The term *Kano method* refers to the procedure (i.e., the questioning technique) for categorizing features and for different evaluation rules. The term *Kano model* refers to the concept of customer satisfaction as presented in the previous chapter.

as illustrated in Figure 3.2-3. Hereby, the evaluation scheme is not appropriate to draw conclusions about the importance of individual features (see M. C. Lee and Newcomb (1997) for the design of an importance matrix based on the Kano questionnaire).

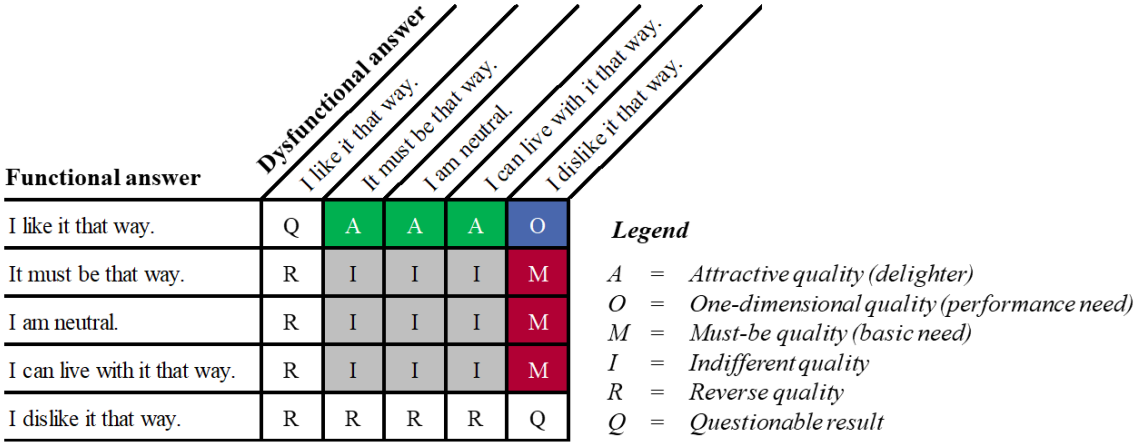


Figure 3.2-3: Evaluation scheme for the derivation of Kano categories

The most intuitive and easiest way to determine the resulting Kano model categorization of an attribute is the mode (Berger et al., 1993). However, solely using the mode leads to a lack of further information about other frequently appearing categorizations, especially if the shares of categories are of similar size (Schaule, 2014). Thus, further analyses are common and necessary to determine the categorization significance (Gimpel et al., 2018; Schaule, 2014).

M. C. Lee and Newcomb (1997) developed the variable category strength, which can be used to determine whether an attribute belongs to only one category. The category strength is calculated as the difference between the shares of the most and second-most frequently assigned categories. It may be considered statistically significant if it is equal to or greater than 6%; otherwise, the attribute belongs to a mixed category (M. C. Lee & Newcomb, 1997). The approach proposed by Fong (1996) supports a categorization if the category strength is higher than a calculated reference value that is based on the observed categorization frequencies and the overall sample size. If the categorization based on the mode is not supported by Fong's approach, Berger et al. (1993) proposed applying the (A, O, M) < > (I, R, Q) rule, where the categorizations are divided into two groups based on their (non)influence on user satisfaction. A categorization of A (attractive), O (one-dimensional), or M (must-be) means that an attribute influences user satisfaction. In contrast, a categorization of I (indifferent), R (reverse), or Q (questionable) indicates that an attribute has no (positive) influence on user satisfaction. The proposed evaluation rule is applicable if both the most and second-most categorizations

belong to different groups (e.g., A and I). Given the latter, the rule is executed by first determining the group with the highest share of categorizations of the overall sample and then selecting the most frequently chosen category within this group.

In the current work, we proceed in the same way as Gimpel et al. (2018) to determine the resulting categories of the features. Therefore, we assign categories to the features based on the mode if the category strength is significant at a 10% level, according to Fong's approach. If the respective category strength is not significant and the (A, O, M) < > (I, R, Q) rule is applicable, we execute this rule. If the (A, O, M) < > (I, R, Q) rule is not applicable, we assign the feature to a mixed category. In this case, we also name all categories that do not significantly differ according to Fong's approach compared to the most frequently chosen category.

3.2.3.2 Operationalization of user characteristics

We derived all four user characteristics (Figure 3.2-2) based on the existing literature and operationalized them on a seven-point Likert scale (1 = strongly disagree to 7 = strongly agree). The respective measures are provided in Appendix A.

To measure *privacy concerns* regarding personal health data, we used the 15-item scale from Angst and Agarwal (2009). Angst and Agarwal (2009) adapted one of the most influential scales to measure individuals' concerns for information privacy, originally developed and tested by Smith et al. (1996).

To operationalize mHealth literacy, we followed the approach by Lin and Bautista (2017). They used the widely adopted and comprehensively tested eight-item scale developed by Norman and Skinner (2006) and replaced the word computer with mobile phone. Lin and Bautista (2017) suggested that mHealth literacy is a higher-order construct including two mHealth factors: information searching (four items) and information appraisal (four items). Information searching comprises the skill to search for and find health-related information on a smartphone. In contrast, information appraisal covers the capability to understand, appraise, and apply health-related information on a smartphone. Given the inconsistency of the underlying factor structure across previous studies (Juvalta et al., 2020), we decided to test both operationalizations (single-factor and two-factor structures) and report the two-factor results.

For mHealth self-efficacy, we used the three-item scale from Fox and Connolly (2018). Fox and Connolly built on the work by J. Kim and Park (2012) on a measurement instrument consisting of six items.

We followed Proyer (2012) for adult playfulness and used the Short Measure of Adult Playfulness (SMAP). The SMAP consists of five items and is based on the need for a play scale (D. N. Jackson, 1974), the Adult Playfulness Scale (Glynn & Webster, 1992), and a list of playfulness qualities by Barnett (2007).

3.2.3.3 Survey

Before conducting the survey, four fellow researchers and six other voluntary participants pretested the English survey. Based on their feedback, we added further explanations and examples to the features' descriptions and divided the survey into three mandatory parts and one optional part.

In the first part, we presented screenshots of a fictional PHR app to give participants a basic impression of the potential PHR app. We put them into the situation of evaluating its features, similar to an app store site (see Figure 3.2-4 in Appendix B). In the second part, participants were asked one functional and one dysfunctional question for each of the 26 features. For example, for Feature F13 (Table 3.2-2), the functional question was as follows: "Communication with caregivers. The app provides an integrated messaging system that enables direct interaction with caregivers (e.g., doctors)." The dysfunctional question was as follows: "'Communication with caregivers' is not provided." The third part contained the scales for privacy concerns, mHealth literacy, mHealth self-efficacy, adult playfulness and the demographic data (gender, age, level of education, employment status, usage of healthcare-related apps, and understanding of the survey).

The optional part contained questions about the culturally influenced values and sentiments of the participants. We used this part to support the cultural representativeness of the sample regarding Germany and Denmark. As a measure, we used the Values Survey Module questions covering the six Hofstede dimensions (Hofstede et al., 2010).

The survey ran from February through March 2020. We recruited participants via social media and email and incentivized them through a lottery of vouchers for an online retailer. Overall, 323 participants from 27 different countries completed the survey. Given the focus on Denmark and Germany, we excluded 45 valid responses from other countries. Furthermore, we excluded six participants because they sped through the survey or stated difficulties in understanding the survey questions.

The final sample comprises 274 participants, including 215 Germans and 59 Danes. Both men (52%) and women (48%) completed the survey. The sample mostly consists of students (51%) and employees (46%). The age of participants was between 18 and 73 years (average age 28.9

years). Most participants (84%) indicated having at least a university degree). The majority of participants reported never using healthcare-related apps (45%) or using them less than once a month (27%). Table 3.2-11 (Appendix C) describes the composition of participants in both countries. Although the sample characteristics are similar in several parts, there may be a risk of bias due to the comparatively unbalanced sample size (Guyatt et al., 2011).

Out of the final sample, 208 participants (76%) completed the optional part, including 157 Germans and 51 Danes. Our assessment of the Hofstede dimensions (Table 3.2-12, Appendix C) reveals that the subsamples' cultural differences are qualitatively comparable with the differences between the original Hofstede values for Germany and Denmark (Hofstede Insights, 2020), indicating the cultural representativeness of the sample.

3.2.4 Results

This section first presents the overall evaluation of the 26 PHR features between Germans and Danes before testing the hypothesized differences in the user characteristics (H2a to H5a) and their influence on the feature evaluation (H2b to H5b).

3.2.4.1 Evaluation of personal health record features

Table 3.2-3 presents the categorization of PHR features according to the Kano model, split into the German and Danish subsamples. For both subsamples, we present the category strength and final categorization of each feature. The results indicate that the categorization of delighters (attractive quality) was assigned most frequently in both subsamples (Germany: 11; Denmark: 14), whereas the categorization of performance needs (one-dimensional quality) is very rare (Germany: 0; Denmark: 1). Furthermore, *protected personal access* (F1) and *data encryption* (F3) are considered by both Germans and Danes to be basic needs (must-be quality). Thus, the implementation of these security features is not rewarded, but downside risks exist if they are not implemented. Consequently, these two features should be implemented during the development of the PHR. This result is not unexpected, since data protection and high security standards are important issues regarding mobile applications in general (Jain & Shanbhag, 2012). This applies in particular to personal health data, which is among the most sensitive personal data (Martínez-Pérez et al., 2015; Müthing et al., 2019; Zhou, Bao, Watzlaf, & Parmanto, 2019). However, it should be emphasized that the resulting evaluation is neither a question of the clinical necessity of these two features, nor dependent of the type of technical implementation. The categorization as must-be qualities is solely based on the contribution of these two features to the personal satisfaction of potential users in Germany and Denmark. The survey participants categorized several features as indifferent (Germany: 10; Denmark:

4). Also, *social media* (F15) is considered to have a reverse quality in Germany, whereas Danes categorized no feature as having a negative effect on user satisfaction. Finally, for a few features, the categorization was not significant, and the features were assigned a mixed category (Germany: 2; Denmark: 5).

#	Short description	Germany (n = 215)		Denmark (n = 59)		Diff.
		Category strength	Category	Category strength	Category	
F1	Protected personal access	13% *	M	63% *	M	no
F2	Direct emergency access	5% ¹	A	2% ²	Mixed (A, O)	yes
F3	Data encryption	20% *	M	69% *	M	no
F4	Health record	8% *	I	20% *	O	yes
F5	Integration of other health-related records	5% ¹	A	8% ²	Mixed (O, A)	yes
F6	Integration of trackers	2% ¹	A	47% *	A	no
F7	Manual upload	7% ¹	A	3% ²	Mixed (A, O)	yes
F8	Consideration of health predispositions	24% *	I	27% *	A	yes
F9	Health check/health diary	22% *	I	47% *	A	yes
F10	Sharing data with doctors	8% *	A	2% ²	Mixed (A, O)	yes
F11	Sharing data with peers	3% ²	Mixed (I, R)	17% *	I	yes
F12	Sharing data with organizations	4% ²	Mixed (R, I)	36% *	A	yes
F13	Communication with caregivers	8% *	I	58% *	A	yes
F14	Community forum	15% *	I	36% *	A	yes
F15	Social media	56% *	R	2% ²	Mixed (R, I)	yes
F16	Health provider registry	22% *	A	64% *	A	no
F17	Booking appointments	29% *	A	63% *	A	no
F18	Reminders	10% *	A	68% *	A	no
F19	Medication support	5% ¹	A	53% *	A	no
F20	Care plan	8% *	A	47% *	A	no
F21	General education	11% *	A	49% *	A	no
F22	Virtual assistant	14% *	I	47% *	A	yes
F23	Health rewards	14% *	I	24% *	A	yes
F24	Motivational messages	19% *	I	3% ¹	I	no
F25	Challenges and quests	16% *	I	3% ¹	I	no
F26	Personalized avatars	30% *	I	2% ¹	I	no

Legend: * = Categorization according to Fong's approach
¹ = (O + A + M) < > (I + R + Q) rule applicable
² = (O + A + M) < > (I + R + Q) rule not applicable
A = Attractive quality (delighter)
O = One-dimensional quality (performance need)
M = Must-be quality (basic need)
I = Indifferent quality
R = Reverse quality

Table 3.2-3: Empirical results of the personal health record feature evaluation via the Kano model

Overall, 14 measures (54%) exhibit different categorizations between Germans and Danes. For five of these features, the categorization in one of the subsamples corresponds to the most frequent result of the mixed category categorization in the other subsample (F2, F7, F10, F11, and F15 in Table 3.2-2). Although these categorizations are not equal, the tendencies are more similar. We notice clear differences between Germany and Denmark for nine of the features. Most of these differences follow one of the two following patterns. First, features that are categorized as indifferent by Germans are frequently categorized as one-dimensional qualities

or delighters by Danes (F4, F8, F9, F13, F14, F22, and F23 in Table 2). Second, in some cases, features are categorized as delighters in Germany, whereas Danes categorized them ambiguously as performance needs and delighters (F2, F5, F7, and F10 in Table 2). The feature *sharing data with organizations* (F12) stands out in that most Germans categorized it as a reverse quality. Not only do they not want the feature, but they also do not expect this feature to be there, whereas Danes categorized the feature as a delighter.

We underline these results by examining the feature categorization in more detail on the participant level. For both Germans and Danes, Table 3.2-4 presents the minimum, mean, and maximum number of feature categorizations and the standard deviation per survey participant. Furthermore, Table 3.2-4 lists the share of participants who categorized none or at least nine (i.e., more than one-third) of the features as a specific Kano model category.

	Germans (n = 215)						Danes (n = 59)					
	Min[a]	Mean[a]	Max[a]	Sd[a]	None[b]	≥ 9[b]	Min[a]	Mean[a]	Max[a]	Sd[a]	None[b]	≥ 9[b]
Attractive quality	0	7.04	20	4.63	10%	37%	1	13.00	21	5.58	0%	81%
One-dimensional quality	0	3.17	17	3.18	17%	7%	0	3.03	11	2.32	3%	3%
Must-be quality	0	2.08	8	1.84	23%	0%	0	2.53	7	1.58	10%	0%
Indifferent quality	0	9.27	25	4.93	1%	50%	0	5.90	21	4.85	8%	20%
Reverse quality	0	4.40	24	3.98	11%	13%	0	1.54	10	2.27	44%	2%
Questionable result	0	0.06	3	0.30	96%	0%	0	0.00	0	0.00	100%	0%

[a] reference value: number of features; [b] reference value: number of survey participants

Table 3.2-4: Statistics regarding the number of Kano categories by survey participants

Overall, the data support hypothesis H1 for both the German and Danish subsamples. However, we also see clear differences between the German and Danish subsamples. The features with indifferent quality are dominant for German participants: every other German (50%) categorized at least 9 of the 26 features as having indifferent quality. In Denmark, this is only 1 in 5 (20%). Further, 81% of all Danish participants categorized at least nine features as delighters, compared to only 37% of Germans. The low proportion of questionable results in both subsamples indicates good data quality. In summary, several differences in the evaluation of features in Germany and Denmark were found, which we aim to explain in the next part based on certain user characteristics.

3.2.4.2 Explanatory power of user characteristics

We first evaluate the psychometric adequacy of the measurement model for user characteristics before we test the research hypotheses.

3.2.4.2.1 Measurement model assessment

To evaluate the psychometric adequacy, we conducted an exploratory factor analysis (EFA) with oblique rotation (reported in Table 3.2-9 in Appendix A). To assess the suitability of the sample data for the factor analysis, we calculated the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy (Kaiser, 1970) and Bartlett's test of sphericity (Bartlett, 1950). Both results (KMO: .83; Bartlett's test of sphericity: $p < .001$) indicated good prerequisites for the EFA. Via Horn's parallel analysis and assessment of interpretability, we determined the number of factors to extract as eight (Horn, 1965). Tabachnick and Fidell (2013, p. 651) suggested using oblique rotation when a high overlap exists in the variance (≥ 10%) of some oblique rotated factors.

Correlations that exceed the associated factor correlation threshold of .32 (Table 3.2-5) were in line with the theoretical conceptualization and well-established in the literature. First, we anticipated a strong link between all four first-order concerns for information privacy constructs (*collection*, *errors*, *unauthorized access*, and *secondary use*), as they are often aggregated into an overall score (H. J. Smith et al., 1996; Stewart & Segars, 2002). Second, we expected a strong correlation between the two factors of mHealth literacy (*mHealth information seeking* and *mHealth information appraisal*) because these factors are grounded in a single construct (Norman & Skinner, 2006).

Means, standard deviations, scale alphas, and inter-construct correlations are summarized in Table 3.2-5. Cronbach's alpha (≥ 0.80) suggests that all scales have convergent validity (Cronbach, 1951). Discriminant validity was confirmed using two assessments. First, indicators should load stronger on their corresponding construct than on other constructs in the model (Gefen & Straub, 2005). Further, items with factor loadings above .55 can be considered good (Comrey & Lee, 2016) and cross-loadings below .32 are negligible (Tabachnick & Fidell, 2013, p. 654). While all items loaded stronger on their corresponding construct and had good factor loading, one item (HIA1) had a cross-loading above the threshold of .32 and was dropped. Second, the square root of the average variance extracted (bold diagonal in Table 3.2-5) should be larger than the inter-construct correlations (Fornell & Larcker, 1981). Because both criteria were met, we conclude that the items and constructs exhibit adequate discriminant validity. Finally, we conducted a confirmatory factor analysis to evaluate the model fit of the eight-factor solution. Following the guidelines by D. L. Jackson et al. (2009), we calculated several fit measures (see Table 3.2-10 in Appendix A). The fit measures indicate a good model fit and support the eight-factor solution, initially derived by the EFA.

Construct	Mean	SD	Alpha	No. of items	1	2	3	4	5	6	7	8
1. Collection (privacy concerns)	3.99	1.55	0.90	4	**0.87**							
2. Errors (privacy concerns)	5.04	1.13	0.87	4	0.35***	**0.86**						
3. Unauthorized access (privacy concerns)	6.02	1.06	0.88	3	0.36***	0.65***	**0.90**					
4. Secondary use (privacy concerns)	6.34	0.89	0.80	4	0.36***	0.42***	0.71***	**0.80**				
5. mHealth information searching (mHealth literacy)	5.24	1.20	0.89	4	0.03	0.00	-0.01	-0.06	**0.87**			
6. mHealth information appraisal (mHealth literacy)	4.85	1.40	0.86	3	0.05	0.01	-0.01	-0.11	0.73***	**0.88**		
7. mHealth self-efficacy	5.62	1.27	0.87	3	-0.02	-0.02	-0.08	-0.06	0.21***	0.30***	**0.89**	
8. Adult playfulness	4.83	1.26	0.87	5	-0.01	-0.09	-0.12*	-0.04	0.12*	0.18**	0.18**	**0.82**

* $p < .05$; ** $p < .01$; *** $p < .001$; bold diagonals represent the square root of the average variance extracted for multi-item scales; product term is standardized; $N = 274$.

Table 3.2-5: Construct correlations and distributions

3.2.4.2.2 Influences on feature evaluation

To test the hypotheses, we first test whether significant differences exist in the user characteristics between Germans and Danes (H2a to H5a). Then we identify potential influences of the user characteristics on the evaluation of PHR features (H2b to H5b). For the first step, we applied the one-tailed Welch's *t*-test and the one-tailed Mann–Whitney U-test on the factor and sub-factor scores of the user characteristics. The means, standard deviations, and test results are summarized in Table 3.2-6.

User characteristics	Germany			Denmark		*t*-value	*W*-value	Hypothesis
	Mean	SD	Mean comp.	Mean	SD			
Privacy concerns[a]	5.44	0.77	≥	4.92	0.92	-3.83 ***	4,338 ***	H2a: Supported
Collection	3.96	1.53	≥	3.60	1.38	-2.01 *	5,342 *	
Errors	5.15	1.12	≥	4.56	1.06	-3.81 ***	4,342 ***	
Unauthorized access	6.21	0.84	≥	5.42	1.30	-3.88 ***	4,194 ***	
Secondary use	6.42	0.79	≥	6.10	1.16	-1.99 *	5,747	
mHealth literacy[b]	5.00	1.17	≤	5.43	1.01	2.54 **	7,436 *	H3a: Supported
mHealth information searching	5.22	1.19	≤	5.52	1.09	1.34	6,999	
mHealth information appraisal	4.77	1.42	≤	5.33	1.24	2.99 **	7,675 **	
mHealth self-efficacy	5.67	1.19	≤	6.18	0.85	3.96 ***	8,126 ***	H4a: Supported
Adult playfulness	4.72	1.20	≤	5.24	1.43	2.29 *	7,794 **	H5a: Supported

* $p < .05$; ** $p < .01$; *** $p < .001$; [a] average of the four first-order construct scores of collection, errors, unauthorized access, and secondary use; [b] average of the two first-order construct scores of mHealth information searching and mHealth information appraisal.

Table 3.2-6: Differences between Germany and Denmark regarding the potential influencing user characteristics

The data reveal significant factor-level differences between Germany and Denmark for all four user characteristics and, therefore, support the hypotheses (H2a to H5a). According to the data, Germans have significantly higher privacy concerns, lower mHealth literacy, lower mHealth self-efficacy, and lower adult playfulness than Danes.

To test the user characteristics' influences on the evaluation of PHR features (H2b to H5b), we followed a three-step approach. First, we subdivided the sample for each of the four user characteristics in three groups using a quartile-based sample-split approach. The first group (*low*) consists of participants that scored in the lower quartile of the respective characteristic. The second group (*middle*) includes participants from both the second and third quartiles jointly. The third group (*high*) comprises participants from the upper quartile of the respective variable. Second, we applied the Kano model to each subsample 12 times. Because the second research question focuses on differences in the PHR feature evaluation, we focus on these 14

features with ascertained differences between Germany and Denmark (see column Diff. in Table 3.2-3). Table 3.2-7 displays the different results regarding the feature *consideration of health predispositions* (F8) and the user characteristic *privacy concerns*. The table lists the relative share of chosen categories, category strength, and final categorization of the feature. Thus, this approach is appropriate for identifying evaluation differences between the different groups.

Quartile (*group*)	A	O	M	I	R	Q	Category strength	Category
1st (*low*)	46%	4%	3%	38%	8%	0%	8% [1]	A
2nd and 3rd (*middle*)	31%	7%	1%	49%	10%	1%	18% *	I
4th (*high*)	22%	1%	6%	49%	21%	0%	27% *	I

Legend: * = Categorization according to Fong's approach
[1] = (O + A + M) < > (I + R + Q) rule applicable
A = Attractive quality (delighter)
O = One-dimensional quality (performance need)
M = Must-be quality (basic need)
I = Indifferent quality
R = Reverse quality
Q = Questionable result

Table 3.2-7: Exemplary categorization of consideration of health predispositions (F8) for low, middle, and high privacy concerns

The complete categorization results of the 14 PHR features for the three groups and all four user characteristics are provided in Table 3.2-13 (Appendix D). Third, we compare the results for the low and high quartiles from the second step (Table 3.2-13, Appendix D) with the categorizations of Germans and Danes (Table 3.2-3) to explore similarities that can explain the categorization of a feature. To identify potential explanations, we use the grammar of the formal language theory (Harrison, 1978). This formalization assigns a mathematical meaning to the categorizations, which is useful for automated relationship verification. The following relationships apply:

$$\left[\{x_i^{Germany}\} \circ \{x_i^{Denmark}\} = \{y_i^{j,low}\} \circ \{y_i^{j,high}\}\right] \wedge \left[\bar{z}^{j,Germany} < \bar{z}^{j,Denmark}\right]$$
$$\longrightarrow potential\ explanation$$
$$\left[\{x_i^{Denmark}\} \circ \{x_i^{Germany}\} = \{y_i^{j,low}\} \circ \{y_i^{j,high}\}\right] \wedge \left[\bar{z}^{j,Germany} > \bar{z}^{j,Denmark}\right]$$
$$\longrightarrow potential\ explanation$$

where

x categorization of feature i in the respective country

y categorization of feature i in the respective subsample of user characteristic j

$\bar{z}$ the arithmetic mean of user characteristic j in the respective country

$x, y \in \{A, O, M, I, R, Q, Mixed()\}$

$z \in \mathbb{R}^+$

$i \in \{2,4,5,7,8,9,10,11,12,13,14,15,22,23\}$

$j \in$ *{privacy concerns, mHealth literacy, mHealth self-efficacy, adult playfulness}*

Table 3.2-8 presents the results. Potential identified explanations are labeled with ✓. Furthermore, identified similarities based on comparisons between mixed categories (e.g., $\{A\}\{Mixed(O, A)\} \approx \{A\}\{Mixed(O, A, I\})$ are labeled with (✓). A match is assumed if the first two categorizations between the mixed categories match. The following example refers to the feature *consideration of health predispositions* (F8) and illustrates the comparison procedure. According to Table 3.2-3, Germans evaluated F8 as an indifferent quality, whereas Danes evaluated F8 as a delighter. According to Table 3.2-13 (Appendix D), participants with low privacy concerns evaluated F8 as a delighter, whereas participants with high privacy concerns evaluated F8 as an indifferent quality. According to Table 3.2-6, the arithmetic mean of privacy concerns in Germany (5.44) is higher than in Denmark (4.92). Applying the algorithm results in $[\{A\}\{I\} = \{A\}\{I\}] \wedge [5.44 > 4.92]$. Thus, the comparison indicates a potential reason Germans evaluate F8 as indifferent and why Danes evaluated it as a delighter: specifically, because Germans are more privacy-sensitive while Danes are less privacy-sensitive.

The comparison for all features and subsamples demonstrates the explanatory power of all the user characteristics for 9 of the 14 differently evaluated features (F2, F5, F7, F8, F9, F11, F13, F15, and F22). Therefore, the results support the hypotheses regarding the influences of privacy concerns (H2b), mHealth literacy (H3b), mHealth self-efficacy (H4b), and adult playfulness (H5b) on the evaluation of *some* of the PHR features. For five of the features, explanations via at least two user characteristics (F2, F8, F9, F13, and F22) indicate that the influences are not mutually exclusive. However, the comparison does not yield explanatory results for all features, implying that further explanatory factors may influence different evaluations of PHR features in the two investigated countries.

#	Feature	Germany (n = 215)		Denmark (n = 59)			Potential explanatory user characteristics			
		Category strength	Category	Category strength	Category		Privacy Concerns	mHealth Literacy	mHealth Self-Efficacy	Adult Playfulness
F2	Direct emergency access	5% [1]	A	2% [2]	Mixed (A, O)				✓	(✓)
F4	Health record	8% *	I	20% *	O					
F5	Integration of other health-related records	5% [1]	A	8% [2]	Mixed (O, A)				(✓)	
F7	Manual upload	7% [1]	A	3% [2]	Mixed (A, O)				✓	
F8	Consideration of health predispositions	24% *	I	27% *	A		✓	✓		✓
F9	Health check/health diary	22% *	I	47% *	A		✓	✓	✓	✓
F10	Sharing data with doctors	8% *	A	2% [2]	Mixed (A, O)					
F11	Sharing data with peers	3% [2]	Mixed (I, R)	17% *	I			✓		
F12	Sharing data with organizations	4% [2]	Mixed (R, I)	36% *	A					
F13	Communication with caregivers	8% *	I	58% *	A		✓		✓	✓
F14	Community forum	15% *	I	36% *	A					
F15	Social media	56% *	R	2% [2]	Mixed (R, I)		✓			
F22	Virtual assistant	14% *	I	47% *	A			✓	✓	✓
F23	Health rewards	14% *	I	24% *	A					
						∑	4	4	6	5

Legend: * = Categorization according to Fong's approach
[1] = (O + A + M) < > (I + R + Q) rule applicable
[2] = (O + A + M) < > (I + R + Q) rule not applicable
A = Attractive quality (delighter)
O = One-dimensional quality (performance need)
M = Must-be quality (basic need)
I = Indifferent quality
R = Reverse quality

Table 3.2-8: Potential influences of user characteristics on the evaluation of features in Germany and Denmark

3.2.5 Discussion

This study was motivated by two questions regarding *how* users across different countries evaluate specific features of mHealth apps and *whether* individual user characteristics can explain potential differences in evaluating these features. To answer the research questions and test the developed hypotheses, we conducted an online survey in Germany and Denmark and used PHRs as a prominent example of mHealth apps.

To answer the first research question, we composed a current and comprehensive list of 26 PHR features based on extant literature in the research stream of PHR functionalities and features. Further, we analyzed the evaluation of these features by potential German and Danish users. Using the Kano method, we empirically captured users' perceptions of the PHR features as having an attractive, one-dimensional, must-be, indifferent, or reverse quality and found support for a multi-categorial structure of potential user satisfaction in both the German and Danish subsamples (H1). We found a nuanced situation where each of the different quality perceptions appears, and both cross-country similarities and differences exist.

To the best of our knowledge, our study is the first to include an evaluation of PHR features based on potential users' perceptions; thus, we contribute to the overall understanding of PHR user satisfaction. For both countries, we demonstrated that certain PHR features are evaluated differently, indicating differences between Germans and Danes. Our study contributes to the extant cross-country research of categorization results based on the Kano method, which has repeatedly found differences of product features in the evaluation across different countries (e.g., Basfirinci & Mitra, 2015; Bennur & Jin, 2013; Hejaili et al., 2009). Further, we identified two especially interesting patterns, as they support Kano's lifecycle theory (Noriaki Kano, 2001). Because Denmark already launched PHRs in 2003, whereas Germany has not yet done so, one might expect that the Danish assessment is more mature than the German assessment. However, given the differences in user characteristics that extend beyond healthcare (e.g., privacy concerns), we do not assume that the evaluation of PHR features from a German user's perspective would be identical to the current evaluation from a Danish user's perspective.

Addressing the second research question, we collected data on four user characteristics: privacy concerns, mHealth literacy, mHealth self-efficacy, and adult playfulness. We found support for the hypotheses regarding significant cross-country differences. Compared to Danes, Germans tend to have higher privacy concerns (H2a), lower mHealth literacy (H3a), lower mHealth self-efficacy (H4a), and lower adult playfulness (H5a). While the results of the first

three characteristics support the hypotheses, the significant difference regarding adult playfulness is revealing. It may be considered a complement to international adult playfulness and gamification research (Pang & Proyer, 2018).

Furthermore, we also present an approach to explain the differences in the feature evaluation with user characteristics. In this, we found support for the hypotheses concerning the explanatory power of user characteristics regarding feature evaluation, that is privacy concerns (H2b), mHealth literacy (H3b), mHealth self-efficacy (H4b), and adult playfulness (H5b) influence the evaluation of some PHR features. These cross-country differences in user characteristics may partly explain the cross-country differences in PHR feature evaluation for 9 out of 14 features with a cross-country difference. The extant literature applying the Kano method in health care (e.g., Materla et al., 2019) and other domains (e.g., Luor et al., 2015) focuses on the evaluation results without examining the underlying rationale behind the outcomes. Instead, this approach offers a new perspective of understanding differences in the evaluation and enriches the existing body of knowledge.

3.2.5.1 Theoretical contributions

This work offers two key theoretical contributions, one for mHealth and one for Kano research. First, by applying the Kano method to evaluate PHR features, the results explain the relationship between certain PHR features and user satisfaction, building a bridge between more technical, feature-oriented mHealth research and more behavioral user acceptance and marketing-oriented mHealth research. Although other researchers have repeatedly demanded the application of the Kano model within the healthcare domain in general (Materla et al., 2019) and the evaluation of PHRs in particular (Baird et al., 2011), prior literature has lacked adequate examination of PHRs or other mHealth apps in connection with the satisfaction of potential users. Our work provides the first empirical arguments regarding which features can satisfy potential PHR users in the future. This can be a starting point for investigating other types of mHealth apps.

Second, using theoretical arguments and empirical evidence on the explanatory power of user characteristics regarding differences in the feature evaluation of Germans and Danes, we provide a methodological augmentation of the Kano method that can be applied to explain potential subgroup differences. The gathered knowledge associated with these differences can provide a starting point for further conceptual developments of the Kano method. Future studies applying the Kano method could collect data on other pertinent user characteristics that may influence the evaluation of product features. Our work is the first step toward understanding

evaluation differences in the context of digitalized healthcare and, thus, may be used for the evaluation of other apps in health care and other domains.

3.2.5.2 Managerial implications

Our work provides implications for mHealth app developers and policymakers. First, our work offers an up-to-date overview of potential PHR features that app developers can use as a starting point. Second, we learned that these features contribute differently to the satisfaction of potential users. App developers could use user perceptions to elaborate on where to invest resources in the future. Third, the results indicate the explanatory power of user characteristics regarding the evaluation of such features. Therefore, internationally operating app providers should be aware of country-specific differences and provide customizability regarding their respective solutions' features.

Moreover, the results provide insight for policymakers. First, policymakers in Germany and Denmark could use user characteristics to educate their citizens or inform and consciously address potential users' fears. Striving for user satisfaction could be the first step to increase the currently low adoption and retention rates of mHealth solutions significantly. Second, our study indicates major differences between the user characteristics in Germany and Denmark. Therefore, European policymakers in the healthcare domain could consider these differences in future European legislation, for example, by updating the existing EU legal framework applicable to lifestyle and wellbeing apps.

3.2.5.3 Limitations

As in every research endeavor, our work has limitations. First, we focused solely on PHR as a major and potent yet single class of mHealth apps. Second, the literature review led to a comprehensive but not necessarily exhaustive set of PHR features. Other reviews and approaches might yield different features. Third, the set of PHR features was evaluated solely from a user's point of view. Unlike other researchers who chose a clinical point of view within their studies (Hankins et al., 2020; Jongerius et al., 2019), we did not examine the importance of single PHR features from a clinical or organizational perspective within our study. Furthermore, our user-centric study contributes only indirectly to the important field of mHealth app regulation that is discussed by several other authors due to the plethora of available mHealth apps (Larson, 2018; Rojas Mezarina et al., 2020). Fourth, we identified potential explanations for several differences in the feature evaluation based on user characteristics. However, some evaluation differences cannot be explained by the user characteristics covered in this study. There are likely other characteristics that we did not measure. For instance, users' general

experience of mHealth apps usage as well as other aspects such as time and support might be different in Germany and Denmark and could explain existing evaluation differences. Last, the empirical results' generalizability is limited, and the results should only be interpreted in a country- and user-specific manner. Although we cover a broad range of sociodemographic characteristics, including different ages, educational backgrounds, and employment states, the sample is not representative of Germany or Denmark. Although our chosen methodological approach provides the highest possible degree of validity and reliability, the risk of bias cannot be completely excluded, due to the comparatively unbalanced sample and the overall small sample size. Furthermore, because most participants were not experienced using mHealth apps, the results only account for user evaluations in the preadoption stage. Future surveys and analyses must be conducted to verify the validity of the conclusions for other countries and user groups.

3.2.5.4 Future research

Three promising directions for future research emerged from this work. First, due to the high speed of technological developments, future research could include new trends (e.g., augmentation or robotics in healthcare) and resulting features to have them evaluated in due course. An investigation of additional features could enrich the understanding of satisfaction drivers regarding PHRs. Second, we suggest expanding the scope of other potential explanatory user characteristics to increase future analyses' power. We covered four pertinent user characteristics, although more research is still to be done. One promising direction for further user characteristics might be users' general experience or exposure of mHealth apps usage or other influencing factors such as time and support. Additionally, this may also apply to non-covered user segments, as the sample data is not representative for Germany or Denmark. Finally, future research could focus on evaluating the general validity of our research in other countries, with other user groups, and other mHealth apps. More empirical research would help refine the identified influences of user characteristics and provide a better overall understanding of the relationships between user characteristics and the evaluation of PHR features. A first promising approach would be to focus on users that continually use PHRs or other mHealth apps.

3.2.6 Conclusion

This study contributes to mHealth research by providing two novel results. First, using PHRs as an example, the application of the Kano method implies that app features contribute differently to the satisfaction of potential mHealth app users. We determine different influences on

potential users' satisfaction across a comprehensive list of 26 features and differences in the general perception in two countries. Second, our empirical study demonstrates significant differences between Germany and Denmark for all four user characteristics tested within our research. We found that Germans tend to have higher privacy concerns, lower mHealth literacy, lower mHealth self-efficacy, and lower adult playfulness than Danes. Moreover, we found that these differences in user characteristics explain some of the differences in evaluating distinct features. Thus, this paper contributes to a better understanding of what constitutes and influences user satisfaction concerning potential mHealth app features. We hope our findings regarding feature evaluation and user characteristics' explanatory power stimulate further empirical studies on PHRs and other mHealth apps. Because this model implies application in two countries, it could be applied by global app providers in other countries to understand user needs better. Moreover, healthcare providers could apply the model when introducing or changing existing technical mHealth app solutions. Thus, our work may increase the adoption rates of existing and other promising mHealth solutions in the future.

References

Abd-Alrazaq, A. A., Bewick, B. M., Farragher, T., & Gardner, P. (2019). Factors that affect the use of electronic personal health records among patients: A systematic review. *International Journal of Medical Informatics*, *126*, 164–175. https://doi.org/10.1016/j.ijmedinf.2019.03.014

Ahmed, S. (2017). *mHealth literacy: characterizing people's ability to use smartphone-based health-related applications (Doctoral thesis).* University of Illinois. http://hdl.handle.net/2142/97267

Aitken, M., Clancy, B., & Nass, D. (2017). *The growing value of digital health: evidence and impact on human health and the healthcare system.* IQVIA Institute for Human Data Science. https://wwwhttps://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/the-growing-value-of-digital-health.pdf?_=1637506479822iqvia.com/insights/the-iqvia-institute/reports/the-growing-value-of-digital-health

Akter, S., D'Ambra, J., & Ray, P. (2010). Service quality of mHealth platforms: development and validation of a hierarchical model using PLS. *Electronic Markets*, *20*(3-4), 209–227. https://doi.org/10.1007/s12525-010-0043-x

Ali, E. E., Chew, L., & Yap, K. Y.-L. (2016). Evolution and current status of mhealth research: a systematic review. *BMJ Innovations*, *2*(1), 33–40. https://doi.org/10.1136/bmjinnov-2015-000096

Allen, J. K. (2012). *Icons of Danish modernity: Georg Brandes and Asta Nielsen*. University of Washington Press. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=607560

AlMarshedi, A., Wills, G. B., & Ranchhod, A. (2015). The Wheel of Sukr: A Framework for Gamifying Diabetes Self-Management in Saudi Arabia. *Procedia Computer Science*, *63*, 475–480. https://doi.org/10.1016/j.procs.2015.08.370

Altin, S. V., & Stock, S. (2016). The impact of health literacy, patient-centered communication and shared decision-making on patients' satisfaction with care received in German primary care practices. *BMC Health Services Research*, *16*, 450. https://doi.org/10.1186/s12913-016-1693-y

Anderson, C. L., & Agarwal, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Information Systems Research*, *22*(3), 469–490. https://doi.org/10.1287/isre.1100.0335

Anderson, J. G. (2007). Social, ethical and legal barriers to e-health. *International Journal of Medical Informatics*, *76*(5-6), 480–483. https://doi.org/10.1016/j.ijmedinf.2006.09.016

Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly*, *33*(2), 339–370. https://doi.org/10.2307/20650295

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279–314. https://doi.org/10.1504/IJIEM.2010.035624

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. A., & Straus, S. E. (2011). Personal health records: A scoping review. *Journal of the American Medical Informatics Association : JAMIA*, *18*(4), 515–522. https://doi.org/10.1136/amiajnl-2011-000105

Atkinson, P. (1992). The Ethnography of a Medical Setting: Reading, Writing, and Rhetoric. *Qualitative Health Research*, *2*(4), 451–474. https://doi.org/10.1177/104973239200200406

Bailom, F., Hinterhuber, H. J., Matzler, K., & Sauerwein, E. (1996). Das Kano-Modell der Kundenzufriedenheit. *Marketing ZFp*, *18*(2), 117–126.

Baird, A., North, F., & Raghu, T. S. (2011). Personal Health Records (PHR) and the future of the physician-patient relationship. In *Proceedings of the 2011 iConference* (pp. 281–288). ACM. https://doi.org/10.1145/1940761.1940800

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. *Prentice-Hall series in social learning theory*. Prentice-Hall.

Barnett, L. A. (2007). The nature of playfulness in young adults. *Personality and Individual Differences*, *43*(4), 949–958. https://doi.org/10.1016/j.paid.2007.02.018

Bartikowski, B., & Llosa, S. (2004). Customer satisfaction measurement: comparing four methods of attribute categorisations. *The Service Industries Journal*, *24*(4), 67–82. https://doi.org/10.1080/0264206042000275190

Bartlett, M. S. (1950). Tests of Significance in Factor Analysis. *British Journal of Statistical Psychology*, *3*(2), 77–85. https://doi.org/10.1111/j.2044-8317.1950.tb00285.x

Basfirinci, C., & Mitra, A. (2015). A cross cultural investigation of airlines service quality through integration of Servqual and the Kano model. *Journal of Air Transport Management*, *42*, 239–248. https://doi.org/10.1016/j.jairtraman.2014.11.005

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., & Carrasco, A. (2020). Assessment of the Fairness of Privacy Policies of Mobile Health Apps: Scale Development and Evaluation in Cancer Apps. *JMIR MHealth and UHealth*, *8*(7), e17134. https://doi.org/10.2196/17134

Bennur, S., & Jin, B. (2013). Cross-cultural investigation of US and Indian consumer's apparel attribute choices applying Kano's theory. *Journal of Fashion Marketing and Management: An International Journal*, *17*(3), 306–321. https://doi.org/10.1108/JFMM-03-2012-0007

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, *107*(2), 238–246. https://doi.org/10.1037/0033-2909.107.2.238

Berens, E. M., Vogt, D., Gille, S., & Schaeffer, D. (2018). The role of self-efficacy in the association between health literacy and self-perceived health in Germany. *European Journal of Public Health*, *28*(4). https://doi.org/10.1093/eurpub/cky213.070

Berger, C., Blauth, R., Boger, D., Bolster, C., Burchill, G., DuMouchel, W., Pouliot, F., Richter, R., Rubinoff, A., Shen, D., Timko, M., & Walden, D. (1993). Kano's Methods for Understanding Customer-defined Quality. *Center for Quality of Management Journal*, *2*(4), 3–36.

Bertelsmann Stiftung. (2018). *Smart Health Systems: International comparison of digital strategies*. Gütersloh, Germany.

Bhavnani, S. P., Narula, J., & Sengupta, P. P. (2016). Mobile technology and the digitization of healthcare. *European Heart Journal*, *37*(18), 1428–1438. https://doi.org/10.1093/eurheartj/ehv770

Bin Azhar, F. A., & Dhillon, J. S. (2016). A systematic review of factors influencing the effective use of mHealth apps for self-care. In *2016 3rd International Conference on Computer and Information Sciences (ICCOINS): A conference of World Engineering, Science & Technology Congress (ESTCON) : 15-17 August 2016, Kuala Lumpur Convention Centre : Proceedings* (pp. 191–196). IEEE. https://doi.org/10.1109/ICCOINS.2016.7783213

Birkhoff, S. D., & Moriarty, H. (2020). Challenges in mobile health app research: Strategies for interprofessional researchers. *Journal of Interprofessional Education & Practice*, *19*, 100325. https://doi.org/10.1016/j.xjep.2020.100325

Borghese, N. A., Mainetti, R., Pirovano, M., & Lanzi, P. L. (2013). An intelligent game engine for the at-home rehabilitation of stroke patients. In *IEEE 2nd International Conference on Serious Games and Applications for Health*, Vilamoura, Portugal.

Cabitza, F., Simone, C., & Michelis, G. de (2015). User-driven prioritization of features for a prospective InterPersonal Health Record: Perceptions from the Italian context. *Computers in Biology and Medicine*, *59*, 202–210. https://doi.org/10.1016/j.compbiomed.2014.03.009

Charlier, N., Zupancic, N., Fieuws, S., Denhaerynck, K., Zaman, B., & Moons, P. (2016). Serious games for improving knowledge and self-management in young people with chronic conditions: A systematic review and meta-analysis. *Journal of the American Medical Informatics Association : JAMIA*, *23*(1), 230–239. https://doi.org/10.1093/jamia/ocv100

Cheema, J. R., & Skultety, L. S. (2017). Self-efficacy and literacy: a paired difference approach to estimation of over-/under-confidence in mathematics- and science-related tasks. *Educational Psychology*, *37*(6), 652–665. https://doi.org/10.1080/01443410.2015.1127329

Codish, D., & Ravid, G. (2015). Detecting playfulness in educational gamification through behavior patterns. *IBM Journal of Research and Development*, *59*(6), 6:1-6:14. https://doi.org/10.1147/JRD.2015.2459651

Comrey, A. L., & Lee, H. B. (2016). *A first course in factor analysis* (Second edition). Psychology Press.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

Ćwiklicki, M., Schiavone, F., Klich, J., & Pilch, K. (2020). Antecedents of use of e-health services in Central Eastern Europe: A qualitative comparative analysis. *BMC Health Services Research*, *20*(1), 171. https://doi.org/10.1186/s12913-020-5034-9

Dameff, C., Clay, B., & Longhurst, C. A. (2019). Personal Health Records: More Promising in the Smartphone Era? *JAMA*, *321*(4), 339–340. https://doi.org/10.1001/jama.2018.20434

Davis, S., Roudsari, A., Raworth, R., Courtney, K. L., & MacKay, L. (2017). Shared decision-making using personal health record technology: A scoping review at the crossroads. *Journal of the American Medical Informatics Association : JAMIA*, *24*(4), 857–866. https://doi.org/10.1093/jamia/ocw172

Dehzad, F., Hilhorst, C., Bie, C. de, & Claassen, E. (2014). Adopting Health Apps, What's Hindering Doctors and Patients? *Health*, *6*(16), 2204–2217. https://doi.org/10.4236/health.2014.616256

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness. In A. Lugmayr, H. Franssila, C. Safran, & I. Hammouda (Eds.), *Proceedings of the 15th International Academic MindTrek Conference on Envisioning Future Media Environments* (pp. 9–15). ACM Press. https://doi.org/10.1145/2181037.2181040

Dexheimer, J. W., Greiner, M. V., Beal, S. J., Johnson, D., Kachelmeyer, A., & Vaughn, L. M. (2019). Sharing personal health record data elements in protective custody: Youth and stakeholder perspectives. *Journal of the American Medical Informatics Association : JAMIA*, *26*(8-9), 714–721. https://doi.org/10.1093/jamia/ocz067

European Commission. (2014). *European Citizens' Digital Health Literacy: Report*. https://ec.europa.eu/commfrontoffice/publicopinion/flash/fl_404_en.pdf

Fitte, C., Meier, P., Behne, A., Miftari, D., & Teuteberg, F. (2019). Die elektronische Gesundheitsakte als Vernetzungsinstrument im Internet of Health: Anwendungsfälle und Anbieter im deutschen Gesundheitswesen. In D. Klaus, K. Geihs, M. Lange, & G. Stumme (Eds.), *INFORMATIK 2019: Konferenzbeiträge der 49. Jahrestagung der Gesellschaft für Informatik* (pp. 111–124). https://doi.org/10.18420/INF2019_17

Flaherty, D. H. (2014). *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. UNC Press.

Fong, D. (1996). Using the self-stated importance questionnaire to interpret Kano questionnaire results. *Center for Quality Management Journal*, *5*(3), 21–24.

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

Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal*, *28*(6), 995–1019. https://doi.org/10.1111/isj.12179

Füller, J., & Matzler, K. (2008). Customer delight and market segmentation: An application of the three-factor theory of customer satisfaction on life style groups. *Tourism Management*, *29*(1), 116–126. https://doi.org/10.1016/j.tourman.2007.03.021

Gefen, D., & Straub, D. (2005). A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example. *Communications of the Association for Information Systems*, *16*, 91–109. https://doi.org/10.17705/1CAIS.01605

George, A., & Kumar, G. S. G. (2014). Impact of service quality dimensions in internet banking on customer satisfaction. *DECISION*, *41*(1), 73–85. https://doi.org/10.1007/s40622-014-0028-2

Gherardi, S., Østerlund, C., & Kensing, F. (2014). Editorial. *Information Technology & People*, *27*(4). https://doi.org/10.1108/ITP-09-2014-0193

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2018). The upside of data privacy – delighting customers by implementing data privacy measures. *Electronic Markets*, *28*(4), 437–452. https://doi.org/10.1007/s12525-018-0296-3

Glynn, M. A., & Webster, J. (1992). The Adult Playfulness Scale: An Initial Assessment. *Psychological Reports*, *71*(1), 83–103. https://doi.org/10.2466/pr0.1992.71.1.83

Grembowski, D., Patrick, D., Diehr, P., Durham, M., Beresford, S., Kay, E., & Hecht, J. (1993). Self-Efficacy and Health Behavior Among Older Adults. *Journal of Health and Social Behavior*, *34*(2), 89–104. https://doi.org/10.2307/2137237

Gronholdt, L., Martensen, A., & Kristensen, K. (2000). The relationship between customer satisfaction and loyalty: Cross-industry differences. *Total Quality Management*, *11*(4-6), 509–514. https://doi.org/10.1080/09544120050007823

Guyatt, G. H., Oxman, A. D., Vist, G., Kunz, R., Brozek, J., Alonso-Coello, P., Montori, V., Akl, E. A., Djulbegovic, B., Falck-Ytter, Y., Norris, S. L., Williams, J. W., Atkins, D., Meerpohl, J., & Schünemann, H. J. (2011). Grade guidelines: 4. Rating the quality of evidence—study limitations (risk of bias). *Journal of Clinical Epidemiology*, *64*(4), 407–415. https://doi.org/10.1016/j.jclinepi.2010.07.017

Halamka, J. D., Mandl, K. D., & Tang, P. C. (2008). Early experiences with personal health records. *Journal of the American Medical Informatics Association : JAMIA*, *15*(1), 1–7. https://doi.org/10.1197/jamia.M2562

Hankins, J. S., Shah, N., DiMartino, L., Brambilla, D., Fernandez, M. E., Gibson, R. W., Gordeuk, V. R., Lottenberg, R., Kutlar, A., Melvin, C., Simon, J., Wun, T., Treadwell, M., Calhoun, C., Baumann, A., Potter, M. B., Klesges, L., & Bosworth, H. (2020). Integration of Mobile Health Into Sickle Cell Disease Care to Increase Hydroxyurea Utilization: Protocol for an Efficacy and Implementation Study. *JMIR Research Protocols*, *9*(7), e16319. https://doi.org/10.2196/16319

Harrison, M. A. (1978). *Introduction to formal language theory*. *Addison-Wesley series in computer science*. Addison-Wesley Publ. Co.

Hejaili, F. F., Assad, L., Shaheen, F. A., Moussa, D. H., Karkar, A., AlRukhaimi, M., Barhamein, M., Al Suwida, A., Al Alhejaili, F. F., Al Harbi, A. S., Al Homrany, M., Attar, B., & Al-Sayyari, A. A. (2009). Culture-related service expectations: A comparative study using the Kano model. *Quality Management in Health Care*, *18*(1), 48–58. https://doi.org/10.1097/01.QMH.0000344593.40886.b5

Helmer, A., Lipprandt, M., Frenken, T., Eichelberg, M., & Hein, A. (2011). Empowering Patients through Personal Health Records: A Survey of Existing Third-Party Web-Based PHR Products. *Electronic Journal of Health Informatics*, *6*(3), e26.

Hoefler, J. M., & Vejlgaard, T. B. (2011). Something's ironic in Denmark: An otherwise progressive welfare state lags well behind in care of patients at the end of life. *Health Policy*, *103*(2-3), 297–304. https://doi.org/10.1016/j.healthpol.2010.11.012

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind ; intercultural cooperation and its importance for survival* (Revised and expanded 3rd edition). McGraw-Hill.

Hofstede, G., Hofstede, G. J., Minkov, M., & Vinken, H. (2013). *Values survey module 2013*. https://geerthofstede.com/research-and-vsm/vsm-2013/

Hofstede Insights. (2020). *Country Comparison: Denmark, Germany*. https://www.hofstede-insights.com/country-comparison/denmark,germany/

Hölzing, J. A. (2008). *Die Kano-Theorie der Kundenzufriedenheitsmessung: Eine theoretische und empirische Überprüfung*. Zugl.: Mannheim, Univ., Diss., 2007 (1. Aufl.). *Gabler Edition Wissenschaft*. Gabler Verlag / GWV Fachverlage GmbH Wiesbaden. http://gbv.eblib.com/patron/FullRecord.aspx?p=749291 https://doi.org/10.1007/978-3-8349-9864-4

Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. *Psychometrika*, *30*, 179–185. https://doi.org/10.1007/BF02289447

Hors-Fraile, S., Schneider, F., Fernandez-Luque, L., Luna-Perejon, F., Civit, A., Spachos, D., Bamidis, P., & Vries, H. de (2018). Tailoring motivational health messages for smoking cessation using an mHealth recommender system integrated with an electronic health record: A study protocol. *BMC Public Health*, *18*(1), 698. https://doi.org/10.1186/s12889-018-5612-5

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (Eds.). (2011). *Culture, leadership, and organizations: The GLOBE study of 62 societies*. Sage publications.

Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J. M., Kobsa, A., Mattern, F., Mitchell, J. C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Terzopoulos, D., Tygar, D., Weikum, G., & Marcus, A. (Eds.). (2014). *Lecture notes in computer science*. *Design, User Experience, and Usability. User Experience Design for Diverse Interaction Platforms and Environments*. Springer International Publishing. https://doi.org/10.1007/978-3-319-07626-3

Iakovidis, I. (1998). Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe. *International Journal of Medical Informatics, 52*(1-3), 105–115. https://doi.org/10.1016/S1386-5056(98)00129-4

IBM. (1999). *IBM Multi-National Consumer Privacy Survey: A comprehensive and comparative look at consumers in the United States, Germany, and United Kingdom and their attitudes toward privacy in everyday business transactions.* ftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf

Jackson, D. L., Gillaspy, J. A., & Purc-Stephenson, R. (2009). Reporting practices in confirmatory factor analysis: An overview and some recommendations. *Psychological Methods, 14*(1), 6–23. https://doi.org/10.1037/a0014694

Jackson, D. N. (1974). *Personality research form manual*. research psychologists press.

Jain, A. K., & Shanbhag, D. (2012). Addressing Security and Privacy Risks in Mobile Applications. *IT Professional, 14*(5), 28–33. https://doi.org/10.1109/MITP.2012.72

Jensen, D. M. N. (2017). *The Denmark Canon in a Tourism Perspective*. http://projekter.aau.dk/projekter/files/260346776/The_Denmark_Canon__In_a_Tourism_Perspective_.pdf

Jimenez, G., Lum, E., & Car, J. (2019). Examining Diabetes Management Apps Recommended From a Google Search: Content Analysis. *JMIR MHealth and UHealth, 7*(1), e11848. https://doi.org/10.2196/11848

Jones, C., O'Toole, K., Jones, K., & Brémault-Phillips, S. (2020). Quality of Psychoeducational Apps for Military Members With Mild Traumatic Brain Injury: An Evaluation Utilizing the Mobile Application Rating Scale. *JMIR MHealth and UHealth, 8*(8), e19807. https://doi.org/10.2196/19807

Jones, D. A., Shipman, J. P., Plaut, D. A., & Selden, C. R. (2010). Characteristics of personal health records: Findings of the Medical Library Association/National Library of Medicine Joint Electronic Personal Health Record Task Force. *Journal of the Medical Library Association : JMLA*, *98*(3), 243–249. https://doi.org/10.3163/1536-5050.98.3.013

Jongerius, C., Russo, S., Mazzocco, K., & Pravettoni, G. (2019). Research-Tested Mobile Apps for Breast Cancer Care: Systematic Review. *JMIR MHealth and UHealth*, *7*(2), e10930. https://doi.org/10.2196/10930

Jöreskog, K. G., & Sörbom, D. (1986). *LISREL VI: Analysis of linear structural relationships by maximum likelihood, instrumental variables, and least squares methods*. Scientific Software.

Juvalta, S., Kerry, M. J., Jaks, R., Baumann, I., & Dratva, J. (2020). Electronic Health Literacy in Swiss-German Parents: Cross-Sectional Study of eHealth Literacy Scale Unidimensionality. *Journal of Medical Internet Research*, *22*(3), e14492. https://doi.org/10.2196/14492

Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association : JAMIA*, *15*(6), 729–736. https://doi.org/10.1197/jamia.M2547

Kaiser, H. F. (1970). A second generation little jiffy. *Psychometrika*, *35*(4), 401–415. https://doi.org/10.1007/BF02291817

Kano, N [N], Seraku, N., & Tsuji, F. (1984). Attractive quality and must-be quality. *The Journal of Japanese Society for Quality Control*, *14*(2), 39–48.

Kano, N [Noriaki]. (2001). Life cycle and creation of attractive quality. In *4th International QMOD Quality Management and Organisational Development Conference* (pp. 12–14).

Kao, C.-K., & Liebovitz, D. M. (2017). Consumer Mobile Health Apps: Current State, Barriers, and Future Directions. *PM & R*, *9*(5), S106-S115. https://doi.org/10.1016/j.pmrj.2017.02.018

Kerns, J. W., Krist, A. H., Longo, D. R., Kuzel, A. J., & Woolf, S. H. (2013). How patients want to engage with their personal health record: A qualitative study. *BMJ Open*, *3*(7), e002931. https://doi.org/10.1136/bmjopen-2013-002931

Kerpedzhiev, G., Manner-Romberg, T., Meindl, O., & Regal, C. (2019). Towards a Maturity Model: Bed Management Capabilities in Hospitals. In *Proceedings of the 27th European Conference on Information Systems* (pp. 1–17).

Khalaf Ahmad, A. M., & Ali Al-Zu'bi, H. (2011). E-banking Functionality and Outcomes of Customer Satisfaction: An Empirical Investigation. *International Journal of Marketing Studies*, *3*(1). https://doi.org/10.5539/ijms.v3n1p50

Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: An evaluation of features and functionality. *International Journal of Medical Informatics*, *81*(9), 579–593. https://doi.org/10.1016/j.ijmedinf.2012.04.007

Kierkegaard, P. (2013). Ehealth in Denmark: A case study. *Journal of Medical Systems*, *37*(6), 9991. https://doi.org/10.1007/s10916-013-9991-y

Kim, J., & Park, H.-A. (2012). Development of a health information technology acceptance model using consumers' health behavior intention. *Journal of Medical Internet Research*, *14*(5), e133. https://doi.org/10.2196/jmir.2143

Kim, M. I., & Johnson, K. B. (2002). Personal health records: Evaluation of functionality and utility. *Journal of the American Medical Informatics Association : JAMIA*, *9*(2), 171–180. https://doi.org/10.1197/jamia.m0978

Knöppler, K., Neisecke, T., & Nölke, L. (2016). *Digital-Health-Anwendungen für Bürger: Kontext, Typologie und Relevanz aus Public-Health-Perspektive* [Entwicklung und Erprobung eines Klassifikationsverfahrens]. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Studie_VV_Digital-Health-Anwendungen_2016.pdf

Korte, E. M. de, Wiezer, N., Janssen, J. H., Vink, P., & Kraaij, W. (2018). Evaluating an mHealth App for Health and Well-Being at Work: Mixed-Method Qualitative Study. *JMIR MHealth and UHealth*, *6*(3), e72. https://doi.org/10.2196/mhealth.6335

Kreps, G. L. (2017). The Relevance of Health Literacy to mHealth. *Studies in Health Technology and Informatics*, *240*, 347–355.

La Torre Díez, I. de, Garcia-Zapirain, B., López-Coronado, M., Rodrigues, J. J. P. C., & Del Pozo Vegas, C. (2017). A New mHealth App for Monitoring and Awareness of Healthy Eating: Development and User Evaluation by Spanish Users. *Journal of Medical Systems*, *41*(7), 109. https://doi.org/10.1007/s10916-017-0753-0

Ladhari, R. (2009). A review of twenty years of SERVQUAL research. *International Journal of Quality and Service Sciences*, *1*(2), 172–198. https://doi.org/10.1108/17566690910971445

Larson, R. S. (2018). A Path to Better-Quality mHealth Apps. *JMIR MHealth and UHealth*, *6*(7), e10414. https://doi.org/10.2196/10414

Lee, M. C., & Newcomb, J. F. (1997). Applying the Kano Methodology to Meet Customer Requirements: NASA's Microgravity Science Program. *Quality Management Journal*, *4*(3), 95–106. https://doi.org/10.1080/10686967.1997.11918805

Lee, R. A., & Jung, M. E. (2018). Evaluation of an mHealth App (DeStressify) on University Students' Mental Health: Pilot Trial. *JMIR Mental Health*, *5*(1), e2. https://doi.org/10.2196/mental.8324

Lentelink, S. J., Spil, A., Broens, T., Hermens, H. J., & Jones, V. M. (2013). Healthy weight game! Lose weight together. In *IEEE 2nd International Conference on Serious Games and Applications for Health,* Vilamoura, Portugal.

Li, T., & Slee, T. (2014). The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology*, *65*(8), 1541–1554. https://doi.org/10.1002/asi.23068

Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, *28*, 453–496. https://doi.org/10.17705/1CAIS.02828

Lin, T. T. C., & Bautista, J. R. (2017). Understanding the Relationships between mHealth Apps' Characteristics, Trialability, and mHealth Literacy. *Journal of Health Communication*, *22*(4), 346–354. https://doi.org/10.1080/10810730.2017.1296508

Lister, C., West, J. H., Cannon, B., Sax, T., & Brodegard, D. (2014). Just a fad? Gamification in health and fitness apps. *JMIR Serious Games*, *2*(2), e9. https://doi.org/10.2196/games.3413

Löfgren, M., & Witell, L. (2008). Two Decades of Using Kano's Theory of Attractive Quality: A Literature Review. *Quality Management Journal*, *15*(1), 59–75. https://doi.org/10.1080/10686967.2008.11918056

Luor, T., Lu, H.-P., Chien, K.-M., & Wu, T.-C. (2015). Contribution to quality research: a literature review of Kano's model from 1998 to 2012. *Total Quality Management & Business Excellence*, *26*(3-4), 234–247. https://doi.org/10.1080/14783363.2012.733264

Lusignan, S. de, Ross, P., Shifrin, M., Hercigonja-Szekeres, M., & Seroussi, B. (2013). A comparison of approaches to providing patients access to summary care records across old and new europe: An exploration of facilitators and barriers to implementation. *Studies in Health Technology and Informatics*, *192*, 397–401. https://doi.org/10.3233/978-1-61499-289-9-397

Machmud, S. (2018). The Influence of Self-Efficacy on Satisfaction and Work-Related Performance. *The International Journal of Management and Business Administration*, *4*(4), 43–47. https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.44.1005

MacLeod, S., Musich, S., Gulyas, S., Cheng, Y., Tkatch, R., Cempellin, D., Bhattarai, G. R., Hawkins, K., & Yeh, C. S. (2017). The impact of inadequate health literacy on patient satisfaction, healthcare utilization, and expenditures among older adults. *Geriatric Nursing (New York, N.Y.)*, *38*(4), 334–341. https://doi.org/10.1016/j.gerinurse.2016.12.003

Maloney, F. L., & Wright, A. (2010). Usb-based Personal Health Records: An analysis of features and functionality. *International Journal of Medical Informatics*, *79*(2), 97–111. https://doi.org/10.1016/j.ijmedinf.2009.11.005

Mani, M., Kavanagh, D. J., Hides, L., & Stoyanov, S. R. (2015). Review and Evaluation of Mindfulness-Based iPhone Apps. *JMIR MHealth and UHealth*, *3*(3), e82. https://doi.org/10.2196/mhealth.4328

Marent, B., Henwood, F., & Darking, M. (2018). Development of an mHealth platform for HIV Care: Gathering User Perspectives Through Co-Design Workshops and Interviews. *JMIR MHealth and UHealth*, *6*(10), e184. https://doi.org/10.2196/mhealth.9856

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

Martínez-Pérez, B., La Torre-Díez, I. de, & López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems*, *39*(1), 181. https://doi.org/10.1007/s10916-014-0181-3

Materla, T., Cudney, E. A., & Antony, J. (2019). The application of Kano model in the healthcare industry: a systematic literature review. *Total Quality Management & Business Excellence*, *30*(5-6), 660–681. https://doi.org/10.1080/14783363.2017.1328980

Matzler, K., Bailom, F., Hinterhuber, H. H., Renzl, B., & Pichler, J. (2004). The asymmetric relationship between attribute-level performance and overall customer satisfaction: a reconsideration of the importance–performance analysis. *Industrial Marketing Management*, *33*(4), 271–277. https://doi.org/10.1016/S0019-8501(03)00055-5

Matzler, K., Hinterhuber, H. H., Bailom, F., & Sauerwein, E. (1996). How to delight your customers. *Journal of Product & Brand Management*, *5*(2), 6–18. https://doi.org/10.1108/10610429610119469

Maxwell, J. (2009). Designing a Qualitative Study. In D. J. Rog & L. Bickman (Eds.), *The SAGE handbook of applied social research methods* (2nd ed., pp. 214–253). SAGE. https://doi.org/10.4135/9781483348858.n7

McKee, D., Simmers, C. S., & Licata, J. (2006). Customer Self-Efficacy and Response to Service. *Journal of Service Research*, *8*(3), 207–220. https://doi.org/10.1177/1094670505282167

Melin, J., Bonn, S. E., Pendrill, L., & Trolle Lagerros, Y. (2020). A Questionnaire for Assessing User Satisfaction With Mobile Health Apps: Development Using Rasch Measurement Theory. *JMIR MHealth and UHealth*, *8*(5), e15909. https://doi.org/10.2196/15909

Mendiola, M. F., Kalnicki, M., & Lindenauer, S. (2015). Valuable features in mobile health apps for patients and consumers: Content analysis of apps and user ratings. *JMIR MHealth and UHealth*, *3*(2), e40. https://doi.org/10.2196/mhealth.4283

Messner, E.-M., Probst, T., O'Rourke, T., Stoyanov, S., & Baumeister, H. (2019). mHealth Applications: Potentials, Limitations, Current Quality and Future Directions. In H. Baumeister & C. Montag (Eds.), *Studies in Neuroscience, Psychology and Behavioral Economics. Digital Phenotyping and Mobile Sensing* (Vol. 3, pp. 235–248). Springer International Publishing. https://doi.org/10.1007/978-3-030-31620-4_15

Miller, A. S., Cafazzo, J. A., & Seto, E. (2016). A game plan: Gamification design principles in mHealth applications for chronic disease management. *Health Informatics Journal*, *22*(2), 184–193. https://doi.org/10.1177/1460458214537511

Miller, R. A. (Ed.). (2017). *Privacy and power: A transatlantic dialogue in the shadow of the NSA-Affair*. Cambridge University Press. https://doi.org/10.1017/CBO9781316658888sc

Miloff, A., Marklund, A., & Carlbring, P. (2015). The challenger app for social anxiety disorder: New advances in mobile psychological treatment. *Internet Interventions*, *2*(4), 382–391. https://doi.org/10.1016/j.invent.2015.08.001

Müller-Stewens, J., Schlager, T., Häubl, G., & Herrmann, A. (2017). Gamified Information Presentation and Consumer Adoption of Product Innovations. *Journal of Marketing*, *81*(2), 8–24. https://doi.org/10.1509/jm.15.0396

Müthing, J., Brüngel, R., & Friedrich, C. M. (2019). Server-Focused Security Assessment of Mobile Health Apps for Popular Mobile Platforms. *Journal of Medical Internet Research*, *21*(1), e9818. https://doi.org/10.2196/jmir.9818

Nayeri, N. D., & Aghajani, M. (2010). Patients' privacy and satisfaction in the emergency department: A descriptive analytical study. *Nursing Ethics*, *17*(2), 167–177. https://doi.org/10.1177/0969733009355377

Nazi, K. M., Hogan, T. P., Wagner, T. H., McInnes, D. K., Smith, B. M., Haggstrom, D., Chumbler, N. R., Gifford, A. L., Charters, K. G., Saleem, J. J., Weingardt, K. R., Fischetti, L. F., & Weaver, F. M. (2010). Embracing a health services research perspective on personal health records: Lessons learned from the VA My HealtheVet system. *Journal of General Internal Medicine*, *25*(Suppl 1), 62–67. https://doi.org/10.1007/s11606-009-1114-6

Nohl-Deryk, P., Brinkmann, J. K., Gerlach, F. M., Schreyögg, J., & Achelrod, D. (2018). Hürden bei der Digitalisierung der Medizin in Deutschland – eine Expertenbefragung. *Gesundheitswesen – Bundesverband der Ärzte des Öffentlichen Gesundheitsdienstes (Germany)*, *80*(11), 939–945. https://doi.org/10.1055/s-0043-121010

Norman, C. D., & Skinner, H. A. (2006). Eheals: The eHealth Literacy Scale. *Journal of Medical Internet Research*, *8*(4), e27. https://doi.org/10.2196/jmir.8.4.e27

Okan, O., Bauer, U., Levin-Zamir, D., Pinheiro, P., & Sørensen, K. (Eds.). (2019). *International Handbook of Health Literacy: Research, practice and policy across*. Policy Press.

Oliver, R. L. (2014). *Satisfaction: A Behavioral Perspective on the Consumer* (2nd edition). Taylor and Francis.

Ozok, A. A., Wu, H., & Gurses, A. P. (2017). Exploring Patients' Use Intention of Personal Health Record Systems: Implications for Design. *International Journal of Human–Computer Interaction*, *33*(4), 265–279. https://doi.org/10.1080/10447318.2016.1277637

Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of electronic personal health records. *BMJ*, *335*(7615), 330–333. https://doi.org/10.1136/bmj.39279.482963.AD

Pang, D., & Proyer, R. T. (2018). An Initial Cross-Cultural Comparison of Adult Playfulness in Mainland China and German-Speaking Countries. *Frontiers in Psychology*, *9*, 421. https://doi.org/10.3389/fpsyg.2018.00421

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A Conceptual Model of Service Quality and Its Implications for Future Research. *Journal of Marketing*, *49*(4), 41–50. https://doi.org/10.2307/1251430

Poncin, I., Garnier, M., Ben Mimoun, M. S., & Leclercq, T. (2017). Smart technologies and shopping experience: Are gamification interfaces effective? The case of the Smartstore. *Technological Forecasting and Social Change*, *124*, 320–331. https://doi.org/10.1016/j.techfore.2017.01.025

Proyer, R. T. (2012). Development and initial assessment of a short measure for adult playfulness: The SMAP. *Personality and Individual Differences*, *53*(8), 989–994. https://doi.org/10.1016/j.paid.2012.07.018

Roehrs, A., da Costa, C. A., Righi, R. d. R., & Oliveira, K. S. F. de (2017). Personal Health Records: A Systematic Literature Review. *Journal of Medical Internet Research*, *19*(1), e13. https://doi.org/10.2196/jmir.5876

Rojas Mezarina, L., Silva-Valencia, J., Escobar-Agreda, S., Espinoza Herrera, D. H., Egoavil, M. S., Maceda Kuljich, M., Inga-Berrospi, F., & Ronceros, S. (2020). Need for the Development of a Specific Regulatory Framework for Evaluation of Mobile Health Apps in Peru: Systematic Search on App Stores and Content Analysis. *JMIR MHealth and UHealth*, *8*(7), e16753. https://doi.org/10.2196/16753

Sachverständigenrat Gesundheitswesen. (2020, April 22). *Daten teilen heißt besser heilen! Digitalisierung als ein Schlüssel zur Überwindung der Coronakrise.* Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen. https://www.svr-gesundheit.de/fileadmin/user_upload/Aktuelles/2020/2020_04_22_Pressemitteilung_SVR_Digitalisierung_gegen_Corona_SPON-Gastbeitrag.pdf

Sailer, M., Hense, J. U., Mayr, S. K., & Mandl, H. (2017). How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. *Computers in Human Behavior*, *69*, 371–380. https://doi.org/10.1016/j.chb.2016.12.033

Salathé, M., Althaus, C. L., Neher, R., Stringhini, S., Hodcroft, E., Fellay, J., Zwahlen, M., Senti, G., Battegay, M., Wilder-Smith, A., Eckerle, I., Egger, M., & Low, N. (2020). Covid-19 epidemic in Switzerland: On the importance of testing, contact tracing and isolation. *Swiss Medical Weekly*, *150*, w20225. https://doi.org/10.4414/smw.2020.20225

Sardi, L., Idri, A., & Fernández-Alemán, J. L. (2017). A systematic review of gamification in e-Health. *Journal of Biomedical Informatics*, *71*, 31–48. https://doi.org/10.1016/j.jbi.2017.05.011

Schaule, M. S. (2014). *Anreize für eine nachhaltige Immobilienentwicklung-Nutzerzufriedenheit und Zahlungsbereitschaft als Funktion von Gebäudeeigenschaften bei Büroimmobilien (Doctoral thesis).* TUM. https://mediatum.ub.tum.de/doc/1210050/file.pdf

Schmidt-Kraepelin, M., Toussaint, P. A., Thiebes, S., Hamari, J., & Sunyaev, A. (2020). Archetypes of Gamification: Analysis of mHealth Apps. *JMIR MHealth and UHealth*, *8*(10), e19280. https://doi.org/10.2196/19280

Schneider, H., Hill, S., & Blandford, A. (2016). Patients Know Best: Qualitative Study on How Families Use Patient-Controlled Personal Health Records. *Journal of Medical Internet Research*, *18*(2), e43. https://doi.org/10.2196/jmir.4652

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Smith, J. H., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Stahl, H. K., Hinterhuber, H. H., Friedrich, S. A., & Matzler, K. (2000). Kundenzufriedenheit und Kundenwert. In H. H. Hinterhuber & K. Matzler (Eds.), *Kundenorientierte Unternehmensführung: Kundenorientierung Kundenzufriedenheit Kundenbindung* (2nd ed., pp. 177–196). Gabler Verlag. https://doi.org/10.1007/978-3-663-10592-3_10

Steiger, J. H. (1980). Statistically based tests for the number of common factors. *The annual meeting of the Psychometric Society*. Iowa City, IA.

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97

Stoyanov, S. R., Hides, L., Kavanagh, D. J., Zelenko, O., Tjondronegoro, D., & Mani, M. (2015). Mobile app rating scale: A new tool for assessing the quality of health mobile apps. *JMIR MHealth and UHealth*, *3*(1), e27. https://doi.org/10.2196/mhealth.3422

Stroetmann, K. A., Artmann, J., Stroetmann, V. N., Protti, D., Dumortier, J., Giest, S., Walossek, U., & Whitehouse, D. (2011). *European countries on their journey towards national eHealth infrastructures*. http://www.ehealth-strategies.eu/report/eHealth_Strategies_Final_Report_Web.pdf

Suki, N. M [Norazah Mohd], Lian, J. C. C., & Suki, N. M [Norbayah Mohd] (2011). Do patients' perceptions exceed their expectations in private healthcare settings? *International Journal of Health Care Quality Assurance*, *24*(1), 42–56. https://doi.org/10.1108/09526861111098238

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th Edition). *Always learning*. Pearson.

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association : JAMIA*, *13*(2), 121–126. https://doi.org/10.1197/jamia.M2025

Thies, K., Anderson, D., & Cramer, B. (2017). Lack of Adoption of a Mobile App to Support Patient Self-Management of Diabetes and Hypertension in a Federally Qualified Health Center: Interview Analysis of Staff and Patients in a Failed Randomized Trial. *JMIR Human Factors*, *4*(4), e24. https://doi.org/10.2196/humanfactors.7709

Tucker, L. R., & Lewis, C. (1973). A reliability coefficient for maximum likelihood factor analysis. *Psychometrika*, *38*(1), 1–10. https://doi.org/10.1007/BF02291170

Vaghefi, I., & Tulu, B. (2019). The Continued Use of Mobile Health Apps: Insights From a Longitudinal Study. *JMIR MHealth and UHealth*, *7*(8), e12983. https://doi.org/10.2196/12983

van der Vaart, R., & Drossaert, C. (2017). Development of the Digital Health Literacy Instrument: Measuring a Broad Spectrum of Health 1.0 and Health 2.0 Skills. *Journal of Medical Internet Research*, *19*(1), e27. https://doi.org/10.2196/jmir.6709

van Haasteren, A., Vayena, E., & Powell, J. (2020). The Mobile Health App Trustworthiness Checklist: Usability Assessment. *JMIR MHealth and UHealth*, *8*(7), e16844. https://doi.org/10.2196/16844

Warren, C., & Laslett, B. (1977). Privacy and Secrecy: A Conceptual Comparison. *Journal of Social Issues*, *33*(3), 43–51. https://doi.org/10.1111/j.1540-4560.1977.tb01881.x

Wheaton, B., Muthen, B., Alwin, D. F., & Summers, G. F. (1977). Assessing Reliability and Stability in Panel Models. *Sociological Methodology*, *8*(1), 84–136. https://doi.org/10.2307/270754

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*, *113*(6), 1151–1222. https://doi.org/10.2139/ssrn.476041

Wickramasinghe, N. (2019). Essential Considerations for Successful Consumer Health Informatics Solutions. *Yearbook of Medical Informatics*, *28*(1), 158–164. https://doi.org/10.1055/s-0039-1677909

Wickramasinghe, N., Bali, R., Suomi, R., & Kirn, S. (2012). *Critical Issues for the Development of Sustainable E-health Solutions*. Springer US. https://doi.org/10.1007/978-1-4614-1536-7

Wickramasinghe, N., & Schaffer, J. (2010). *Realizing value driven e-health solutions*. Report for IBM. Washington DC. https://pdfs.semanticscholar.org/4016/68d5223501c11dfa43d224ca6460a3c7db31.pdf

Winston, T. G., Paul, S., & Iyer, L. (2016). A Study of Privacy and Security Concerns on Doctors' and Nurses' Behavioral Intentions to Use RFID in Hospitals. In *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA.

Xu, W., & Liu, Y. (2015). Mhealthapps: A Repository and Database of Mobile Health Apps. *JMIR MHealth and UHealth*, *3*(1), e28. https://doi.org/10.2196/mhealth.4026

Yi, Y. (1990). A critical review of consumer satisfaction. *Review of Marketing*, *4*(1), 68–123.

Zapata, B. C., Fernández-Alemán, J. L., Idri, A., & Toval, A. (2015). Empirical studies on usability of mHealth apps: A systematic literature review. *Journal of Medical Systems*, *39*(2), 1. https://doi.org/10.1007/s10916-014-0182-2

Zhang, X., Yan, X., Cao, X., Sun, Y., Chen, H., & She, J. (2018). The role of perceived e-health literacy in users' continuance intention to use mobile healthcare applications: an exploratory empirical study in China. *Information Technology for Development*, *24*(2), 198–223. https://doi.org/10.1080/02681102.2017.1283286

Zhou, L., Bao, J., Setiawan, I. M. A., Saptono, A., & Parmanto, B. (2019). The mHealth App Usability Questionnaire (MAUQ): Development and Validation Study. *JMIR MHealth and UHealth*, *7*(4), e11500. https://doi.org/10.2196/11500

Zhou, L., Bao, J., Watzlaf, V., & Parmanto, B. (2019). Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study. *JMIR MHealth and UHealth*, 7(4), e11223. https://doi.org/10.2196/11223

Appendix

Appendix 3.2-A: Measures

All multi-item scales used 7-point measures. The scale anchors were 1: Strongly disagree – 7: Strongly agree.

Privacy concerns were calculated by averaging the four first-order construct scores of *collection, errors, unauthorized access* and *secondary use,* which were measured by adapting Angst and Agarwal's (2009) fifteen-item scale*: Collection*: (1) It usually bothers me when healthcare entities ask me for personal information, (2) When healthcare entities ask me for personal information, I sometimes think twice before providing it, (3) It bothers me to give personal information to so many healthcare entities, (4) I am concerned that healthcare entities are collecting too much personal information about me. *Errors*: (1) All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs, (2) Healthcare entities should take more steps to make sure that the personal information in their files is accurate, (3) Healthcare entities should have better procedures to correct errors in personal information, (4) Healthcare entities should devote more time and effort to verifying the accuracy of the personal information in their databases. *Unauthorized Access*: (1) Healthcare entities should devote more time and effort to preventing unauthorized access to personal information, (2) Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs, (3) Healthcare entities should take more steps to make sure that unauthorized people cannot access personal information in their computers. *Secondary Use*: (1) Healthcare entities should not use personal information for any purpose unless it has been authorized by the individuals who provided the information, (2) When people give personal information to a company for some reason, the company should never use the information for any other reason, (3) Healthcare entities should never sell the personal information in their computer databases to other healthcare entities, (4) Healthcare entities should never share personal information with other healthcare entities unless it has been authorized by the patient who provided the information.

mHealth literacy was calculated by averaging the two first-order construct scores of *mHealth information searching* and *mHealth information appraisal,* which were measured by adapting Lin and Bautista's (2017) eight-item scale: *mHealth information searching*: (1) I know how to find helpful health resources on the mobile phone, (2) I know how to use the mobile phone to answer my health questions, (3) I know what health resources are available on the mobile

phone, (4) I know where to find helpful health resources on the mobile phone. *mHealth information appraisal*: (1) I know how to use the health information I find on the mobile phone to help me (dropped), (2) I have the skills I need to evaluate the health resources I find on the mobile phone, (3) I can tell high quality from low-quality health resources on the mobile phone, (4) I feel confident in using information from the mobile phone to make health decisions.

mHealth self-efficacy was measured using three items developed by Fox and Connolly (2018): (1) I could use health technologies to manage my health, if I had used a similar technology before, (2) I could use health technologies to manage my health, if someone showed me how to, (3) I could use health technologies to manage my health, if I had time to try them out.

Adult playfulness was measured using Proyer's (2012) five-item scale: (1) I am a playful person, (2) Good friends would describe me as a playful person, (3) I frequently do playful things in my daily life, (4) It does not take much for me to change from a serious to a playful frame of mind, (5) Sometimes, I completely forget about the time and am absorbed in a playful activity.

	Factor							
Item	1	2	3	4	5	6	7	8
AdultPlayfulness1.	**0.95**	0.01	-0.06	-0.04	0.03	-0.04	0.07	0.02
AdultPlayfulness2.	**0.88**	-0.06	0.00	-0.08	-0.03	-0.02	0.05	0.02
AdultPlayfulness3.	**0.81**	-0.11	0.06	0.04	-0.05	-0.02	-0.04	0.03
AdultPlayfulness5.	**0.62**	0.09	0.09	-0.05	0.02	0.10	-0.04	-0.09
AdultPlayfulness4.	**0.60**	0.04	-0.10	0.07	0.03	-0.03	-0.03	0.02
mHealthLiteracy.InformationSear-ching4.	-0.03	**1.07**	-0.01	0.02	0.05	0.01	-0.10	-0.17
mHealthLiteracy.InformationSear-ching1.	-0.01	**0.76**	-0.01	-0.02	0.03	0.00	0.03	0.10
mHealthLiteracy.InformationSear-ching2.	0.05	**0.75**	-0.07	0.00	-0.07	-0.01	0.17	0.05
mHealthLiteracy.InformationSear-ching3.	-0.04	**0.74**	0.08	0.00	-0.03	-0.01	-0.08	0.04
PrivacyConcerns.Collection1.	-0.02	0.02	**0.87**	-0.07	-0.04	-0.06	0.02	0.04
PrivacyConcerns.Collection2.	-0.05	0.02	**0.82**	0.07	0.01	0.01	-0.10	0.00
PrivacyConcerns.Collection3.	0.00	0.01	**0.82**	-0.10	-0.01	0.03	0.14	-0.02
PrivacyConcerns.Collection4.	0.04	-0.05	**0.79**	0.07	0.09	-0.02	-0.02	0.00
PrivacyConcerns.Errors4.	-0.03	0.02	-0.02	**0.92**	0.00	-0.02	-0.06	-0.03
PrivacyConcerns.Errors2.	0.03	0.02	-0.05	**0.89**	-0.03	-0.04	0.02	0.02
PrivacyConcerns.Errors3.	-0.06	0.00	-0.11	**0.83**	0.07	0.00	0.00	0.04
PrivacyConcerns.Errors1.	0.03	-0.04	0.22	**0.58**	-0.09	0.08	0.09	-0.07
PrivacyConcerns.SecondaryUse1.	0.02	0.05	0.09	0.03	**0.78**	0.07	-0.12	-0.02
PrivacyConcerns.SecondaryUse4.	0.02	-0.03	0.09	0.04	**0.75**	-0.07	-0.07	0.07
PrivacyConcerns.SecondaryUse3.	-0.05	0.02	-0.07	-0.06	**0.65**	0.01	0.19	-0.02
PrivacyConcerns.SecondaryUse2.	0.01	-0.06	-0.07	-0.01	**0.64**	0.00	0.10	-0.05
mHealthSelf-Efficacy2.	-0.04	-0.05	0.02	0.02	-0.02	**0.92**	-0.03	-0.04
mHealthSelf-Efficacy3.	-0.04	-0.06	-0.03	-0.05	0.04	**0.85**	0.06	0.10
mHealthSelf-Efficacy1.	0.08	0.10	-0.03	0.02	-0.01	**0.72**	-0.02	0.01
PrivacyConcerns.UnauthorizedAccess3.	-0.05	0.04	0.02	0.03	0.07	0.04	**0.86**	-0.02
PrivacyConcerns.UnauthorizedAccess2.	0.01	-0.01	0.02	-0.02	0.04	-0.03	**0.79**	-0.02
PrivacyConcerns.UnauthorizedAccess1.	0.04	-0.01	0.03	0.23	0.07	0.01	**0.60**	0.03
mHealthLiteracy.InformationAppraisal3.	-0.04	0.06	0.03	-0.06	-0.05	0.01	0.06	**0.85**
mHealthLiteracy.InformationAppraisal4.	-0.01	0.00	-0.02	0.00	0.02	0.10	-0.10	**0.74**
mHealthLiteracy.InformationAppraisal2.	0.07	0.20	0.05	0.07	0.02	-0.07	0.02	**0.69**
Eigenvalue	**3.09**	**3.00**	**2.86**	**2.84**	**2.15**	**2.14**	**2.06**	**1.95**
Percentage of variance explained (%)	**10.30**	**10.01**	**9.54**	**9.45**	**7.18**	**7.14**	**6.86**	**6.49**

Table 3.2-9: Factor loadings from exploratory factor analysis (main loading bold font)

Fit measure	Value	Level of acceptance	Reference
	662.156/377.000 = 1.76	< 3	Wheaton et al. (1977)
CFI	0.942	> 0.9	Bentler (1990)
TLI	0.934	> 0.9	Tucker and Lewis (1973)
AGFI	0.826	> 0.8	Jöreskog and Sörbom (1986)
RMSEA	0.053	< 0.6	Steiger (1980)

Table 3.2-10: Confirmatory factor analysis fit measures

Appendix 3.2-B: App screenshots

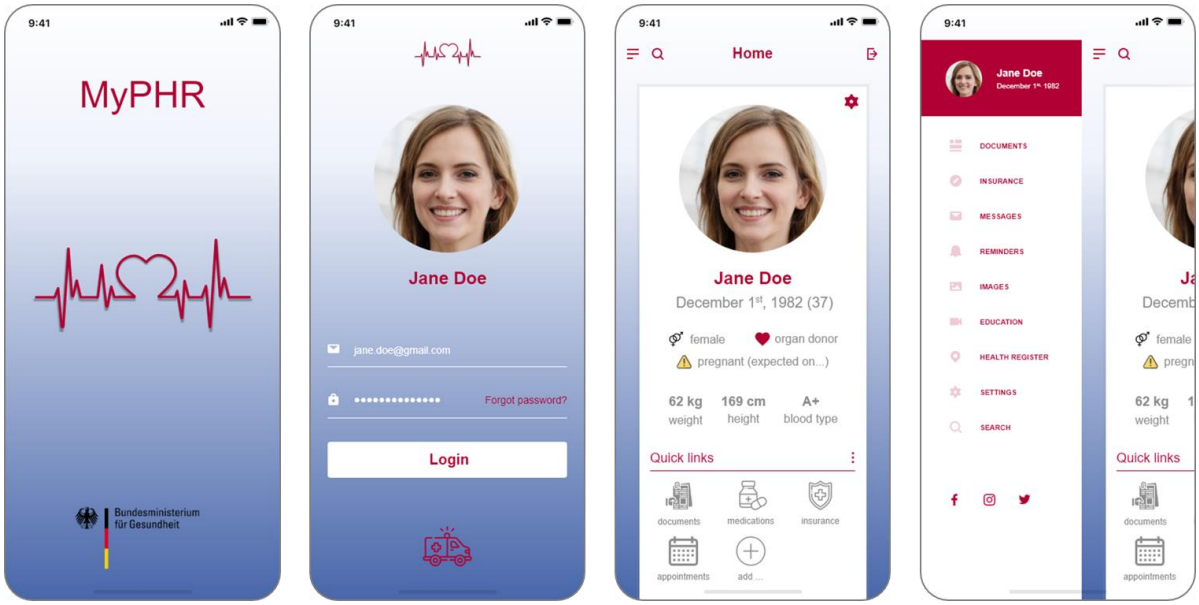


Figure 3.2-4: Exemplary screenshots of a fictional PHR

Appendix 3.2-C: Sample characteristics

Variable	Germany (n = 215)		Denmark (n = 59)		Entire sample (n = 274)	
	absolute	relative	absolute	relative	absolute	relative
Gender						
female	100	47%	32	54%	132	48%
male	115	53%	27	46%	142	52%
Age						
18 - 25	97	45%	19	32%	116	42%
26 - 35	95	44%	21	36%	116	42%
36 - 45	11	5%	12	20%	23	8%
46 - 73	12	6%	7	12%	19	7%
Employment status						
Student	115	53%	24	41%	139	51%
Employed	93	43%	33	56%	126	46%
Self-employed	2	1%	1	2%	3	1%
Unemployed	1	0%	1	2%	2	1%
Retired	4	2%	0	0%	4	1%
Educational background						
Less than a high school diploma	3	1%	0	0%	3	1%
High school degree or equivalent	34	16%	8	14%	42	15%
Bachelor's degree or equivalent	82	38%	33	56%	115	42%
Master's degree or equivalent	83	39%	13	22%	96	35%
Doctoral degree or equivalent	13	6%	5	8%	18	7%
Usage of healthcare-related apps						
Never	103	48%	21	36%	124	45%
Less than once a month	47	22%	26	44%	73	27%

Variable	Germany (n = 215)		Denmark (n = 59)		Entire sample (n = 274)	
	absolute	relative	absolute	relative	absolute	relative
More than once a month	24	11%	10	17%	34	12%
Once a week	16	7%	0	0%	16	6%
More than once a week	6	3%	1	2%	7	3%
Daily	19	9%	1	2%	20	7%

Table 3.2-11: Sample characteristics

To compare the cultural values of Germans and Danes, we used the Values Survey Module questions (Hofstede et al., 2013) covering the six Hofstede dimensions (Hofstede et al., 2010). For calculating the constant, we chose Denmark as reference and see that the differences between our samples are qualitatively the same as the differences between the countries' cultures in the data of Hofstede Insights (2020).

	Country	Power Distance	Individualism	Masculinity	Uncertainty Avoidance	Long Term Orientation	Indulgence
Scores according to Hofstede	Denmark	18	74	16	23	35	70
	Germany	35	67	66	65	83	40
Difference according to Hofstede (Germany minus Denmark)		+17	-10	+50	+42	+38	-30
Scores in our survey	Denmark	18	74	16	23	35	70
	Germany	40	66	60	50	63	43
Difference in our data (Germany minus Denmark)		+22	-8	+44	+27	+28	-27

Table 3.2-12: Cultural dimensions of participants in Germany and Denmark

Appendix 3.2-D: Sample split

	#	1st quartile ("low")								2nd and 3rd quartile ("middle")								4th quartile ("high")							
		A	O	M	I	R	Q	Category strength	Category	A	O	M	I	R	Q	Category strength	Category	A	O	M	I	R	Q	Category strength	Category
Privacy Concerns	F2	45%	21%	10%	15%	7%	1%	24% *	A	30%	29%	15%	23%	4%	0%	1% ²	Mixed (A, O, I)	25%	15%	12%	33%	15%	0%	7% ¹	A
	F4	31%	31%	10%	25%	3%	0%	0% ²	Mixed (A, O)	16%	30%	19%	30%	4%	1%	0% ¹	O	19%	22%	15%	30%	13%	0%	7% ¹	O
	F5	39%	24%	11%	21%	4%	0%	15% *	A	38%	23%	6%	26%	7%	0%	11% *	A	22%	22%	4%	33%	18%	0%	10% ¹	I
	F7	41%	21%	7%	31%	0%	0%	10% ¹	A	35%	29%	10%	26%	1%	0%	6% ²	Mixed (A, O, I)	36%	24%	12%	19%	9%	0%	12% ²	Mixed (A, O, I)
	F8	46%	4%	3%	38%	8%	0%	8% ¹	A	31%	7%	1%	49%	10%	1%	18% *	I	22%	1%	6%	49%	21%	0%	27% *	I
	F9	41%	7%	6%	38%	8%	0%	3% ¹	A	33%	14%	0%	43%	10%	0%	10% ¹	I	28%	4%	1%	40%	25%	0%	12% ¹	I
	F10	41%	27%	13%	18%	1%	0%	14% *	A	32%	25%	18%	21%	5%	0%	7% ²	Mixed (A, O, I)	27%	22%	16%	16%	18%	0%	4% ²	Mixed (A, O, R, M, I)
	F11	17%	3%	3%	54%	24%	0%	30% *	I	11%	1%	1%	51%	35%	1%	15% *	I	10%	1%	0%	34%	54%	0%	19% *	R
	F12	28%	6%	0%	39%	27%	0%	11% ¹	I	22%	3%	2%	37%	35%	1%	1% ²	Mixed (I, R)	9%	1%	1%	28%	60%	0%	31% *	R
	F13	56%	10%	3%	28%	3%	0%	28% *	A	41%	10%	2%	43%	4%	0%	2% ¹	A	36%	12%	1%	37%	13%	0%	1% ¹	I
	F14	35%	6%	0%	39%	20%	0%	4% ¹	I	26%	6%	1%	44%	22%	1%	18% *	I	22%	0%	0%	37%	40%	0%	3% ²	Mixed (R, I)
	F15	3%	0%	0%	42%	55%	0%	13% ²	Mixed (R, I)	1%	1%	0%	22%	76%	1%	54% *	R	0%	0%	0%	21%	79%	0%	58% *	R
	F22	45%	4%	0%	42%	8%	0%	3% ¹	I	38%	8%	1%	43%	10%	0%	5% ¹	I	42%	1%	0%	39%	18%	0%	3% ¹	I
	F23	35%	6%	1%	35%	23%	0%	0% ¹	A	29%	1%	0%	43%	26%	0%	13% *	I	25%	1%	0%	42%	31%	0%	10% ²	Mixed (I, R, A)
mHealth Literacy	F2	26%	27%	11%	27%	9%	0%	0% ¹	O	39%	18%	14%	23%	7%	0%	16% *	A	28%	30%	12%	21%	7%	1%	1% ²	Mixed (O, A, I)
	F4	16%	31%	11%	34%	7%	0%	3% ¹	O	23%	26%	15%	29%	6%	1%	3% ¹	O	21%	30%	22%	22%	4%	0%	7% ²	Mixed (O, M, I, A)
	F5	31%	23%	7%	30%	9%	0%	1% ¹	A	36%	20%	4%	30%	9%	0%	7% ¹	A	33%	30%	12%	16%	9%	0%	3% ²	Mixed (A, O)
	F7	39%	30%	7%	24%	0%	0%	9% ²	Mixed (A, O, I)	39%	20%	10%	27%	3%	0%	12% *	A	28%	31%	10%	25%	4%	0%	3% ²	Mixed (O, A, I)
	F8	27%	7%	3%	44%	17%	1%	17% *	I	31%	2%	3%	50%	12%	1%	19% *	I	42%	9%	3%	39%	7%	0%	3% ¹	A
	F9	26%	11%	1%	44%	17%	0%	19% *	I	32%	9%	3%	42%	14%	0%	9% ¹	I	46%	9%	0%	36%	9%	0%	10% ¹	A
	F10	30%	29%	11%	21%	9%	0%	1% ²	Mixed (A, O, I)	36%	20%	18%	20%	6%	0%	16% *	A	28%	30%	18%	15%	9%	0%	1% ²	Mixed (O, A, M, I)
	F11	7%	3%	3%	50%	37%	0%	13% ²	Mixed (I, R)	12%	1%	0%	47%	39%	1%	7% ²	Mixed (I, R)	19%	1%	1%	46%	31%	0%	15% *	I
	F12	19%	1%	0%	40%	40%	0%	0% ²	Mixed (I, R)	19%	3%	1%	34%	42%	1%	7% ²	Mixed (R, I)	25%	6%	3%	33%	33%	0%	0% ²	Mixed (I, R, A)
	F13	33%	11%	6%	41%	9%	0%	9% ¹	A	48%	9%	1%	37%	4%	0%	11% *	A	46%	12%	0%	36%	6%	0%	10% ¹	A
	F14	30%	6%	0%	37%	26%	1%	7% ¹	I	23%	4%	0%	47%	26%	0%	20% *	I	36%	3%	1%	34%	25%	0%	1% ¹	I
	F15	3%	0%	0%	27%	70%	0%	43% *	R	1%	0%	0%	27%	72%	1%	45% *	R	0%	1%	0%	27%	72%	0%	45% *	R
	F22	37%	6%	1%	43%	13%	0%	6% ¹	I	39%	6%	0%	45%	11%	0%	6% ¹	I	49%	4%	0%	36%	10%	0%	13% ¹	A
	F23	26%	4%	0%	39%	31%	0%	7% ²	Mixed (I, R, A)	28%	2%	1%	45%	24%	0%	16% *	I	37%	1%	0%	34%	27%	0%	3% ¹	I

	#	1st quartile ("low")								2nd and 3rd quartile ("middle")								4th quartile ("high")							
		A	O	M	I	R	Q	Category strength	Category	A	O	M	I	R	Q	Category strength	Category	A	O	M	I	R	Q	Category strength	Category
mHealth Self-Efficacy	F2	24%	15%	17%	30%	14%	0%	6% [1]	A	39%	25%	9%	23%	4%	0%	13% *	A	33%	30%	14%	16%	5%	2%	3% [2]	Mixed (A, O)
	F4	17%	19%	14%	39%	11%	0%	20% *	I	25%	31%	10%	30%	3%	1%	1% [1]	O	17%	37%	29%	13%	5%	0%	8% [2]	Mixed (O, M)
	F5	27%	17%	7%	33%	15%	0%	6% [1]	A	42%	20%	7%	25%	6%	0%	17% *	A	29%	37%	6%	21%	8%	0%	8% [2]	Mixed (O, A, I)
	F7	31%	24%	11%	31%	4%	0%	0% [1]	A	39%	24%	8%	27%	2%	0%	13% *	A	38%	30%	11%	17%	3%	0%	8% [2]	Mixed (A, O)
	F8	21%	6%	2%	49%	19%	2%	27% *	I	35%	5%	5%	47%	9%	0%	13% *	I	44%	5%	0%	40%	11%	0%	5% [1]	I
	F9	20%	7%	2%	49%	21%	0%	27% *	I	35%	13%	1%	39%	12%	0%	4% [1]	I	49%	8%	3%	33%	6%	0%	16% *	A
	F10	29%	21%	15%	21%	13%	0%	7% [2]	Mixed (A, O, I, M)	33%	23%	16%	23%	6%	0%	10% *	A	38%	33%	17%	8%	3%	0%	5% [2]	Mixed (A, O)
	F11	6%	2%	2%	38%	51%	0%	13% *	R	17%	2%	1%	50%	30%	1%	20% *	I	13%	2%	0%	54%	32%	0%	22% *	I
	F12	11%	1%	1%	31%	56%	0%	25% *	R	21%	5%	2%	40%	31%	1%	9% [2]	Mixed (I, R)	32%	3%	2%	32%	32%	0%	0% [1]	I
	F13	33%	10%	2%	44%	11%	0%	11% [1]	I	46%	9%	2%	38%	6%	0%	9% [1]	A	52%	14%	3%	30%	0%	0%	22% *	A
	F14	18%	6%	0%	44%	32%	0%	12% [2]	Mixed (I, R)	33%	3%	1%	39%	24%	1%	6% [1]	I	30%	5%	0%	43%	22%	0%	13% [1]	I
	F15	1%	0%	0%	19%	80%	0%	61% *	R	2%	1%	0%	33%	64%	1%	31% *	R	0%	0%	0%	25%	75%	0%	49% *	R
	F22	31%	5%	1%	48%	15%	0%	17% *	I	40%	8%	0%	43%	9%	0%	3% [1]	I	56%	2%	0%	32%	11%	0%	24% *	A
	F23	26%	2%	0%	44%	27%	0%	17% *	I	33%	2%	1%	39%	26%	0%	6% [1]	I	29%	5%	0%	40%	27%	0%	11% [1]	I
Playfulness	F2	42%	26%	8%	18%	6%	0%	17% *	A	29%	20%	17%	27%	6%	0%	2% [1]	A	30%	27%	9%	22%	11%	2%	3% [2]	Mixed (A, O, I)
	F4	17%	33%	17%	27%	5%	1%	6% [1]	O	28%	20%	14%	33%	5%	0%	5% [1]	A	11%	41%	17%	23%	8%	0%	17% *	O
	F5	36%	22%	5%	28%	9%	0%	8% [1]	A	38%	18%	8%	26%	11%	0%	12% *	A	25%	34%	8%	27%	6%	0%	8% [1]	O
	F7	40%	28%	10%	21%	1%	0%	12% [2]	Mixed (A, O)	39%	17%	8%	35%	2%	0%	4% [1]	A	28%	41%	13%	14%	5%	0%	13% [2]	Mixed (O, A)
	F8	36%	8%	3%	41%	13%	0%	5% [1]	I	28%	2%	3%	53%	12%	2%	25% *	I	39%	8%	3%	38%	13%	0%	2% [1]	A
	F9	26%	9%	3%	50%	13%	0%	24% *	I	35%	8%	2%	41%	14%	0%	6% [1]	I	42%	14%	0%	30%	14%	0%	13% [1]	A
	F10	33%	22%	18%	21%	6%	0%	12% [2]	Mixed (A, O, I)	37%	23%	11%	23%	6%	0%	14% *	A	23%	31%	25%	9%	11%	0%	6% [2]	Mixed (O, M, A)
	F11	13%	4%	3%	46%	35%	0%	12% [2]	Mixed (I, R)	9%	1%	0%	50%	39%	1%	11% *	I	19%	2%	2%	44%	34%	0%	9% [2]	Mixed (I, R)
	F12	23%	4%	3%	38%	32%	0%	6% [2]	Mixed (I, R, A)	16%	2%	1%	37%	44%	1%	7% [2]	Mixed (R, I)	27%	6%	2%	28%	38%	0%	9% [2]	Mixed (R, I, A)
	F13	42%	4%	1%	45%	8%	0%	3% [1]	I	39%	13%	2%	41%	6%	0%	2% [1]	A	56%	13%	5%	23%	3%	0%	33% *	A
	F14	31%	3%	0%	38%	28%	0%	8% [1]	I	24%	5%	0%	45%	25%	1%	20% *	I	31%	6%	2%	36%	25%	0%	5% [1]	I
	F15	3%	0%	0%	23%	74%	0%	51% *	R	0%	0%	0%	31%	68%	1%	37% *	R	2%	2%	0%	23%	73%	0%	50% *	R
	F22	35%	6%	1%	46%	12%	0%	12% [1]	I	38%	5%	0%	45%	11%	0%	8% [1]	I	55%	5%	0%	30%	11%	0%	25% *	A
	F23	22%	1%	0%	49%	28%	0%	21% *	I	30%	2%	1%	42%	25%	0%	13% *	I	41%	5%	0%	27%	28%	0%	13% [1]	R

Legend: * = Categorization significant at a ten-percent level according to Fong test
[1] = (O + A + M) < > (I + R + Q) rule applicable
[2] = (O + A + M) < > (I + R + Q) rule not applicable
A = Attractive quality (delighter)
O = One-dimensional quality (performance need)
M = Must-be quality (basic need)
I = Indifferent quality
R = Reverse quality
Q = Questionable result

Table 3.2-13: Empirical results of the PHR feature evaluation based on the sample split

4 Mitigation mechanisms to cope with the negative consequences of digitalization

4.1 The upside of data privacy – delighting customers by implementing data privacy measures

Abstract: The targeted analysis of customer data becomes increasingly important for data-driven business models. At the same time, the customers' concerns regarding data privacy have to be addressed properly. Existing research mostly describes data privacy as a necessary evil for compliance and risk management and does not propose specific data privacy measures which address the customers' concerns. We therefore aim to shed light on the upside of data privacy. In this paper, we derive specific measures to deal with customers' data privacy concerns based on academic literature, legislative texts, corporate privacy statements, and expert interviews. Next, we leverage the Kano model and data from two internet-based surveys to analyze the measures' evaluation by customers. From a customer perspective, the implementation of the majority of measures is obligatory as those measures are considered as basic needs of must-be quality. However, delighting measures of attractive quality do exist and have the potential to create a competitive advantage. In this, we find some variation across different industries suggesting that corporations aiming to improve customer satisfaction by superior privacy protection should elicit the demands of their specific target customers.

Keywords: Privacy concerns, privacy measures, customer data, customer satisfaction, survey research

Authors: Henner Gimpel, Dominikus Kleindienst, Niclas Nüske, Daniel Rau, Fabian Schmied

Status: This article is published in Electronic Markets, Volume 28, Issue 4, pp. 437-452 (2018).

4.1.1 Introduction

In the future, the ability to analyze customer data will be a growing source of competitive advantage (Morey et al., 2015). With the growing amount of data generated worldwide, digital business models emerge which are based on insights gained from customer data (Matthing et al., 2004; Saarijärvi et al., 2014). At the same time, trust in data privacy is becoming more relevant for customers (Berendt et al., 2005; Preibusch et al., 2013) which is amplified by several data privacy scandals in the recent past. For instance, a serious incident occurred when the credit card information of 56 million Home Depot customers was stolen (Inman & Nikolova, 2017; Morey et al., 2015). Other examples are Ashley Madison, an online dating portal which lost user data of 37 million registered married men and women to the public (BBC, 2015); Apple which was accused of collecting location data on iPhones and iPads without authorization from and without notifying their customers (The Guardian, 2011); and Facebook which was discovered to be collecting data from user profiles and transmitting these data to advertising companies and others (The Telegraph, 2010). For companies, such publicly exploited scandals cause economic damage (Acquisti et al., 2006; Muntermann & Roßnagel, 2009) and competitive disadvantages in brand image and customer satisfaction. Conversely, it might be possible that companies which perform well in terms of data privacy could increase customer satisfaction and gain a competitive advantage. For instance, companies such as DuckDuckGo or Silent Circle already try to differentiate themselves by providing privacy friendly services (Tanner, 2013). DuckDuckGo is a search engine which differs substantially from many conventional search engines. The company collects neither personal information nor behavioral data about its users. Silent Circle is a company which provides solutions for secure communication. For instance, the company developed a smartphone which ensures private and encrypted communication. However, many companies see data privacy as necessary evil. As such, data privacy limits the opportunities to gain valuable customer insights and its implementation binds valuable resources (Culnan & Armstrong, 1999). In addition to this downside perspective, an integrated management of data privacy requires an upside perspective. Moreover, practitioners should be aware of specific available data privacy measures which go beyond the mere application of laws and regulations and, thus, enable their companies to differentiate themselves from their competitors.

Also in academic literature, data privacy management is mostly seen from a risk perspective which focusses on corporate data (e.g., from internal research departments) without considering customers' concerns regarding the protection of their personal information. For instance, Buhl (2013) states that privacy protection measures which address threats such as technology

spying and obstruction should be implemented only if the risk-reducing effects outweigh the related costs. Acquisti et al. (2006) link a company's privacy incidents to the negative impacts on its market value. Only to a small extent does the literature consider an upside perspective on data privacy, such as Preibusch et al. (2013) who found that customers who bought a DVD at a privacy-friendly but more expensive online retailer are more satisfied than customers of cheaper but privacy-unfriendly online retailers. Even so, specific data privacy measures which might be implemented to generate customer delight are yet to be considered in the literature. Thus, we raise the following two research questions:

RQ1: Which data privacy measures can companies take?

RQ2: Are some of these measures perceived as attractive measures that delight customers?

To answer these research questions, we first develop an overview of data privacy measures by investigating and consolidating academic literature, legislative texts, company privacy statements, and findings from expert interviews. Second, using the Kano model, we evaluate the customers' perception of these different measures, that is, whether measures are considered to be of must-be, one-dimensional, attractive, or indifferent quality. This paper is organized as follows: We discuss the context of the problem and related work. We outline our methodical approach, derive measures which can be taken by companies to address data privacy concerns and analyze the customers' perceptions of these measures on the basis of the results of two surveys. The discussion provides an overview of the theoretical contribution and managerial implications as well as the paper's limitations. Lastly, we conclude with a summary and an outlook on potential areas of future research.

4.1.2 Problem context

As previously motivated, public attention regarding data privacy issues is growing. This attention is reflected in different scientific disciplines, such as philosophy, psychology, economics, marketing, law, and information systems (Ahmad & Mykytyn, 2012; Pavlou, 2011). Moreover, privacy incidents such as the scandals previously mentioned as well as their prevention are the subject of numerous research projects[15]. Privacy incidents appear regularly and have consequences for both companies and customers. They are defined by Acquisti et al. (2006) as events "involving misuses of individuals' personal information." Consequently,

[15] Examples: Acquisti et al. (2006); Ahmad and Mykytyn (2012); Campbell et al. (2003); Cavusoglu et al. (2004); Dhasarathan et al. (2015); Hovav and D'Arcy (2003); Mamonov and Koufaris (2014); Moshki and Barki (2016); Nicholas-Donald et al. (2011); Nofer, Hinz, Muntermann, and Roßnagel (2014).

customers might become victims of fraud or identity theft (Acquisti et al., 2006). Furthermore, the misuse of personal information might have negative effects on personal relationships, job applications, insurance contracts, and credit decisions.

Smith et al. (1996) elaborated seven major data privacy concerns of customers relating to Data Collection (storage of large amounts of personal customer data), Data Combination (combination of customer data from different databases to gain additional information about a customer), Internal Secondary Usage (usage of customer data for an unauthorized secondary purpose within the company), External Secondary Usage (disclosure of customer data for an unauthorized secondary purpose outside the company), Errors (deliberate or accidental errors in customer data), Improper Access (unauthorized views and edits of customer data), and Reduced Judgment (automated decision-making based on customer data). The work of Smith et al. (1996) is described as the first and most influential work in the field of data privacy concerns (Preibusch, 2013). Though some publications adapt the concerns (e.g., Hong & Thong, 2013; Malhotra et al., 2004), mostly to better measure the concerns with multi-item survey scales and factor analysis, recent publications also refer to Smith et al. (1996) without any modification of the privacy concerns (e.g., Eastin et al., 2016; Keith et al., 2013).

Academic literature provides recommendations for customers themselves as well as public authorities responsible for protecting customers' privacy rights through laws and regulations (Buchmann et al., 2008; Klingspor, 2016). From a company perspective, privacy incidents may be caused by technical, managerial, organizational, or human failures (Acquisti et al., 2006). Companies might suffer direct economic damage, such as punishment by penalties or loss of market value, as well as indirect effects, such as increasing insurance fees or decreasing customer satisfaction (Acquisti et al., 2006; Nicholas-Donald et al., 2011). The effect of privacy breaches on a firm's market value is considered in several papers. Cavusoglu et al. (2004) investigate the effect of internet security breach announcements on the market value of publicly traded US firms. A similar study was conducted by Campbell et al. (2003). The authors investigate the effect of public announcements of information security breaches on the market value of publicly traded US firms. Within their analysis, Campbell et al. (2003) differentiate between security breaches which involve unauthorized access to confidential data and security breaches which do not involve confidential data. Interestingly, significant effects can only be shown in the case of the involvement of confidential data (Campbell et al., 2003). In contrast, Nofer, Hinz, Muntermann, and Rossnagel (2014) investigate the direct effect of privacy violations and security breaches on consumers' investment behavior, which was examined in a laboratory experiment.

Consequently, companies must decide on how to deal with data privacy issues and the related risks. In line with this issue, articles which address companies' handling of data privacy focus on potential threats and how to avoid their occurrence. Occasionally, the management of data privacy is considered as a part of corporate data governance which can be seen as a "framework for assigning decision-related rights and duties in order to be able to adequately handle data as a company asset" (Otto, 2011). As an example, Khatri and Brown (2010) propose to define the role of a data security officer as a part of the data governance in order to specify and monitor access requirements to data. Also, Culnan and Armstrong (1999) argue that companies need to implement a comprehensive governance structure in order to manage data privacy appropriately.

Many authors describe a trade-off between the use of personal data to improve the customer experience, e.g., by personalizing customer services, and the implementation of data privacy measures which are often considered as obstacles to profitability (Schneider et al., 2017). Only a limited set of articles considers data privacy measures as an opportunity to create a competitive advantage. For instance, Preibusch et al. (2013) show that appropriate management of data privacy issues may have positive implications on customer satisfaction. By conducting an experiment, the article examined the effects of different levels of data privacy in online retail. With regard to online retail, the authors state that privacy becomes a competitive factor. Sarathy and Robertson (2003) provide a framework which assists companies in implementing a data privacy strategy which considers ethical aspects. The authors propose strategies which exceed the level of data privacy required by laws and regulations. Within a research-in-progress paper, Lyons et al. (2016) propose to examine the effects of different privacy protection approaches on customer trust. In this regard, the authors distinguish organizational privacy protection approaches which are driven by control values and such which are driven by justice values.

However, neither article provides recommendations for specific data privacy measures which can be implemented to address customers' data privacy concerns and increase customer satisfaction. Although the importance of customer satisfaction for long-term customer relationships is commonly accepted, using data privacy to delight customers to gain a competitive advantage or to implement different pricing strategies has yet to be comprehensively examined. To the best of our knowledge, related work does not provide insights into addressing customers' different privacy concerns using concrete measures and the extent to which such measures affect customer satisfaction.

As customer satisfaction has a positive impact on customer loyalty (Gronholdt et al., 2000) and the value of a company (Matzler & Stahl, 2000), many companies strive to achieve a high level of customer satisfaction. Due to this well-supported relation, the literature provides numerous methods of measuring customer satisfaction and its antecedents. In this context, a commonly used method to measure the quality of service attributes is SERVQUAL (Ladhari, 2009; Parasuraman et al., 1985). As part of a causal structure, the concept of customer satisfaction can be analyzed with the help of structural equation modeling and neural networks (Hackl & Westlund, 2000). Bartikowski and Llosa (2004) analyze further methods, namely Penalty Reward Contrast Analysis, Correspondence Analysis, Dual Importance Mapping, and the Kano model which was originally proposed by Kano et al. (1984). The Kano model has been discussed and applied in many theoretical and empirical research projects (Füller & Matzler, 2008; Löfgren & Witell, 2008) as it provides a comprehensive presentation of attributes of products or services which influence the degree of customer satisfaction. For instance, the model has been used by Lai and Wu (2011) in order to gain insights in the customers' needs of a public transport company and by Arbore and Busacca (2009) who studied determinants of customer satisfaction for a retail bank.

4.1.3 Research method

To answer the research questions, we first identify and structure the field of possible data privacy measures and then use the Kano model and data from two online surveys to evaluate customers' perceptions regarding different data privacy measures.

4.1.3.1 Identification of data privacy measures

As a basis for identifying data privacy measures, we conducted a comprehensive search for relevant statements, that is, any piece of information on any type of action which addresses customers' data privacy concerns. Therefore, our sources are legislative texts in particular (European General Data Protection Regulation (EU-GDPR), German Bundesdatenschutzgesetz (BDSG), and Telemediengesetz (TMG)) but also scientific literature. Beyond using the pertinent literature known to us from prior research on data privacy, we conducted a structured literature search in the databases AISeL, EBSCOhost, and JSTOR. In these databases, we used the following search term: ("data privacy") AND ("concern" OR "issue") AND ("measure" OR "protection" OR "policy"). As interactions between companies and customers and also the amount of generated customer data changed tremendously with the emergence of smartphones and other digital channels, we decided to consider articles which were published within the last ten years (2008-2017). The search was limited to peer-reviewed articles. In

total, we found 128 articles. By conducting an abstract screening, we identified four potentially relevant articles (Bélanger & Crossler, 2011; Clement & Obar, 2016; Keith et al., 2016; Payne et al., 2015). The in-depth analysis resulted in two papers that contain concrete statements for deriving feasible data privacy measures: Clement and Obar (2016), who examine the data privacy transparency of Canadian internet carriers and Payne et al. (2015), who focus on a list of different laws, regulations, and frameworks and attempt to reconcile the conflicting agendas of companies and customers. Practical recommendations from Audatis Consulting (2016) were used to complement the statements from a practitioner-oriented perspective. Furthermore, we analyzed nine corporate privacy statements across industries: Amazon (2017), Apple (2017), Deutsche Bank (2017), Dropbox (2017), easyJet (2017), Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017), and Zalando (2017). We aimed to sample these privacy statements from corporations in different industries, partially known for a strong reliance on gathering and analyzing customer data or a strong obligation to protect customer data. Additionally, we conducted three expert interviews, each lasting approximately 30 to 60 minutes. In the first interview, we talked to an in-house data privacy officer of a German automotive company in order to gain an overview of existing and potential data privacy measures as well as the challenges and difficulties entailed. To verify existing statements and to check whether we had covered all relevant aspects, we conducted a second interview with a researcher who was working on a project with the goal of developing a long-term data privacy strategy for a German bank. For instance, this interviewee mentioned that customers may want to know which personal data a company stores about them. This statement was later considered to develop a data privacy measure that allows customers to easily get a copy of all their personal data stored and processed by a company. To complement our research with input from a legal perspective, we interviewed a lawyer who works for a renowned German business law office and consults on data privacy. Therefore, he possesses expertise in European privacy laws and regulations.

The examination of the different sources resulted in 202 statements. All statements were then grouped by semantic similarity. In doing so, the authors jointly decided on the grouping of the statements. Without having pre-defined groups, each statement was either used to create a new group with a particular data privacy measure or mapped to an existing group. In the rare case of disagreement between the authors, every author firstly explained the reasons for his preferred grouping then the team of authors discussed the different aspects and repeated the grouping process for the respective measure. The procedure resulted in 32 groups, each consisting of one or several statements regarding a particular data privacy measure. From each of

the groups of statements, we derived a single measure which addresses all statements within the group. After the formulation of the measures, we assigned each of the measures to one or more specific customer data privacy concerns. To validate the mapping of all measures to the seven concerns, eleven aviation and retail customers were asked for their assessment in an ex-post quality check. The majority of customers mapped 27 out of all 32 measures to the same concern as the team of authors. For almost all of the remaining five measures, customers' second most frequent classification was congruent with the authors' mapping and the measure had content-related similarity with both the authors' and the customers' mapping. As only slight differences in customers' and experts' assessment can be observed, this ex-post quality check suggests adequate data quality.

4.1.3.2 Evaluation of customers' perceptions

After the derivation of data privacy measures and their assignment to specific data privacy concerns, we now focus on determining their effect on customer satisfaction. As the context at hand requires the possibility of individual investigation of each measure and applicability to hypothetical cases, we decided to use the Kano model. To evaluate customers' perceptions regarding the identified data privacy measures, we conducted two online surveys.

4.1.3.2.1 Kano model

The Kano model describes customer satisfaction on the basis of the degree of implementation or availability of certain attributes of products or services (Kano et al., 1984; Matzler et al., 1996). Thereby, the perceived degree of implementation or availability depends on the customers' expectations. The model differentiates between four major types of factors. We list these factors in Table 4.1-1 and illustrate their nature in Figure 4.1-1.

Factor	*Customers' expectations*	*Effect on satisfaction*	
		if implemented	*if not implemented*
Attractive quality (delighter)	Customers do not expect implementation of measure	positive	none
One-dimensional quality (performance need)	Customers explicitly demand implementation of measure	positive	negative
Must-be quality (basic need)	Customers implicitly demand implementation of measure	none	negative
Indifferent quality	Customers are indifferent to implementation of measure	none	none

Table 4.1-1: List of the Kano model factors as described by Matzler et al. (1996) and applied to the data privacy context

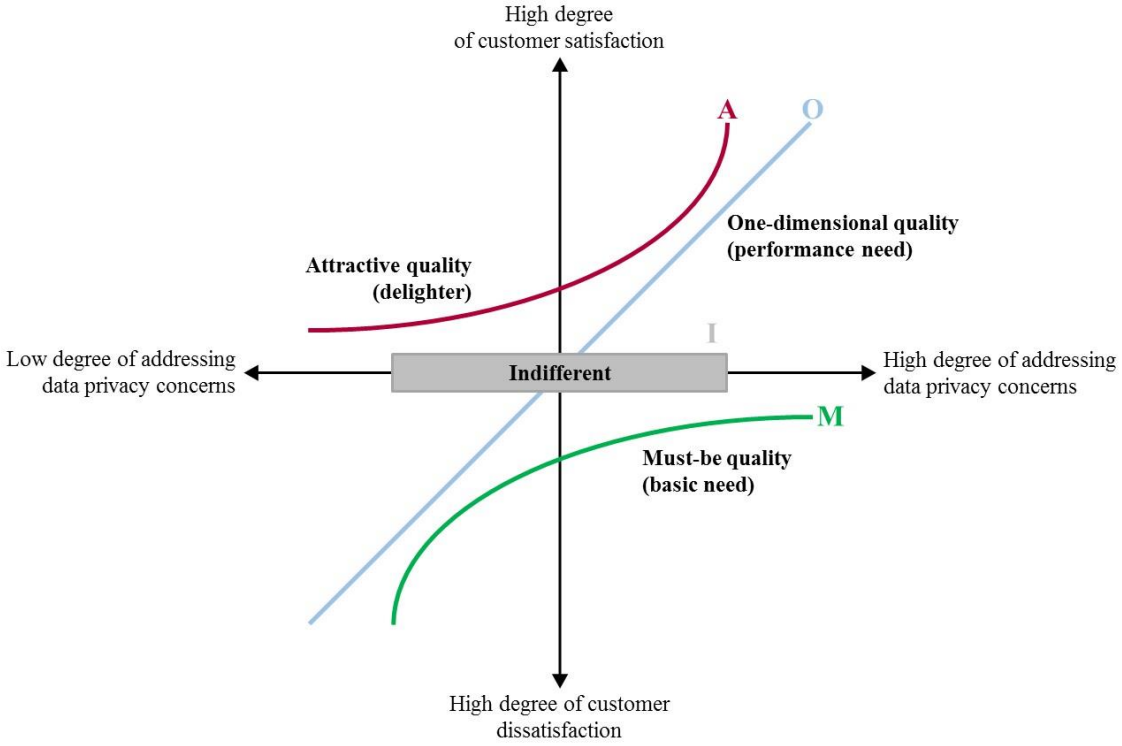
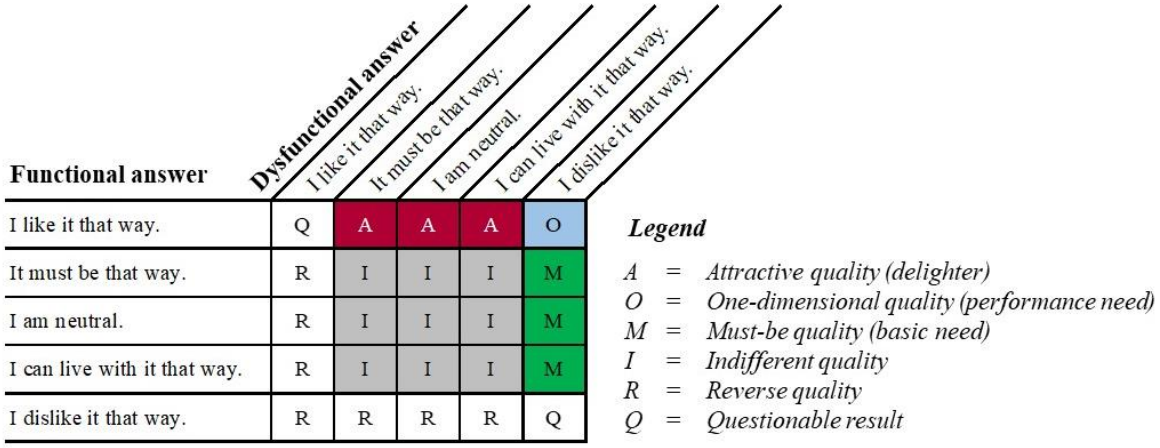


Figure 4.1-1: Illustration of the Kano model factors as described by Matzler et al. (1996) and applied to the data privacy context

The classification of a measure as a certain factor depends on customers' answers to both a functional and a dysfunctional question (Kano et al., 1984; Matzler et al., 1996). That is, customers are asked about their evaluation of the hypothetical case in which a measure is implemented and a case in which it is not. Each time, they can choose one of five possible answers: "I like it that way," "It must be that way," "I am neutral," "I can live with it that way," and "I dislike it that way." The different answers do not stand for a level of acceptance and there is no ordinal scale. Each possible combination of answers can be interpreted in an individual manner and leads to a certain pre-defined classification (Kano et al., 1984; Matzler et al., 1996), as shown in Figure 4.1-2.



Functional answer \ Dysfunctional answer	I like it that way.	It must be that way.	I am neutral.	I can live with it that way.	I dislike it that way.
I like it that way.	Q	A	A	A	O
It must be that way.	R	I	I	I	M
I am neutral.	R	I	I	I	M
I can live with it that way.	R	I	I	I	M
I dislike it that way.	R	R	R	R	Q

Legend

A = *Attractive quality (delighter)*
O = *One-dimensional quality (performance need)*
M = *Must-be quality (basic need)*
I = *Indifferent quality*
R = *Reverse quality*
Q = *Questionable result*

Figure 4.1-2: Derivation of Kano model factors based on Matzler et al. (1996)

The easiest and most intuitive way to determine the final classification of a measure as one of the Kano model factors for the overall sample is to choose the classification which appeared the most often, that is, the mode (Berger et al., 1993). However, determining and presenting the results solely based on the mode leads to a lack of further information about other frequently chosen categorizations. This is especially disadvantageous if the shares of participants who evaluated the measures as one of the other frequently chosen categorizations are of similar size (Schaule, 2014). There are numerous ways to determine whether a categorization based on the mode is significant as compared to other frequently chosen ones. Lee and Newcomb (1996) use the variable category strength, which is calculated as the difference between the shares of the most and second most frequently chosen categorizations. If the category strength is higher than six percent, they conclude that assigning the attribute to only one category is justified. If it is below six percent, they assign the attribute to a mixed category. A more sophisticated approach to decide whether the frequencies of the most and second most frequently chosen categorizations are significantly different is the test proposed by Fong (1996). It assumes significance if the category strength is higher than a reference value calculated based on the observed frequencies and the sample size. If determining a result based on the mode is not reasonable, Berger et al. (1993) propose to apply the (A, O, M) < > (I, R, Q) rule. Thereby, categorizations as attractive, one-dimensional, or must-be ((A, O, M) group) mean that an attribute has an influence on customer satisfaction. Categorizations as indifferent, reverse, or questionable ((I, R, Q) group) mean that an attribute has no influence on satisfaction. If one of the most and second most frequently chosen categorizations belong to one group and the remaining one to the other group, the (A, O, M) < > (I, R, Q) rule is applicable. It is executed by determining the group with the highest share of categorizations of the overall sample and then selecting the most frequently chosen categorization within this group. In the

current work, we will use the following approach for the determination of the final classification of our measures as one of the Kano model factors: we assign a category based on the mode if the category strength is significant at a ten-percent level according to the Fong test[16]. If the category strength is not significant and the (A, O, M) < > (I, R, Q) rule is applicable, we execute this rule. If it is not applicable, we assign the measure to a mixed category following Lee and Newcomb (1996). Additionally, we list all categorizations which do not exhibit a significant difference according to the Fong test as compared to the most frequently chosen one.

An alternative, continuous approach which avoids assigning categories to attributes altogether is the calculation of satisfaction ("better") and dissatisfaction ("worse") coefficients (Berger et al., 1993; Schaule, 2014). The satisfaction coefficient is calculated as the sum of all participants who categorized an attribute as a factor which has the power to increase their satisfaction (attributes of attractive and one-dimensional quality) over the sum of all participants who categorized the attribute as attractive, one-dimensional, must-be, or indifferent. The satisfaction coefficient's possible values range from 0 to 1. Reversely, the dissatisfaction coefficient is calculated as the sum of all participants who categorized the attribute as a factor which has the power to decrease their satisfaction (measures of must-be and one-dimensional quality) over the same denominator. Its value range is -1 to 0. The coefficients thus state the mean importance of attributes over all survey participants with regard to their power to both improve customer satisfaction and avoid customer dissatisfaction. In particular, it can be used to prioritize the implementation of measures (Berger et al., 1993). We will additionally use satisfaction and dissatisfaction coefficients to graphically represent and verify the results of our surveys.

4.1.3.2.2 Surveys

To determine the customers' evaluation of the identified data privacy measures, we conducted two Internet-based surveys. To enable the participants to assume a perspective as natural as possible and to illustrate the situation, we decided to use specific, well-known, and simple scenarios which relate to an exemplary industry sector for which data privacy is a considerable issue. That is, the sectors should feature a business-to-consumer market with a significant occurrence of processed customer data. To be able to consider the possible exchange of customer data between companies, cooperation agreements should exist between major actors in

[16] Unfortunately, due to a misreading of the underlying source, an incorrect significance level for the Fong test was stated in the published version of this research article. The significance level was 10 % instead of 5 %. The error has been corrected in this dissertation. The journal has been notified.

the industry. Furthermore, companies should provide loyalty programs because they are typically based on gathering data on a customer's behavior over a long period.

All of these requirements are fulfilled by the aviation sector. A considerable amount of customer data is collected at different interaction points (Clayton & Hilz, 2015). Data are transmitted to public authorities, airport operators, or other airlines which are partners in global alliances (Harris, 2007). Furthermore, airlines often provide loyalty programs (e.g., Miles & More, Emirates Skywards). Finally, the aviation sector is a commonly known industry. Therefore, we decided to face the participants with a typical customer process from the aviation sector.

To ensure high quality results, we first ran a pretest followed by the main survey. In the pretest, we asked 85 German-speaking participants to imagine booking a flight through an airline's website. Each participant was asked a functional and a dysfunctional question for each of the measures. Using the insights of the pretest, we made several modifications to the main survey: for improving the response rate, we mixed the questions with invitations to guess the correct answers to fun-fact questions about the aviation sector. For improving understandability, we grouped the questions with regard to the data privacy concerns they address and preceded them by short explanations of these concerns. The following example of an explanation, a functional, and a dysfunctional question demonstrates the survey's design. The example refers to a measure which addresses the concern External Secondary Usage (see measure D1 in Table 4.1-2 for detail). In the survey, the questions regarding this measure were preceded by the following explanation to acquaint the participants with the concern: "Your customer data may be used by a third party outside of the company for a purpose not previously agreed upon. The company implements the following measures:" The functional question directly related to the measure then read: "Information. If your customer data are passed on to external third parties, you are informed." The dysfunctional question was: "If your customer data are passed on to external third parties, you are not informed." Afterwards, the participants were asked a functional and a dysfunctional question each for every remaining measure which addresses the concern External Secondary Usage. To answer the functional and the dysfunctional question, the participants can choose one of the five previously mentioned possible answer options. In this way, we asked the participants about each of the 32 identified measures, resulting in 32 pairs of questions, each of them addressing one of the data privacy concerns.

227 German-speaking participants completed the main survey, 219 of whom correctly answered a control question. The participants were recruited via social media and email and

incentivized through a lottery of vouchers for an online retailer. The sample mostly consists of students (78%) and employees (16%). The age of the participants is between 18 and 57 years (average age 25.4 years). The survey was completed by both women (55%) and men (45%). The majority of the participants is well-educated. The share of participants holding a university degree is 51%. Another 42% of the participants achieved degrees with the matriculation standard.

In order to verify the initial results, we subsequently conducted a second survey. To ensure the comparability of both surveys, we used the same questionnaire as in the first survey. However, to take a step towards a generalizability of the results, the participants of the second survey were faced with a modified scenario. Due to its growing importance and the vast amount of customer data which is collected and processed within a purchase process, we decided to consider the online retail sector. Most of the customers create personal accounts. Furthermore, leading online retailers provide own loyalty programs (Mohammed, 2014). Usually, customer data are transferred to external logistics service providers in order to ship the products to the customers. Therefore, the online retail sector fulfills the previously defined requirements. In this context, the participants of the second survey were asked to imagine ordering a smartphone on the website of an internationally renowned online retailer.

299 German-speaking participants completed the second survey, 270 of whom correctly answered a control question. As in the first survey, participants were recruited via social media and email and incentivized through a lottery of vouchers for an online retailer. Most of the participants are students (77%) or employees (17%). The age of the participants ranges between 18 and 59 years (average age 24.6 years). The majority of the participants is well-educated. The share of participants holding a university degree is 50%. Another 45% of the participants achieved degrees with the matriculation standard. The majority of the participants (86%) stated that they have not completed a similar survey before, indicating that the set of participants differs significantly from the first survey.

4.1.4 Results

In the first part of this section, we present the overview of possible data privacy measures for companies which resulted from the research process previously described. This overview forms the basis of the presentation of the survey results in the second part of this section, that is, the perceptions which customers have of the identified privacy measures.

4.1.4.1 Data privacy concerns and measures

As described above, the overview of possible data privacy measures is compiled from academic literature, legislative texts, practical recommendations, corporate privacy statements, and expert interviews. From all sources, we collected 202 statements merged to 32 groups. From these groups, we derived particular data privacy measures and mapped them to the seven privacy concerns described by Smith et al. (1996). The measures are presented in Table 4.1-2, numbered and grouped according to the seven concerns. Each measure's detailed explanation is preceded by a short description printed in bold. Some of these short descriptions show recurring themes across concerns, e.g., "empowerment" taking on different facets with respect to most concerns. In the last column, we present the references from which we derived the measures and their detailed descriptions. In summary, Table 4.1-2 represents a comprehensive list of actions which can be taken by companies to mitigate the risk of displeasing customers and to create the potential for delighting customers regarding data privacy.

#	*Detailed description*	*Reference(s)*
A	**Data Collection**	
A1	**Information.** The purpose, scope, and storage time of the data collection and the involved advantages, risks, resulting rights, and obligations are clearly explained to the customer.	§33 (1) BDSG; §13 (1) TMG; 5 (1.a), 12 (1), 14 (1), 15 EU-GDPR, Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017), Zalando (2017)
A2	**Anonymization.** Customer data are, as good as is possible, stored anonymously to prevent backtracking of individual customers.	§3a BDSG; §13 (6) TMG; 23, 30 (1), 30 (1.a), 30 (2.b) EU-GDPR, Apple (2017), Deutsche Bank (2017)
A3	**Restraint.** Only the customer data absolutely necessary to provide the agreed service are collected. The data are deleted as soon as the purpose of their collection no longer applies.	§3a BDSG; §14 (1), §15 (1) TMG; 5 (1.b), 5 (1.c), 23 EU-GDPR, Deutsche Bank (2017), Dropbox (2017), Facebook (2017)
A4	**Empowerment.** The customer can extend, limit or revoke the permission to store and use his data easily, quickly, free of charge and at any time.	6 (1.a), 6 (1.b), 7 (3), 12 (1.a), 17, 17a, 19 (1) EU-GDPR, Amazon (2017), Apple (2017), Deutsche Bank (2017), Tesla Motors (2017), Zalando (2017)
A5	**Data release.** At the request of the customer and without a long delay, the company provides a set of his personal data free of charge in an easily readable form. Furthermore, the customer has the right to pass these data on to other companies.	12 (1.a), 12 (2), 12 (4), 18 (2) EU-GDPR, Deutsche Bank (2017), easyJet (2017), Facebook (2017), Telekom DE-Mail (2017), Zalando (2017)
B	**Data Combination**	
B1	**Information.** The customer is informed if the company combines his data from various internal and external sources.	5 (1.a), 12 (1), 14a, 15 EU-GDPR, Facebook (2017), Tesla Motors (2017)
B2	**Anonymization.** If the company combines customer data from various internal and external sources, combination and storage are carried out using anonymous data to prevent backtracking of individual customers.	§13 (4), §15 (3) TMG; 23, 30 (1), 30 (1.a), 30 (2.b) EU-GDPR
B3	**Restraint.** If customer data are collected for different purposes, the data sets are stored in different databases and are not combined.	Attachment to §9 (1) BDSG; 13 (4) TMG; 23 EU-GDPR, Deutsche Bank (2017)
B4	**Empowerment.** The customer decides whether the company is allowed to combine data from various internal and external sources and can change his decision at any time.	17a EU-GDPR
C	**Internal Secondary Usage**	

#	*Detailed description*	*Reference(s)*
C1	**Information.** The customer is informed whether and what data are passed on within the company or group of companies and for what purposes.	§13 (5) TMG; 5 (1.a), 12 (1), 14 (1), 15 EU-GDPR, Facebook (2017), Tesla Motors (2017)
C2	**Deletion.** Customer data are deleted as soon as the original reason for the collection no longer applies or the customer withdraws his permission to use his data.	§35 (2) BDSG; §13 (4), §15 (7) TMG; 5 (1.e), 17 EU-GDPR, Deutsche Bank (2017), Dropbox (2017), Facebook (2017)
C3	**Tracking.** Entering, viewing, altering, and deleting customer data are recorded to make it possible to retrace who changed the data when, and in what manner at any time. The customer can either directly view the log file or is informed about any alterations of his personal data.	Attachment to §9 (1) BDSG; 17b, 23 EU-GDPR
C4	**Restraint.** If customer data are collected for different purposes, the data sets are stored in different databases and are not combined.	Attachment to §9 (1) BDSG; 13 (4) TMG; 23 EU-GDPR, Deutsche Bank (2017)
C5	**Empowerment.** Customers have the opportunity to easily decide which of their personal data are shared with other departments of the company and/or used for other purposes.	6 (1.a), 6 (1.b), 12 (1.a), 17a EU-GDPR, Facebook (2017)
D	**External Secondary Usage**	
D1	**Information.** If customer data are passed on to external third parties, the customer is informed.	§13 (5) TMG; 5 (1.a), 12 (1), 14 (1), 15 EU-GDPR, Amazon (2017), Clement and Obar (2016), Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017)
D2	**Guidelines.** If customer data are passed on to external third parties, the company ensures that the data are only used in the manner agreed on with the customer through contracts or binding commitments to data protection regulations.	§11 (1) (2) BDSG; 5 (1.a), 26 (1), 26 (1.a), 26 (2), 26 (2.a), 27, 40, 42 (1), 43 EU-GDPR, Amazon (2017), Dropbox (2017), Clement and Obar (2016), easyJet (2017), Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017)
D3	**Compliance check.** If customer data are passed on to external third parties, the company or an independent certification organization regularly checks the external third party's compliance with data privacy regulations.	26 (1), 26 (1.a) EU-GDPR, Deutsche Bank (2017), Telekom DE-Mail (2017)
D4	**Codification.** If customer data are passed on to external third parties, data are only forwarded in aggregated or codified form (e.g. income class instead of exact yearly income).	Tesla Motors (2017)
D5	**Anonymization.** If customer data are passed on to external third parties, the data are forwarded anonymously.	§30 (1) BDSG; §15 (5) TMG, Amazon (2017)
D6	**Restraint.** The company does not pass on customer data to external third parties.	Tesla Motors (2017)
D7	**Empowerment.** The customer has the choice to easily permit or deny sharing his data with external parties.	7 (3), 12 (1.a), 17, 17a EU-GDPR, Amazon (2017), Apple (2017), Morey et al. (2015), Payne et al. (2015), Zalando (2017)
E	**Errors**	
E1	**Reviews.** Customer data are checked regularly by the company for completeness, accuracy, and being up-to-date.	5 (1.d) EU-GDPR, Payne et al. (2015), Tesla Motors (2017)
E2	**Protective measures.** The company ensures that no customer data are destroyed or lost by technical and organizational means (e. g., double data storage).	Attachment to §9 (1) BDSG; §13 (7) TMG; 22 (1), 23, 30 (1), 30 (1.a), 30 (2.b) EU-GDPR, Telekom DE-Mail (2017), Tesla Motors (2017), Zalando (2017)
E3	**Employee supervision.** Employees with access to customer data are selected carefully, their behavior is checked regularly, and they are held responsible for malpractice.	30 (1.a), 30 (2.b) EU-GDPR, Tesla Motors (2017)
E4	**Tracking.** Entering, viewing, altering, and deleting customer data are recorded to make it possible to retrace who changed the data when, and in what manner at any time. The customer can either directly view the log file or is informed about any alterations to his personal data.	Attachment to §9 (1) BDSG; 17b, 23 EU-GDPR

#	*Detailed description*	*Reference(s)*
E5	**Empowerment.** The customer has access to his data to correct errors, make alterations, or delete data. If he is not provided with direct access to edit his data, they are changed by the company on request.	16 EU-GDPR, Amazon (2017), Apple (2017), Deutsche Bank (2017), Payne et al. (2015), Tesla Motors (2017)
F	**Improper Access**	
F1	**Information.** If the protection of customer data was violated and their security is at risk, the company immediately informs the customer and the authorities.	31 (1), 31 (2), 32 (1) EU-GDPR
F2	**Protective measures.** Storage and transmission of customer data are protected by technical (e.g., password protection, encryption) and organizational means (e.g., access control, dual control principle).	§9 BDSG; Attachment to §9 (1) BDSG; §13 (4), §13 (7) TMG; 5 (1.b), 22 (1), 23, 30 (1.a), 30 (2.b) EU-GDPR, Amazon (2017), Apple (2017), Deutsche Bank (2017), Dropbox (2017), easyJet (2017), Payne et al. (2015), Telekom DE-Mail (2017), Tesla Motors (2017), Zalando (2017)
F3	**Secure server location.** The company ensures that customer data are stored and processed only on its own servers within the European Union or countries trusted by the European Commission.	41 (1) EU-GDPR, Clement and Obar (2016), Telekom DE-Mail (2017)
G	**Reduced Judgment**	
G1	**Information.** The customer is informed whether a decision was made by an automated system or by an employee of the company. At the customer's request, the reasons for the decision are communicated and explained.	§6a BDSG; 5 (1.a), 12 (1), 15 EU-GDPR
G2	**Reviews.** Automated decision processes are continuously tested and checked for deviations.	20 (1), 20 (1.b) EU-GDPR
G3	**Restraint.** Decisions which entail legal consequences (e.g., granting a credit) are never made only on the basis of automated systems.	§6a BDSG; 20 (1), 20 (1.b) EU-GDPR

Table 4.1-2: Measures addressing the seven privacy concerns

4.1.4.2 Customers' evaluation of data privacy measures

Companies need to be aware of the customers' evaluation of these data privacy measures which forms the basis for deriving implications for companies' data privacy policies. To determine the customers' view regarding the different identified data privacy measures, we applied the Kano model in two empirical studies as described in the previous research method section. Table 4.1-3 shows the results. Thereby, the measures are numbered and grouped according to the addressed concerns and named with the short descriptions presented in Table 4.1-2. For both the aviation and the retail survey, we present the category strength and the final categorization of each measure as one of the Kano model factors. The final categorizations were determined following the approach which we described in the previous Kano model section. To illustrate this approach, we use measure A3 as an example. For the aviation survey, the difference between the share of the most and second most frequently chosen factor is 12%, a category strength which is significant at a ten-percent level according to the Fong test. The final categorization thus is the most frequently chosen factor which is of a must-be quality. For the retail survey, the differences between the share of the most (one-dimensional quality)

and second most (attractive quality) frequently as well as the most and third most (must-be quality) frequently chosen factor are not significant according to the Fong test. The (O + A + M) < > (I + R + Q) rule is not applicable as both the most and second most frequently chosen factor belong to the (O + A + M) group. Consequently, the measure is assigned to the mixed category and all three categorizations are listed.

#	Short description	Aviation survey (n = 219)		Retail survey (n = 270)		Accordance
		Category strength	*Categorization*	*Category strength*	*Categorization*	
A	**Data Collection**					
A1	Information	21% *	M	30% *	M	yes
A2	Anonymization	10% *	A	11% *	A	yes
A3	Restraint	12% *	M	3% [2]	Mixed (O, A, M)	partially
A4	Empowerment	18% *	M	3% [2]	Mixed (M, A, O)	partially
A5	Data release[17]	4% [2]	Mixed (M, A, O)	3% [1]	A	partially
B	**Data Combination**					
B1	Information	11% *	I	4% [1]	M	no
B2	Anonymization	8% *	M	11% *	M	yes
B3	Restraint	18% *	I	30% *	I	yes
B4	Empowerment	13% *	A	14% *	A	yes
C	**Internal Secondary Usage**					
C1	Information	21% *	M	20% *	M	yes
C2	Deletion	20% *	M	21% *	M	yes
C3	Tracking	17% *	A	4% [2]	Mixed (A, O, I, M)	partially
C4	Restraint	16% *	A	23% *	I	no
C5	Empowerment	13% *	A	13% *	A	yes
D	**External Secondary Usage**					
D1	Information	49% *	M	46% *	M	yes
D2	Guidelines	58% *	M	45% *	M	yes
D3	Compliance check	17% *	M	22% *	M	yes
D4	Codification	4% [2]	Mixed (M, A, I)	3% [1]	M	partially
D5	Anonymization	34% *	M	24% *	M	yes
D6	Restraint	1% [2]	Mixed (A, O)	6% [2]	Mixed (A, O)	yes
D7	Empowerment	14% *	M	8% *	M	yes
E	**Errors**					
E1	Reviews	60% *	I	64% *	I	yes
E2	Protective measures	49% *	I	32% *	I	yes
E3	Employee supervision	37% *	M	40% *	M	yes
E4	Tracking	4% [1]	A	1% [2]	Mixed (M, A, O, I)	partially
E5	Empowerment	11% *	M	13% *	M	yes
F	**Improper Access**					
F1	Information	42% *	M	43% *	M	yes
F2	Protective measures	40% *	M	44% *	M	yes
F3	Secure server location	4% [1]	A	4% [1]	A	yes
G	**Reduced Judgment**					
G1	Information	11% *	I	17% *	I	yes
G2	Reviews	4% [1]	M	4% [1]	M	yes
G3	Restraint	1% [1]	M	10% *	M	yes

Legend: * = Categorization significant at a ten-percent level according to Fong test; [1] = (O + A + M) < > (I + R + Q) rule applicable; [2] = (O + A + M) < > (I + R + Q) rule not applicable; A = Attractive quality (delighter); O = One-dimensional quality (performance need); M = Must-be quality (basic need); I = Indifferent quality

Table 4.1-3: Empirical results of the data privacy measures' evaluation via the Kano model in two surveys

[17] Due to technical complications in the process of revising and providing the retail survey online, the questions regarding measure A5 were answered by 143 instead of 270 participants.

The results of both the aviation and the retail survey show that in both scenarios, five measures are considered by the participants to be of indifferent quality. These measures do not allow distinctive interpretations toward any direction. In each scenario, 17 out of 32 measures are categorized as basic needs (must-be quality). Furthermore, the categorization as basic need is the most frequent one for two measures belonging to the mixed category in each survey. The realization of these measures is not rewarded. Instead, it is a basic prerequisite when engaging in business with the company. An example for a measure of must-be quality is D2 which addresses the concern External Secondary Usage: if customer data are passed on to external third parties, the company ensures that the data are only used in the manner agreed on with the customer through contracts or binding commitments to data protection regulations. Basic needs can be predominantly found among measures addressing the concerns External Secondary Usage (5-6 measures out of 7 categorized as a basic need in both scenarios), Improper Access (2/3), and Reduced Judgment (2/3). They are also frequently found among measures addressing the concern Data Collection (3/5) in the aviation scenario. These basic needs can be considered a necessary evil because they have downside risks if not implemented but offer no upside opportunities if implemented. In both surveys, no measure is considered to be a performance need. However, this factor occurs among the most frequent categorizations in the mixed category for two measures in the aviation and four measures in the retail scenario. The constituting properties of a performance need are, in addition to having a negative impact if not implemented, that it also might increase customer satisfaction when implemented properly.

Seven measures are categorized as delighters in the aviation scenario and five in the retail scenario. Furthermore, three delighters occur among the most frequent categorizations in the mixed category in the aviation scenario and five in the retail scenario. The implementation of these measures is not required by the customers but may please them. Not implementing these measures has no negative impact. These measures go beyond the data privacy measures which customers expect. In the aviation scenario, delighters can be predominantly found among measures addressing the concern Internal Secondary Usage (3 measures out of 5 categorized as a delighter). In the retail scenario, the delighters are distributed over measures addressing four different concerns and there is no concentration observable. In both scenarios, customers can be delighted by storing their data in an anonymized form (A2), empowering them with regard to the combination of their data (B4) and data sharing within the company (C5), and storing their data on servers with a secure location (F3).

Overall, there are eight (25%) measures which exhibit different categorizations in the aviation scenario as compared to the retail scenario. They address five different concerns and include all Kano model factors with the previously mentioned exception of performance needs. For three of these measures, the categorization in one of the scenarios corresponds to the most frequent result of the mixed category categorization in the other scenario. That is, these categorizations are not equal but the tendencies are similar. The remaining 24 measures are categorized in the same way by participants of the aviation and the retail survey. These measures address all seven concerns and include all Kano model factors. All measures addressing the concerns Improper Access and Reduced Judgment exhibit the same results. To assess the reliability of the measure categorizations across the two different scenarios, we conducted a test of inter-rater reliability with two raters. Thereby, the categorizations of measures in the aviation scenario as shown in Table 4.1-3 were interpreted as the choice of the first rater and those of the retail scenario as the choice of the second rater. The percent agreement is 0.75 and the Cohen's Kappa is 0.61, indicating a substantial strength of agreement according to Landis and Koch (1977).

The similarity of the measures' categorizations is also reflected in Figure: 4.1-3. It represents a satisfaction-dissatisfaction diagram of the results of both surveys. The x-coordinate indicates the satisfaction coefficient, the y-coordinate states the dissatisfaction coefficient. We present the data points for both scenarios and connect them with a line. Few measures exhibit relatively large differences between the aviation and the retail surveys' results (e.g., A4, C3 and C4) while the data points for the majority of measures are in rather close proximity to their counterparts. The indication of high reliability of the 32 measures' satisfaction and dissatisfaction coefficients across the two scenarios is confirmed by their high and highly significant Pearson's correlations: 0.91 (p-value << 0.001) for the satisfaction coefficients and 0.96 (p-value << 0.001) for the dissatisfaction coefficients.

We limited the range of the axes to the actually occurring values for better readability. The fact that the dissatisfaction coefficient's axis exhibits a broader range than the satisfaction coefficient's axis as well as the relatively high concentration of measures in the bottom left quadrant emphasize the dominance of measures of must-be quality. They will decrease the overall customer satisfaction if not implemented but will only moderately increase it if implemented. However, the opposite case can be observed as well. Implementing measure B4, for example, has the potential to increase the overall satisfaction of a notable share of survey participants while not implementing it will have a relatively small negative effect.

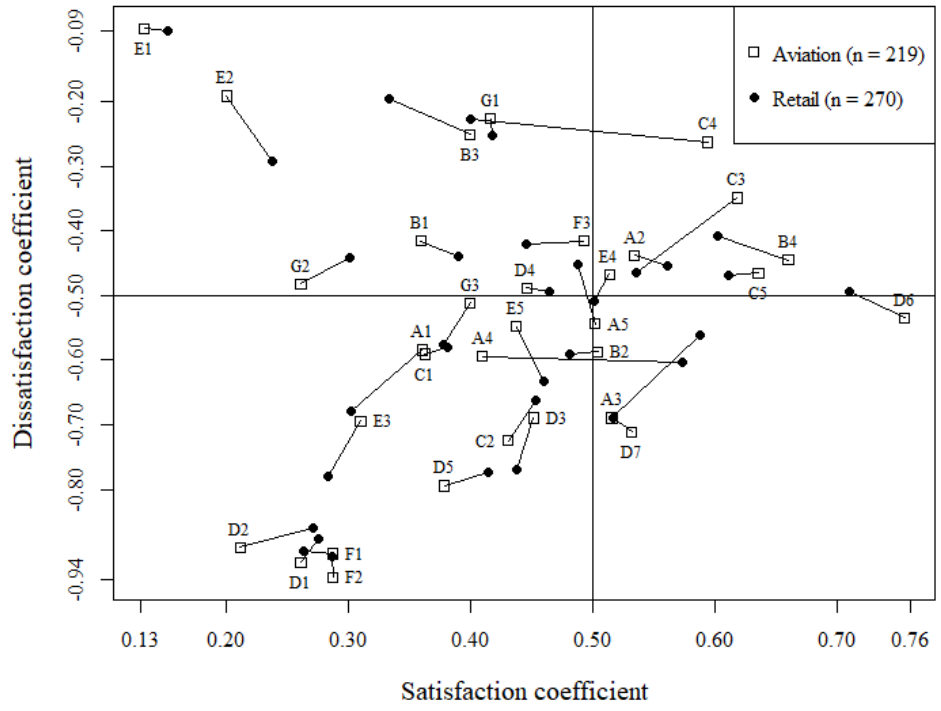


Figure: 4.1-3: Joint satisfaction-dissatisfaction diagram of the results of both surveys

These results are underlined by a more detailed look at the categorization of measures on the participant-level. For both scenarios, Table 4.1-4 presents the minimum, median, mean and maximum count of categorizations as a specific Kano model factor per survey participant. It also indicates the share of participants who categorized zero and at least ten measures as the specific Kano model factor. Measures of must-be quality are dominant: more than 60% of the participants of both surveys categorized more than 10 of our 32 measures as such basic needs. However, only 8% of participants of the aviation survey and 9% of participants of the retail survey evaluated none of the measures as attractive. This implies that data privacy has the overall potential to improve the satisfaction of a very large share of customers: 92% (aviation) and 91% (retail) see at least one data privacy measure as delighter, that is, as a measure with upside potential only. 32% (aviation) and 29% (retail) categorized more than 10 measures as such delighters. All but one (99.5%, aviation) and all but six (97.8%, retail) survey participants categorized at least one measure as performance need or delighter, that is, as a measure with upside potential.

	Aviation survey (n = 219)						Retail survey (n = 270)					
	min	*med*	*mean*	*max*	*none*	*>= 10*	*min*	*med*	*mean*	*max*	*none*	*>= 10*
Attractive quality	0	7	7,4	21	8%	32%	0	6	6,7	25	9%	29%
One-dimensional quality	0	5	6,2	28	7%	20%	0	5	6,4	30	9%	21%
Must-be quality	0	11	11,1	29	3%	60%	0	11	10,7	30	5%	62%
Indifferent quality	0	6	7,0	28	5%	26%	0	6	7,3	30	3%	28%
Reverse quality	0	0	0,3	4	78%	0%	0	0	0,3	10	84%	0%
Questionable result	0	0	0,1	5	95%	0%	0	0	0,1	7	93%	0%

Table 4.1-4: Statistics regarding the number of categorizations per Kano model factor and survey participant

4.1.5 Discussion

4.1.5.1 Theoretical contribution

This paper contributes to the body of knowledge about data privacy. Most scientific and practitioner-oriented literature describes data privacy as necessary evil that organizations have to deal with in order to mitigate risks. We shed light on the upside of data privacy beyond mere risk management. Our paper consists of two main contributions. First, we created a set of 32 specific data privacy measures that address the customers' seven main data privacy concerns. We derived these measures from several legislative texts of the German and European law system as well as from scientific and practitioner-oriented literature and corporate privacy statements. With the consideration of the European General Data Protection Regulation (EU-GDPR) which will become applicable law in May 2018, we took a future-oriented perspective and incorporated the most recent legislation into our research. The consolidated and enriched set of measures from several sources was evaluated in discussions with data privacy experts. It can serve as a basis for the development of further data privacy concepts and strategies. Second, we provided an evaluation of these data privacy measures by customers. Via two online surveys, we empirically captured customers' perceptions of the identified data privacy measures as must-be, one-dimensional, attractive, or as indifferent. A similar classification of most measures across both surveys showed a consistent and reliable picberture of customer sentiment. A further analysis of the survey responses with a satisfaction-dissatisfaction diagram strengthened the dominating assertion of data privacy measures as necessary evil. However, among both industry scenarios, we showed that the implementation of certain data privacy measures has the potential to delight customers. The vast majority of participants could be delighted with data privacy measures and almost a third of all participants could be delighted by 10 or more measures. Our research specifically highlights the upside of data privacy. In summary, the customers' evaluation of data privacy measures as presented in this

paper is a starting point for all researchers who try to understand customer sentiment toward specific measures and data privacy in general.

4.1.5.2 Limitations

Researchers and practitioners should be aware of the limitations of this research. First, the derivation of data privacy measures focused on Germany and Europe. Other regions with different cultures and legislative systems might yield other or further measures. Second, the results of the empirical part of this research should only be interpreted in a company- and customer-specific manner. We selected the booking process for a flight and the online purchase of a product to present realistic scenarios to our survey participants who were predominantly students, that is, potential customers of the present and future. To verify the validity of the conclusions for other industry scenarios and customer groups, the survey and analyses have to be rerun as presented in this paper. Third, in the field of data privacy, statements of customers in empirical surveys do not necessarily match their actions in the real world. The so-called privacy paradox describes the discrepancy between customers' intentions to protect their own privacy and their real-world behavior (Acquisti & Grossklags, 2005; Norberg et al., 2007). The survey answers may be further biased as all data privacy measures were introduced with a description of the concern they address. This concern may not always be present to customers in real life. To take into account this limitation, the results of the survey should be verified in real-world situations not specifically referring to privacy concerns. Fourth, in general, the classification of delighters is less clear than the classification of basic needs. That is, when interpreting this paper's results, implications should be challenged according to the principle of prudence. Future research could follow Matzler et al. (1996) who state that unclear results spread out over several categories can be a starting point for market segmentation.

4.1.5.3 Managerial implications

This paper provides advice to practitioners working in the field of data privacy and thinking about the implementation of certain data privacy measures and an overarching data privacy strategy. Our paper provides practitioners with an overview of possible data privacy measures specifically addressing customers' concerns regarding data privacy. Practitioners also get first insights into the measures' contribution to customer satisfaction and potential for a competitive advantage. Based on the measures' categorization, companies may implement different pricing strategies which take into account the level of data privacy related to a certain product.

For instance, companies may offer a basic product which merely comprises the implementation of basic and performance needs and a more expensive luxury product which additionally entails the implementation of all privacy measures that are categorized as delighters.

Overall, our research indicates that companies can delight the vast majority of customers with appropriate data privacy measures. Though companies might not want to implement every measure that delights customers, they can lever our research in the trade-off between customer excitement, economic value, regulatory requirements, and technical feasibility when deciding between the implementation of individual measures. To establish a generic and systematic "privacy by design" process which goes beyond mere technical solutions (Danezis et al., 2015), companies could follow the procedure of our research. A rational first step could be the derivation of a data privacy strategy that aligns with the overarching company strategy. Companies could gather their existing and potential future customers' concerns with regard to data privacy leveraging the work of Smith et al. (1996). Furthermore, companies could use our set of data privacy measures as a starting point and elaborate measures that specifically address the concerns of their customers. As demonstrated in this paper, companies could get insights into the relationship between individual data privacy measures and customer satisfaction by asking for their customers' evaluation. Considering their data privacy strategy and their customers' evaluation, companies could implement respective measures and measure their performance. Results from the performance measurement could serve as an input for adjustments of the company's data privacy strategy. To decide on the implementation of a data privacy strategy and particular measures, companies should nevertheless employ an interdisciplinary team which works on data privacy related topics and particularly includes a customer perspective besides a legal one.

4.1.6 Conclusion and further research

Answering the first research question, this paper provides an overview of data privacy measures collected from scientific and practitioner-oriented literature, legislative texts, and corporate privacy statements and evaluated by expert interviews. In addition, this paper provides first insights into customers' perceptions of the identified data privacy measures. By using the Kano model to design two online surveys, each with more than 200 participants, we could show that the majority of data privacy measures must be considered as necessary evils for companies. Nevertheless, both surveys highlighted the upside of data privacy, as almost all potential customers could be delighted with at least one measure. Thus, this paper positively answers the research question whether some measures are perceived as attractive and

can delight customers. Their implementation might even lead to a competitive advantage for companies. Accordingly, researchers and practitioners may use our approach as an inspiration when deriving a data privacy strategy. The list of measures may be useful. Evaluating customers' perception may assist in prioritizing the implementation of data privacy measures.

As every research endeavor, our paper leaves room for future research. Firstly, future research could focus on the evaluation of the general validity of our research in other industries than aviation and retail and with other customer groups. Secondly, researchers could segment customers by age, career, education, and other criteria in order to isolate groups that can be especially delighted with data privacy and derive strategies for those customers who do not. Thirdly, a decomposition of single data privacy measures in its individual components could shed light on the influence of individual aspects of a data privacy measure on customers' satisfaction. Fourth, researchers could further investigate the reasons why an individual data privacy measure is classified as one of the factors of the Kano model to better understand customers' sentiment towards data privacy in general.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the 27th International Conference on Information Systems (ICIS)*, Milwaukee, United States of America.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Ahmad, A., & Mykytyn, P. (2012). Perceived privacy breach - The construct, the scale, and its antecedents. In *Proceedings of the 18th Americas Conference on Information Systems (AMCIS)*, Seattle, United States of America.

Amazon. (2017). *Amazon.de-Datenschutzerklärung*. https://www.amazon.de/gp/help/customer/display.html?nodeId=3312401. Accessed on 2017-10-23.

Apple. (2017). *Apple Datenschutzrichtlinie*. https://www.apple.com/legal/privacy/de-ww/. Accessed on 2017-10-23.

Arbore, A., & Busacca, B. (2009). Customer satisfaction and dissatisfaction in retail banking: Exploring the asymmetric impact of attribute performances. *Journal of Retailing and Consumer Services*, *16*(4), 271–280.

Audatis Consulting. (2016). *Checkliste: Technische und organisatorische Maßnahmen*. https://www.audatis.de/wp-content/uploads/Checkliste_Datenschutz_TOM_nach_9_BDSG.pdf. Accessed on 2016-08-18.

Bartikowski, B., & Llosa, S. (2004). Customer satisfaction measurement: Comparing four methods of attribute categorisations. *The Service Industries Journal*, *24*(4), 67–82.

BBC. (2015). *Ashley Madison infidelity site's customer data 'leaked'*. http://www.bbc.com/news/business-33984017. Accessed on 2017-05-10.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM*, *48*(4), 101–106.

Berger, C., Blauth, R., Boger, D., Bolster, C., Burchill, G., DuMouchel, W., Pouliot, F., Richter, R., Rubinoff, A., Shen, D., Timko, M., & Walden, D. (1993). Kano's methods for understanding customer-defined quality. *Center for Quallity Management Journal*, *2*(4), 3–36.

Buchmann, E., Böhm, K., & Raabe, O. (2008). Privacy 2.0: Towards collaborative data-privacy protection. In Y. Karabulut, J. Mitchell, P. Herrmann, & C. D. Jensen (Chairs), *Proceedings of IFIPTM 2008*.

Buhl, H. U. (2013). IT as curse and blessing. *Business & Information Systems Engineering*, *5*(6), 377–381.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69–104.

Clayton, E., & Hilz, A. (2015). *2015 aviation trends*. http://www.strategyand.pwc.com/perspectives/2015-aviation-trends. Accessed on 2016-08-18.

Clement, A., & Obar, J. A. (2016). Keeping internet users in the know or in the dark: An analysis of the data privacy transparency of Canadian internet carriers. *Journal of Information Policy*, *6*, 294–331.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Métayer, D. Le, Tirtea, R., & Schiffner, S. (2015). *Privacy and data protection by design - From policy to engineering*. Athens. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. Accessed on 2017-04-25.

Deutsche Bank. (2017). *Datenschutz*. https://www.deutsche-bank.de/pfb/content/pk-datenschutz.html. Accessed on 2017-10-23.

Dhasarathan, C., Thirumal, V., & Ponnurangam, D. (2015). Data privacy breach prevention framework for the cloud service. *Security and Communication Networks*, *8*(6), 982–1005.

Dropbox. (2017). *Dropbox-Datenschutzrichtlinie*. https://www.dropbox.com/privacy. Accessed on 2017-10-23.

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214–220.

easyJet. (2017). *Datenschutzerklärung*. https://www.easyjet.com/de/politik/datenschutzerklarung. Accessed on 2017-10-23.

Facebook. (2017). *Datenrichtlinie*. Facebook. https://de-de.facebook.com/about/privacy. Accessed on 2017-10-23.

Fong, D. (1996). Using the self-stated importance questionnaire to interpret Kano questionnaire results. *Center for Quallity Management Journal*, *5*(3), 21–23.

Füller, J., & Matzler, K. (2008). Customer delight and market segmentation: An application of the three-factor theory of customer satisfaction on life style groups. *Tourism Management*, *29*(1), 116–126.

Gronholdt, L., Martensen, A., & Kristensen, K. (2000). The relationship between customer satisfaction and loyalty: Cross-industry differences. *Total Quality Management*, *11*(4-6), 509–514.

The Guardian. (2011). *iPhone keeps record of everywhere you go*. https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears. Accessed on 2017-05-10.

Hackl, P., & Westlund, A. H. (2000). On structural equation modelling for customer satisfaction measurement. *Total Quality Management*, *11*(4-6), 820–825.

Harris, E. C. (2007). Personal data privacy tradeoffs and how a Swedish church lady, Austrian public radio employees, and transatlantic air carriers show that Europe does not have the answer. *American University International Law Review*, *22*(5), 745–799.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275–298.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

Inman, J. J., & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing*, *93*(1), 7–28.

Kano, N., Seraku, N., Takahashi, F., & Tsuji, S. i. (1984). Attractive quality and must-be quality. *The Journal of the Japanese Society for Quality Control*, *14*(2), 147–156.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: Consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction*, *8*(3), 88–130.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148.

Klingspor, V. (2016). Why do we need data privacy? In S. Michaelis, N. Piatkowski, & M. Stolpe (Eds.), *Solving Large Scale Learning Tasks: Challenges and Algorithms* (pp. 85–95). Springer.

Ladhari, R. (2009). A review of twenty years of SERVQUAL research. *International Journal of Quality and Service Sciences*, *1*(2), 172–198.

Lai, H.-J., & Wu, H.-H. (2011). A case study of applying Kano's model and ANOVA technique in evaluating service quality. *Information Technology Journal*, *10*(1), 89–97.

Landis, R. J., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*, 159–174.

Lee, M. C., & Newcomb, J. (1996). Applying the Kano methodology in managing NASA's science research program. *Center for Quallity Management Journal*, *5*(3), 13–20.

Löfgren, M., & Witell, L. (2008). Two decades of using Kano's theory of attractive quality: A Literature Review. *The Quality Management Journal*, *15*(1), 59–75.

Lyons, V., van der Werff, L., & Lynn, T. (2016). Ethics as pacemaker: Regulating the heart of the privacy-trust relationship. A proposed conceptual model. In *Proceedings of the 37th International Conference on Information Systems (ICIS),* Dublin, Ireland.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Mamonov, S., & Koufaris, M. (2014). The impact of perceived privacy breach on smartphone user attitudes and intention to terminate the relationship with the mobile carrier. *Communications of the Association for Information Systems*, *34*(60).

Matthing, J., Sandén, B., & Edvardsson, B. (2004). New service development: Learning from and with customers. *International Journal of Service Industry Management*, *15*(5), 479–498.

Matzler, K., Hinterhuber, H. H., Bailom, F., & Sauerwein, E. (1996). How to delight your customers. *Journal of Product & Brand Management*, *5*(2), 6–18.

Matzler, K., & Stahl, H. K. (2000). Kundenzufriedenheit und Unternehmenswertsteigerung. *Die Betriebswirtschaft*, *60*, 626–641.

Mohammed, R. (2014). *Why Amazon should unbundle Prime*. https://hbr.org/2014/02/why-amazon-should-unbundle-prime. Accessed on 2017-10-12.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*(May), 96–105.

Moshki, H., & Barki, H. (2016). Coping with information privacy breaches: An exploratory framework. In *Proceedings of the 37th International Conference on Information Systems (ICIS),* Dublin, Ireland.

Muntermann, J., & Roßnagel, H. (2009). On the effectiveness of privacy breach disclosure legislation in Europe: Empirical evidence from the US stock market. In A. Jøsang, T. Maseng, & S. J. Knapskog (Chairs), *Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age*.

Nicholas-Donald, A., Matus, J. F., Ryu, S., & Mahmood, A. M. (2011). The economic effect of privacy breach announcements on stocks: A comprehensive empirical investigation. In *Proceedings of the 17th Americas Conference on Information Systems (AMCIS),* Detroit, United States of America.

Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). The economic impact of privacy violations and security breaches. *Business & Information Systems Engineering*, *6*(6), 339–348.

Nofer, M., Hinz, O., Muntermann, J., & Rossnagel, H. (2014). The economic impact of privacy violations and security breaches. *Business & Information Systems Engineering*, *6*(6), 339–348.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126.

Otto, B. (2011). Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. *Communications of the Association for Information Systems*, *29*(3), 45–66.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A conceptual model of service quality and its implications for future research. *Journal of Marketing*, *49*(4), 41–50.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, *35*(4), 977–988.

Payne, D., Landry, B. J. L., & Dean, M. D. (2015). Data mining and privacy: An initial attempt at a comprehensive code of conduct for online business. *Communications of the ACM*, *37,* Article 34.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, *71*(12), 1133–1143.

Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy: An experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research*, *13*(4), 423–455.

Saarijärvi, H., Grönroos, C., & Kuusela, H. (2014). Reverse use of customer data: Implications for service-based business models. *Journal of Services Marketing*, *28*(7), 529–537.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, *46*(2), 111–126.

Schaule, M. (2014). *Anreize für eine nachhaltige Immobilienentwicklung: Nutzerzufriedenheit und Zahlungsbereitschaft als Funktion von Gebäudeeigenschaften bei Büroimmobilien* [Doctoral thesis]. Fakultät für Bauingenieur- und Vermessungswesen, Munich.

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, *34*(3), 593–603.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196.

Tanner, A. (2013). *Here are some of America's most privacy friendly companies*. http://www.forbes.com/sites/adamtanner/2013/09/11/here-are-some-of-americas-most-privacy-friendly-companies/. Accessed on 2016-11-02.

The Telegraph. (2010). *Facebook admits 'inadvertent' privacy breach*. http://www.telegraph.co.uk/technology/facebook/8070513/Facebook-admits-inadvertent-privacy-breach.html. Accessed on 2017-05-07.

Telekom DE-Mail. (2017). *Datenschutzhinweise für De-Mail der Telekom Deutschland GmbH*. http://www.telekom.de/dlp/agb/pdf/42734.pdf. Accessed on 2017-10-23.

Tesla Motors. (2017). *Datenschutzerklärung*. https://www.tesla.com/sites/default/files/pdfs/de_DE/tmi_privacy_statement_external_6-14-2013_v2.pdf. Accessed on 2017-10-23.

Zalando. (2017). *Datenschutzerklärung und Einwilligung zur Datennutzung*. https://www.zalando.de/zalando-datenschutz/. Accessed on 2017-10-23.

4.2 Privacy bots - digital assistants for more transparency on the internet

Abstract: Page-long privacy statements are often accepted blindly on the internet. As digital helpers, so-called privacy bots contribute to strengthening the digital sovereignty of internet users by automatically evaluating privacy statements. This article presents a user-assessed concept for a privacy bot and provides three options for evaluating privacy statements.

Authors: Niclas Nüske, Christian Olenberger, Daniel Rau, Fabian Schmied

Status: This article is published in Datenschutz und Datensicherheit, Volume 43, Issue 1, pp. 28-32 (2019)[18].

[18] The original article was published in German and was translated into English for this dissertation.

4.2.1 Introduction

Encouraged by numerous scandals, the protection of personal data is increasingly becoming the focus of public attention. The scandal surrounding Facebook and Cambridge Analytica in particular made headlines. In this context, the disclosure of personal data of 87 million Facebook users aroused great suspicion, primarily due to the cooperation of Cambridge Analytica with the campaign team of the current U.S. President Donald Trump. A data privacy scandal that is far less well known to the general public took place in Austria. In 2018, it became known that the telecommunications service provider A1 had unauthorizedly stored connection and location data of several tens of thousands of users over a period of years[19].

As a result, customers nowadays attach greater importance to ensuring that their personal data is adequately protected. In Germany, the Federal Data Protection Act (BDSG), which first came into force in 1990, provides a legal framework for this. Since May 2018 at the latest, companies in EU member states have also had to comply with the guidelines of the European General Data Protection Regulation (EU GDPR).

In the course of this development, companies that feel particularly committed to the protection of personal data have also been established for some time. For example, unlike other providers, the search engine “DuckDuckGo” explicitly refrains from storing users' personal data. Established companies and corporations are also increasingly addressing the issue. For example, the telecommunications service provider “Telefónica” announced back in 2016 that it would offer its customers complete transparency regarding the personal data it collects[20]. Accordingly, customers would be allowed to decide for themselves which data is used by the company and, if necessary, passed on to third parties. If customers provide personal data, they should receive attractive offers from partner companies in return. However, the app “O_2 Get”[21], which was developed in this context together with the start-up people.io, does not seem to have established itself sustainably at this point in time and is viewed critically by many users.

4.2.2 Current situation

Due to mostly very long and cryptic data protection declarations, users currently often do not have a sufficient overview of what data is collected, stored, and processed when using an

[19] https://www.heise.de/newsticker/meldung/Datenschutzskandal-bei-Telekom-Austria-3989557.html
[20] https://www.zeit.de/digital/datenschutz/2016-09/mobilfunk-telefonica-bewegungsdaten-kunden-verkaufen-zweiter-versuch
[21] https://blog.telefonica.de/2017/05/kooperation-von-telefonica-next-mit-people-io-app-o2-get-ermoeglicht-souveraenen-umgang-mit-eigenen-daten/

internet service. Since the effort required to read and understand a data protection statement is usually out of all proportion to the benefits of an internet service, many internet users often choose to blindly accept the data protection statement. The Federal Ministry of Justice and Consumer Protection (BMJV) has therefore been working for some time to ensure that data protection notices are presented more transparently. Under the motto "data protection at a glance", a user-friendly, clear and comprehensible summary of the data protection information should ideally be provided as a so-called one-pager. However, only a few companies have followed this suggestion so far. In addition, initial studies show that the level of knowledge of internet users is only slightly improved by one-pagers[22].

Another promising solution for strengthening the digital sovereignty of internet users and protecting personal data are so-called privacy bots. These are intended to help provide a quick overview of an internet service's privacy policy. Accordingly, the evaluation of privacy statements no longer even requires the reading of a one-pager but is at best automated and based on individual user preferences. In the following, we present a concept for a privacy bot that is intended to enable internet users to surf the internet without interruption and still be always informed about how the internet services they visit process personal data, what measures are taken to protect the data, and how they match the users' preferences. For this, we present the concept for a privacy bot website that can be simultaneously integrated directly into the user's browser via a plug-in to help them surf the web.

4.2.3 Relevant dimensions of data protection on the internet

The basis for the conception of the privacy bot and its easy-to-understand preparation of a privacy policy is a clear division of the content into assessable criteria. In identifying suitable higher-level categories, we relied on the one-pager[23] of the Federal Ministry of Justice and Consumer Protection. This is intended to supplement the formal privacy statement and lists the following four central questions: What data is collected? What technologies are used? How will data be used? Where is the data shared? Through a detailed evaluation of exemplary data protection declarations from five companies, we identified possible characteristics, henceforth referred to as criteria, each of which can be assigned to one of the four categories. The companies were selected with the intention of covering different industries, company sizes and degrees of innovation with regard to data protection. For this purpose, a sentence-

[22] https://www.conpolicy.de/data/user_upload/Studien/PolicyPaper_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf
[23] https://www.bmj.de/SharedDocs/Downloads/DE/Verbraucherportal/OnePager/11192915_OnePager-Datenschutzhinweise.pdf?__blob=publicationFile&v=3

level analysis of data privacy statements (for example, those of Amazon and Deutsche Bank) was conducted. Individual criteria were identified in the data privacy statements and grouped across all companies according to similarity in content. In discussions among the author team, these groups were condensed into individual questions to be answered in a binary fashion.

A total of 19 criteria were identified. The category "What data is collected?" includes criteria such as user input, location data, and usage data. In the category "How is the data used?", for example, the provision of the service and advertising are represented as possible purposes. For each of the 19 criteria in the four superordinate categories, a simple "yes" or "no" can be used to indicate how a company positions itself in terms of data protection.

4.2.4 Possible functions and their evaluation by users

A core function of the privacy bot is the basically one-time, but customizable storage of individual privacy preferences for the aforementioned criteria. For example, a user may consent to the collection of location data while objecting to its use for advertising. Agreement or disagreement in each of the 19 criteria adds up to a data protection profile of the user that summarizes his or her wishes. Each of the criteria can be explained by simple help texts if required.

The privacy bot allows the internet user to create multiple privacy profiles. For example, a relatively carefree privacy profile for online shopping and a very strict privacy profile for online banking. In this way, the privacy bot takes different data protection requirements into account. To create a privacy profile, the internet user registers once on the privacy bot website. After at least one data protection profile has been stored, the privacy bot enables internet services to be checked against the stored data protection preferences.

The internet user has two options for testing an internet service. Either he enters the URL of the internet service to be checked into the *privacy bot's website* or he uses the associated *browser plug-in*, which automatically checks internet services while surfing. The concept of browser plug-ins is already being used successfully by almost a quarter of all German internet users in the form of ad blockers[24]. If the internet user checks an internet service via the website or automatically in the background via the browser plug-in, the privacy bot checks the privacy statement of the internet service and compares it with the privacy profile stored by the internet user. The internet user thus receives at a glance the answer to the question of whether the corresponding internet service acts along the associated privacy profile of the internet user. If the internet service violates the privacy preferences of the internet user in individual criteria,

[24] https://de.statista.com/statistik/daten/studie/537062/umfrage/adblocker-rate-in-deutschland/

the violations are summarized in a clear form. If required, the internet user can view details of the violations. For the internet user, the privacy bot eliminates the need for time-consuming manual checks of data protection declarations. In this way, the user retains his digital sovereignty or regains it in comparison to the currently widespread "blind acceptance" of data protection declarations. Through the privacy bot, the user is faced with considerably increased transparency with regard to the collection and use of his personal data. In addition to storing privacy preferences and checking internet services against the stored privacy profiles, our privacy bot concept includes several other functionalities. In this way, internet services that have been checked once can be stored in the privacy bot. Regularly and automatically repeated checks of the internet services in the background enable the internet user to be made aware of concretely changed data protection regulations or special incidents in connection with data protection at the internet service. A subsequent change in data protection preferences by the internet user would then also allow a retrospective review of all internet services already checked once. Direct links to the privacy settings on subpages of an internet service also make it easier for internet users to exercise their privacy-related choices. The privacy bot thus becomes the central point of contact for privacy settings for a sovereign internet user. Simple and short help texts support the internet user without burdening him with the effort of difficult-to-understand, page-long data protection declarations - detailed reading by the internet user is of course still possible.

A survey of 78 internet users and thus also potential users of the presented privacy bot indicates that the functionality and actual use of the privacy bot is also in demand by internet users. Survey participants were provided with a clickable prototype of the privacy bot for demonstration. Subsequently, internet users rated the usefulness of the privacy bot with an average of 5.13 (out of 7) points. The presented basic functionality of the privacy bot achieved an average rating of 4.79 (out of 7) points. Ultimately, internet users expressed their intention to actually use the privacy bot with an average score of 4.83 (out of 7). The survey results indicate that the concept of privacy bots is already perceived by a large proportion of internet users as a restoration of digital sovereignty on the internet. Through its functionality, the privacy bot can make a decisive contribution to preventing the "blind acceptance" of data protection declarations in internet services and to strengthening the enforcement of choices with regard to data protection.

4.2.5 Options for evaluating privacy statements

For a broad applicability of the privacy bot, however, a large number of privacy statements must be checked for their conformity with the user's preferences, as automatically as possible. Three implementation options are particularly suitable for this purpose. Privacy statements could be reviewed *manually* by dedicated professionals or using a crowd approach by privacy bot users. It is also conceivable to automatically compare a user's privacy preferences with the information provided by an internet service and to define choices via a standardized *program interface*. Lastly, an algorithmically automated evaluation of the privacy statements using *text mining methods* should be mentioned. The three alternatives will each be explained in more detail below.

4.2.5.1 Manual testing

Privacy statements are analyzed manually by experts, analogous to the authors' procedure for this paper, and the result of the compliance check is recorded for each of the 19 criteria. User preferences are then matched with these evaluations. This option would be advantageous because a high level of quality could be ensured through manual evaluation by experts. A clear disadvantage of the option is the necessary effort.

A crowd-driven approach that engages privacy bot users in evaluating privacy statements may be a more promising variation on manual review. Before a user is given access to the privacy bot features, he or she is asked to review a specific privacy policy or part of it. The quality of the evaluations is ensured by a sufficiently large number of users and on the basis of the majority opinion. The manual evaluation in the crowd approach has the consequence that the number of web pages that can be checked by the privacy bot only increases gradually. Therefore, especially in the start-up phase, attention must be paid to appropriate incentives.

4.2.5.2 Interface setup

An interface is created between the privacy bot and the internet service used, which allows the automatic exchange of information about the respective privacy policy as well as the automatic implementation of settings according to the user's preferences. For this purpose, the list of 19 criteria organized into the four categories presented is converted into a standard machine-readable format such as XML or JSON. This is provided to website operators, each of which indicates whether or not they meet the criteria included and whether the user is given the right to choose. If an item is optional, it can be omitted by the company or the operator at the user's request. If it is not optional, the user must accept it if he wishes to use the internet

service. If a user now visits the website of an internet service, the privacy bot compares the user's specifications with those of the website operator. The result of the matching is fed back to the operator by the privacy bot, whose system then sets all optional items according to the specifications. The user's evaluation of data protection preferences thus shows the optimum achievable level of data protection on the respective website. This is only possible if the operator of the internet service is actively involved, so that here, too, attention must be paid to suitable incentives.

4.2.5.3 Text mining

A variant of automated evaluation is the application of text mining methods. Text mining is a group of methodological approaches used to structure texts in order to extract information from them. The evaluation of privacy statements with text mining is done in four steps.

First, a criterion is selected from the user's privacy preferences, for example, the collection of location data. In the second step, the privacy policy of the internet service is retrieved and searched for relevant paragraphs that relate to the selected criterion. This can happen either with a proprietary text mining method or through a specialized online service. In the third step, text mining is used to analyze the identified text passages to determine whether the respective criterion is met. For this purpose, the search for key formulations lends itself. In the case of location data, such phrases could include "use", "do not use", "usage", "no usage", "employ", "do not employ", "avoid", etc. When using a standard statistical method such as classification, the vector method or hierarchical cluster analysis, a sufficiently large training data set must be created, which must contain common phrases from data protection statements and the respective statement "positive/yes/implementation" or "negative/no/no implementation". Once derived from privacy statements, the training dataset can be further used to assess new privacy statements. Once a conformity evaluation is available, this information can be matched with the user's preferences in the final step.

The advantage of the fast and automated evaluation of arbitrary privacy statements after a sufficiently large training phase is offset by high implementation costs and know-how requirements for text mining.

4.2.6 Monetization as part of a business model

All three methods presented for evaluating privacy statements of internet services can already be implemented with today's methods and enable the presented privacy bot concept from the

technical side. However, all three methods involve effort on the part of the privacy bot operator. By being designed as a digital platform, the privacy bot represents a scalable concept. Once evaluated, privacy statements of internet services would be immediately available to all users. Nevertheless, the implementation and operation of the privacy bot involves financial effort.

Due to its special importance for the digital sovereignty of internet users, a non-profit financing concept is conceivable for the privacy bot, as is already being successfully implemented by the Wikipedia knowledge database. Government funding to secure and enforce the digital sovereignty of internet users is also possible.

An alternative to this is monetization via a private-sector business model. On the one hand, the privacy bot can supplement an existing service offering. For example, as a free supplement to the internet contracts of a telecommunications service provider. On the other hand, the privacy bot can also be monetized as a standalone service. In this case, users would pay a one-time fee, a regular fee, or a fee based on the number of checks. A survey of 78 internet users, to whom the privacy bot was presented in detail, showed the first signs of a different willingness to pay. Just under half of all respondents indicated a basic willingness to pay for the privacy bot, whereas the other half preferred to use the digital helper free of charge.

Against this background, offering the privacy bot in a freemium model is a possible option. Basic functionalities such as manual checking of internet services on the privacy bot's website would be offered free of charge in such a freemium model. In this case, the full range of functions, for example the use of the browser plug-in for automatic background checks or the storage of checked internet services, would only be usable against payment.

Freemium models have already been successfully implemented by internet services such as Spotify, OneDrive or Boxcryptor. The latter enables fully automatic encryption of data in cloud storage services such as OneDrive, Dropbox or Google Drive. In the free basic version, basic functionalities can be used; the paid full version contains the entire range of functions.

Non-profit financing concept, state-funded service or private-sector business model - various monetization forms are conceivable for our privacy bot concept.

4.2.7 Evolution towards a data safe

The concept of a privacy bot presented above already takes a first step toward strengthening the digital sovereignty of internet users. Sensible further developments would be the implementation of an identity management solution or even a data safe for the individual release of

personal data. Provided that the privacy bot is offered by a governmental institution, a scientific organization or comparatively trustworthy companies like Deutsche Telekom or Deutsche Post, the implementation of an identity management solution is a first advancement. At the beginning, the internet user verifies his identity once to the privacy bot. Subsequently, it would be conceivable to verify the internet user against other internet services without verifying the identity again. Traditional verification procedures such as PostIdent or virtual identification procedures could possibly be replaced by this. At the same time, the time delay until verification on the internet will then be a thing of the past. Further development into a data safe would be another alternative for significantly strengthening digital sovereignty. In this scenario, the internet user could store personal data in the privacy bot (e.g., address, credit card data, etc.). At a central point in the privacy bot, the targeted and individual release of data for internet services would then be possible. Internet services are permitted to access the data according to the internet user's specifications, but no further storage of the data. This not only gives internet users better control over access to their data, but also gives them digital sovereignty to manage their footprints on the internet in a traceable manner. Ultimately, storing personal data such as credit card details in a central location in the privacy bot reduces the risk of unauthorized data access or data misuse due to theft by third parties.

However, even without the aforementioned further developments, the concept of a privacy bot described in this article already represents a significant contribution to strengthening the digital sovereignty of internet users. It is also a proposal for how technologies already available today can be used to protect personal data on the internet.

5 General discussion and conclusion

In the following pages, Section 5.1 presents the results and implications of this dissertation, Section 5.2 its limitations and suggestions for future research, whereupon Section 5.3 provides some concluding thoughts.

5.1 Summary of results and implications

This dissertation provides a broad overview of the negative consequences that digitalization has come to be associated with at all levels of modern life. More specifically, it discusses a number of dark side phenomena in detail with special regard for their impact on the individual and organizational levels, such as rogue algorithms and the dissolution of privacy, and for a differentiated view of these contentious issues, it looks at their antecedents and the mechanisms that can be used to mitigate them. Section 5.1.1 summarizes the key findings of the research articles in Chapter 2 so as to refine the understanding of the unintended consequences and other hazardous fallout caused by digitalization. Section 5.1.2 then examines the findings of Chapter 3 with a special focus on the antecedents of the negative consequences of digitalization, and Section 5.1.3 presents the findings of Chapter 4 while concentrating on mitigation mechanisms.

5.1.1 Results and implications of Chapter 2: negative consequences of digitalization

Chapter 2 examines the negative consequences of digitalization. By way of introduction, Section 2.1 provides an initial taxonomy of eleven RSEDs and their subtypes. Section 2.2 extends the taxonomy development process notably with four additional cycles. The final taxonomy of RSED presented in Section 2.2 comprises 11 RSEDs and their 39 subtypes.

Section 2.1 stakes out the position that there is no cohesive view of the adverse effects of digitalization. To provide just that, the research article identifies, structures, and discusses the most severe RSED with the use of the iterative taxonomy development procedure suggested by Nickerson et al. (2013). In total, five cycles of the taxonomy development process were conducted for this article, each of them following an empirical-to-conceptual approach. The first cycle examined the academic literature (i.e., all relevant work available in the AIS eLibrary), while the second cycle processed the results of two workshops with senior scholars in the fields of ethics and law. The third cycle examined the adverse effects of digitalization as identified by leading print media from the U.S. and Germany (i.e., *TIME* and *DER SPIEGEL*).

The fourth cycle reconsiders the academic literature, yet this time the spotlight is on the volumes of *MIS Quarterly* and the *Journal of the AIS*. The last cycle, then, was dedicated to five expert interviews with senior scholars from ethics, criminology, sociology, psychology, and economic and social history.

Since each cycle took account of the lessons learned in the previous one, the RSED taxonomy matured over time. As a result, the final taxonomy comprises 11 RSEDs (e.g., *supporting delinquents*) and 35 related subtypes (e.g., *personal attacks*, *aggravation of prosecution*, *cyberwarfare*), all of which are defined in detail. Further, every one of the 35 subtypes was individually mapped to the particular level it most affected, that being either the *personal*, *interpersonal*, *organizational*, *inter-organizational*, *societal*. These five levels are similar to those of Costello et al. (2013), given that they are both based on the ecological systems theory developed by Bronfenbrenner (1981). The benefit of this structured development process is that our RSED map clearly indicates which subtypes are primarily enabled by certain affordances of digitalization, such as *low transaction costs*, *simplified broadcasting*, *low-cost anonymity*, *high social interconnectedness*, *low-cost ubiquity*, *rapid innovation and diffusion*, *automated decisions and actions*, *simplified profiling*.

Moreover, this research article reveals there to be a broad range of RSEDs, some of which have not yet been adequately researched within the IS discipline. First and foremost, the intended users of our taxonomy are IS researchers. Nevertheless, it may well be useful to those investigating the effects of digitalization through the lenses of other disciplines, be it criminology, psychology, or political science. To name a few examples, researchers may use our taxonomy to identify RSEDs that might occur when using new digital technologies. Furthermore, they may use our taxonomy as a starting point to identify appropriate mechanisms that mitigate the adverse effects of using digital technologies. Meanwhile, those putting the taxonomy to practical use in an organization may take advantage of it to recognize potential RSED and their relation to the application of specific digital technologies within their line of work. Finally, policy experts may use the taxonomy to assess whether or not current legislation is taking adequate account of the potential negative consequences of innovative digital technologies.

Section 2.2 has the same overarching research aim as Section 2.1, which is why the results are the same, too, at least in part. Section 2.1 represents an important stepping stone on the way to the final RSED taxonomy presented in Section 2.2. However, the initial taxonomy was

extended by four additional cycles, again in adherence with the empirical-to-conceptual approach. The first of these cycles was added to obtain feedback about the initial version of the taxonomy. To this end, we received seven blind peer reviews and held discussions with participants of three conferences. The second cycle then broadened the scope of our academic literature review by incorporating relevant articles from seven additional IS journals (i.e., *Information Systems Research*, *Journal of Management Information Systems*, *Journal of Strategic Information Systems*, *Information Systems Journal*, *European Journal of Information Systems*, *Journal of Information Technology*, *Communications of the AIS*). It further included articles published more recently in *MIS Quarterly* and the *Journal of the AIS*. The third cycle turned the focus on current articles in leading print media (i.e., *TIME*, *DER SPIEGEL*), and the final cycle covered recent proceedings of the *International Conference on Information Systems (ICIS)*. In sum, these additional cycles yielded 11 partially adapted RSEDs and 39 more specific subtypes. What is more, the extended research article reveals that, aside from the many benefits associated with digitalization, there are numerous RSED that will require further examination in the future.

With the help of this taxonomy, one is better able to understand the adverse, unintended, and unexpected effects of digitalization, and such understanding is a prerequisite for the development of appropriate mitigation mechanisms. Specifically, the work that has gone into this taxonomy contributes to IS literature in three ways. First, we conceptualize RSEDs as adverse secondary effects or the negative potential of adopting and using digital technologies and media in individual, organizational, and societal contexts. Second, we define and describe 11 RSEDs and their 39 more specific subtypes. Third, we provide a taxonomy of the RSEDs, including a hierarchical network of relationships among those RSEDs, their subtypes, manifestations, and examples. Since each RSED subtype is associated with different affordances of digital technologies, the taxonomy indicates whether the respective subtype affects the individual, organizational, or societal level. As for the other findings of the extended research article, their implications apply to various stakeholders, such as IS researchers, practitioners, and policy experts, as presented in Section 2.1.

The overarching theme to be noted here is that the two research articles reveal digitalization to pose a multitude of serious risks, and indeed cause numerous problematic side effects. By and large, the latter are suffered by *individuals* and *societies as a whole*. This is due to the fact that digital technologies have permeated near enough all aspects of modern life. Special attention must, therefore, be paid to those social groups that are particularly at risk from the use of digital technologies. Further to be noted is that *big data handling, automated decisions and*

actions, *rapid innovation and diffusion*, and the *low-cost ubiquity of DTM* appear to be the most consequential affordances, which makes it imperative that digital technologies related to one or more of these affordances should be developed and evaluated with particular care. To this end, the two research articles focus exclusively on the *negative consequences* of digitalization. *Antecedents* and possible *mitigation mechanisms* are not discussed in either article.

5.1.2 Results and implications of Chapter 3: antecedents of digitalization's negative consequences

Chapter 3 examines the *antecedents* of the negative consequences of digitalization. Section 3.1 focuses on the concerns many individuals have about ADM and its potentially *negative consequences*, whereas Section 3.2 investigates privacy concerns as *antecedents* of user (dis)satisfaction with specific mHealth app features.

Section 3.1, then, is dedicated to the concerns many individuals have about ADM. These concerns were identified by means of a structured literature search and a qualitative content analysis of 13 semi-structured interviews. To cover a sufficiently broad range of research articles from a meaningful variety of disciplines, such as engineering, law, and marketing, the structured literature search was conducted in seven databases: *ACM Digital Library*, *AIS Electronic Library*, *Science direct*, *EBSCOhost*, *JSTOR Library*, *SpringerLink*, and *ProQuest*. 18 of the 175 search results were deemed to be relevant to this analysis. Furthermore, we performed 13 semi-structured interviews with potential users of algorithm-based technologies from diverse backgrounds. Respondents were asked to describe their concerns about five specific use cases of algorithm-based technologies. The detailed analysis of the academic literature along with the qualitative content analysis of the semi-structured interviews yielded 10 inherent concerns about the underlying *technology* (e.g., *security incidents*), *data* (e.g., *data manipulation*), and the *decision* itself (e.g., *lack of transparency & missing verifiability*). It also yielded 14 concerns about the potential consequences of using algorithm-based technologies. The latter were grouped into seven categories adapted from those formulated by Karwatzki et al. (2017), i.e., *physical*, *social*, *resource-related*, *psychological*, *prosecution-related*, *career-related*, *freedom-related*. Examples of these concerns are *discrimination* (*social*), *negative financial impact* (*resource-related*), *job loss* (*career-related*), and *skill loss* (*freedom-related*). All concerns were noted with reference to the literature sources or the respective interviews in which they were cited. *Job loss* and *environmental harms* are the only concerns mentioned exclusively in the academic literature. The other 13 concerns that had been identified in the literature were confirmed by our interviewees, who also raised four other inherent concerns (e.g.,

immaturity, *insufficient or wrong data basis*) and seven further concerns about negative consequences (e.g., *psychological harms*, *monopolization of economy*).

The research article highlights the complexity of concerns that users may develop about the use of specific digital technologies, in this case, algorithm-based technologies. A closer look at the inherent concerns, which can be seen as *antecedents* of potential *negative consequences* of using algorithm-based technologies, reveals that only the concerns in the category *decision* are unique to ADM. Conversely, the *technology* and *data* concerns extend to other emerging technologies, such as IoT or Blockchain. For instance, *security* and *privacy incidents* have already been discussed in the context of IoT, whereas *immaturity* applies to most new technologies. Worth observing in this context is that our interviews revealed not only concerns about ADM but also several aspects that mitigate those concerns. First and foremost, they are found to be manageable when individuals *cannot perceive a difference* between automated decision-making and a human decision-making process. Other mitigating aspects named in our interviews are *transparency* and *trust*. As any digital technology, ADM is associated with potentially negative consequences, but as our interviews indicate, it is also seen as the source of multiple positive opportunities, such as *time savings*, *less effort for individuals*, *less subjectivity and more fairness in decisions*, *variety and positive surprises through ADM*, and a *lower error rate in decisions*.

Section 3.2 extends this differentiated view of innovative digital technologies by examining user (dis)satisfaction with specific mHealth app features. In our research article, we focused on PHR. First, we investigated how potential users in Germany and Denmark evaluate a set of PHR features. Then, we examined whether certain user characteristics (i.e., *privacy concerns*, *mHealth literacy*, *mHealth self-efficacy*, and *adult playfulness*) might account for the different evaluations made by potential users in Germany and Denmark. *Privacy concerns* are widely considered to be *antecedents* of user dissatisfaction with specific app features, which is significant in that this dissatisfaction often leads to the non-usage of the entire app. To account for such complex ramifications, we designed a cross-national survey based on the Kano method after identifying 26 potential PHR app features in the relevant literature. These were evaluated by 215 participants from Germany and 59 from Denmark, and thus by a total of 274 participants. Among both groups of survey participants, features referred to as *delighters* (those with attractive qualities) took the largest share (Germany: 42%; Denmark: 54%). In contrast, the categorization of *performance needs* (one-dimensional quality) was rarely considered important (Germany: 0%; Denmark: 4%). Only two features (8%) were deemed

to be *basic needs* (must-be quality) by both German and Danish participants, those being *protected personal access* and *data encryption*. These features should, therefore, be implemented in every PHR, as failure to do so is almost certain to cause user dissatisfaction.

Moreover, several features elicited indifference (Germany: 38%; Denmark: 15%). *Social media* was thought to have a reverse quality by the Germans, whereas the Danes categorized none of the features as having a reverse quality. Finally, a small proportion of features was assigned to a mixed category as they did not register any significant response (Germany: 8%; Denmark 19%). Overall, 14 of the 26 app features (54%) were categorized differently by Germans and Danes. These subgroup differences could be explained by four antecedent user characteristics, all of which showed significant factor-level differences between Germany and Denmark. According to our study, Germans tend to have significantly *higher privacy concerns*, *lower mHealth literacy*, *lower mHealth self-efficacy*, and *lower adult playfulness* than Danes. The detailed analysis of our survey data shows that the cross-country differences in user characteristics could partly explain cross-country differences in feature evaluation for nine of the 14 features that were found to be markedly different in the two countries.

By explaining the relationship between specific mHealth app features and user satisfaction we build a bridge between the rather technical, feature-oriented mHealth research and more behavioral user acceptance and marketing-oriented mHealth research. To the best of our knowledge, ours is the first empirical study to evaluate PHR features in terms of user satisfaction. Another first of this study is the fact that its methodological augmentation of the Kano method, done to investigate the differences in the feature evaluation of Germans and Danes, provides the added advantage of explaining further potential subgroup differences. From a practical perspective, our research can help developers of PHR apps to prioritize PHR features. With this knowledge, developers can decide, for example, how to allocate future resources in their development process. Furthermore, our results show that user characteristics and cross-country differences can influence how users evaluate specific app features and, indeed, how satisfied they are with mHealth apps overall. Internationally operating app providers should take these findings into account at the development stage of their mHealth apps. Likewise, policymakers would benefit from considering our findings in light of cross-country differences, for instance, by updating the current EU legal framework to make it more suitable for modern lifestyle and wellbeing apps.

In our research article, the Kano method is used to determine the impact of specific mHealth app features on user satisfaction. In doing so, the article goes beyond the originally envisioned

evaluation of components of physical products in as far as it demonstrates the suitability of the Kano method when it comes to the evaluation of products or services in the digital world (see also Section 4.1 concerning the evaluation of data privacy measures). Similarly innovative is the fact that the research article on mHealth app features presents a new approach as to how we can explain differences in the feature evaluation with user characteristics and in so doing advances the research in this important area.

Both research articles included in Chapter 3 reveal there to be different *antecedents* with the potential to influence how users perceive digital technologies. Although the negative consequences presented in the two articles (e.g., user dissatisfaction or non-use) would appear to be of lesser severity than other adverse effects of digitalization (cf. Chapter 2), the results of these studies nevertheless indicate that the *negative consequences* of using digital technologies can have a broad variety of *antecedents*. They also indicate that certain concerns are particularly relevant, regardless of the context of the technology, such as *privacy concerns*. Such consistent barriers to the use of the technology were identified in both articles. Furthermore, both articles address the far-reaching use of new digital technologies, for instance, in automated decision-making and mHealth apps. Due to this focus on the potential consequences of user dissatisfaction and non-usage, both articles contribute to the research on *IS adoption*. While the first article identifies various concerns that can inhibit individuals or indeed prevent them from using digital services, such as concerns about automated decision-making, the second article takes account of individual characteristics that might influence an individual's intention to use mHealth apps.

5.1.3 Results and implications of Chapter 4: mitigation mechanisms to cope with the negative consequences of digitalization

Chapter 4 examines mechanisms that can be used to mitigate the negative consequences of digitalization. Section 4.1 takes an organizational perspective to indicate which data privacy measures may be implemented to achieve a positive impact on customer satisfaction. Section 4.2 takes an individual perspective to reveal how the privacy concerns of users can be resolved with the help of a privacy bot.

Section 4.1 investigates data privacy measures that organizations could implement to address the data privacy issues that many customers lament. To establish a comprehensive overview, we first collected all the data privacy measures discussed in academic literature, legislative texts, company privacy statements, and expert interviews. Our initial analysis synthesized 202 statements into 32 data privacy measures, each of which could be assigned to one of the seven

privacy concerns described by Smith et al. (1996), namely *data collection*, *data combination*, *internal secondary usage*, *external secondary usage*, *errors*, *improper access*, and *reduced judgment*. To analyze the impact of these 32 measures on customer satisfaction, we conducted two online surveys, each with more than 200 participants. In the first study, participants had a flight booking scenario described to them. In the second study, they were placed in an online shopping scenario. We used the survey data from both scenarios to assign each measure to one of the following Kano model factors: *attractive quality (delighters)*, *one-dimensional quality (performance need)*, *must-be quality (basic need)*, and *indifferent quality*. Across the two scenarios, 75% of the measures were assigned to the same category. The consistency with which these measures were categorized is further reflected in a satisfaction-dissatisfaction diagram and a test of inter-rater reliability.

In both scenarios, five measures were considered to be of indifferent quality, whereas 17 were classified as basic needs, meaning that the implementation of these measures is not rewarded with higher customer satisfaction. Rather, it is taken for granted by customers. Meanwhile, no measures were thought to be of one-dimensional quality, whereas delighters were noted in both scenarios (aviation: 7; retail: 5). As our results indicate, the implementation of these measures is not expected by customers, so it can have a significant positive impact on customer satisfaction. In both scenarios, customers can be delighted, inter alia, by *storing their data in an anonymized form*, *empowering them with regard to the combination of their data* and *data sharing within the company*, and *storing their data on servers with a secure location*. As all of these examples show, companies can please customers by implementing data privacy measures. This is a particularly important finding given that most companies treat the issue of data privacy as a necessary evil, which is to say they do little or nothing to mitigate privacy concerns. Also worth noting is that a close look at the survey results indicates that the vast majority of participants (aviation: 92%; retail: 91%) deemed at least one of the 32 data privacy measures to be attractive. Indeed, near enough one-third of the participants (aviation: 32%; retail: 29%) considered 10 or more of the measures to be of attractive quality.

These results reveal an interesting attitude to the issue of data privacy beyond legal compliance and risk management. Although we found that some of the data privacy measures were seen as delighters, it must be stated that the majority of the measures were categorized as basic needs. We recommend, therefore, that these 32 data privacy measures, as derived from various sources and evaluated in discussions with several data privacy experts, can serve as a broad foundation on which to develop further data privacy concepts and strategies. Practitioners can

use the list of privacy measures and the insights from our surveys as a starting point to implement privacy measures that can positively affect customer satisfaction and create greater potential for competitive advantage. Meanwhile, companies might consider offering their customers a variety of price packages, depending on the level of data privacy provided. It is clear, then, that there are tangible and direct benefits for companies and customers alike if our research results are taken into account when those companies decide whether to implement specific data privacy measures. What is more, these findings represent an important decision-making criterion in the trade-off between economic value, regulatory requirements, and technical feasibility.

This brings us to the question of implementing data privacy measures that go beyond the usual and legally prescribed level. As our results indicate, this is commonly seen as an example of how to handle the risks and side effects of digitalization responsibly. The approach presented in this article can be seen as a suitable *mitigation mechanism* when dealing with the RSED *dissolution of privacy* (cf. Chapter 2).

Section 4.2 describes the concept of a privacy bot that addresses the privacy concerns that arise for users when they avail themselves of an online service. The concept aims to strengthen the digital sovereignty of users by letting them see in a transparent and easily understood way what data is collected, stored, and processed when they use an internet service. Provided that users store their preferences for personal data protection in their profile, the privacy statements of internet services are automatically evaluated, and possible conflicts are highlighted. As our research indicates, the use of this privacy bot should be made as comfortable as possible by providing a browser plug-in. Since privacy preferences may differ depending on the type of internet service (e.g., online banking vs. online shopping), users can store different privacy profiles and decide which profile to apply each time they consider a new service. To illustrate these features, we implemented a clickable prototype. In our article, we conceptualize three options to check the conformity of privacy statements with the user's preferences (i.e., *manual testing*, *interface setup*, *text mining*). Furthermore, we describe how a privacy bot could be integrated into existing business models or implemented as a standalone service. In the future, the privacy bot could be further developed into a data safe to replace previous identification verification procedures.

We evaluated our concept for the privacy bot by surveying 78 internet users. For the purpose of demonstration, survey participants were provided with a clickable prototype of the privacy bot. Overall, the participants rated the bot's usefulness with an average of 5.13 (out of 7)

points. Based on their experience in this survey, they then indicated their intention to use such a bot in the future with an average of 4.83 (out of 7) points. As these results indicate, such a privacy bot is deemed rather useful in efforts to strengthen individual digital sovereignty.

Our privacy bot concept serves as an example of how to deal with the risks and side effects of digitalization. The concept was developed in full cognizance of data privacy issues that occur especially on an *individual* level (cf. RSED *loss of privacy*, Chapter 2.2). With the help of the privacy bot, individuals can better understand how their personal data is stored, used, and shared whenever they use internet services, which summarily strengthens their digital sovereignty.

The two research articles on appropriate *mitigation mechanisms* presented in Chapter 4 both relate to the area of data protection that has lately received considerable attention from the general public due to numerous data privacy scandals and the introduction of the European GDPR. The data privacy measures developed in Chapter 4.1 may be implemented by *organizations*, whereas the privacy bot presented in Chapter 4.2 is intended for the use of *individuals*. By developing and providing a privacy bot, companies like telecommunications service providers could signal to their customers and stakeholders that they treat the risks and side effects of digitalization with the seriousness required to take appropriate countermeasures. Furthermore, the *mitigation mechanisms* needed to deal with the issue of data privacy could also be developed in a *societal* context. This task could, for instance, be taken on by universities and other government-funded research institutions. The same is true for the remaining risks and side effects of digitalization identified in Chapter 2, few of which have been as extensively researched as the data privacy issues focused on in Chapter 4.

5.2 Future research

The following sections address the limitations of the six research papers presented above. They also offer suggestions on how to transcend these limitations and present starting points for future research.

5.2.1 Future research based on Chapter 2: negative consequences of digitalization

The two sequential research articles on the risks and side effects of digitalization turn the spotlight on certain aspects worthy of further attention in future research projects. Since Section 2.2 is an extension of Section 2.1 and provides answers to the same research question as

Section 2.1, follow-up research questions that arise from the two articles are discussed together.

Discussions about the dark side effects of digital technology use are not new. As our research articles show, however, previous research on negative effects has been rather unbalanced. Certain dark side phenomena, such as *technostress* and *data privacy issues*, are discussed in-depth, yet many others are still not sufficiently understood.

Since many of the RSEDs have received little to no attention in the scientific literature, future researchers would be well-advised to continue the work of this study by analyzing antecedents, consequences, and boundary conditions of the 11 RSEDs so as to develop new substantive theories about these dark side phenomena. Since the adverse effects of digitalization are not limited in their relevance to IS research but relate to many other disciplines, such as criminology, psychology, economics, and political science, this research question could be answered by interdisciplinary research teams. At the same time, researchers within our own field would do well to look for similarities between familiar areas like technostress and less studied negative effects in terms of affordances and the various levels thus affected. This should advance important efforts to develop broader theories about dark side phenomena.

Since many of the RSEDs are relatively new and therefore under-researched phenomena, each of which can have significant negative consequences for individuals, organizations, or society at large, it is of the utmost importance that appropriate mitigation mechanisms are developed as soon as possible. Due to the large number of identified RSEDs and their subtypes, the first point on the agenda ought to be to prioritize them in terms of severity of impact. This could be done, for example, by means of a broad survey for users of digital technologies. As the current taxonomies of RSEDs tend to have a culturally biased Western perspective, it would be beneficial to have the severity of negative effects assessed by participants from different cultural backgrounds. For example, multiple lists of RSEDs could be developed for different countries or cultural groups so as to help prioritize the development of countermeasures appropriate to those specific contexts. Alternatively, prioritization could also be done with reference to other individual characteristics of the respondents. Conceivably, certain RSEDs might have particularly severe negative effects among adolescents, a likely issue being online gaming addiction. Suitable *mitigation mechanisms* for these RSEDs could then be integrated into the school curriculum at the appropriate level of education. The same knowledge about the risk of negative consequences could also be used by those who develop new digital tech-

nologies as and when they do so, rather than in hindsight, which means they could take appropriate countermeasures, rather than merely devise mitigation mechanisms once the risks have become realities. Meanwhile, researchers could use the findings to decide which areas require more detailed research to minimize the negative impact of digital technologies, while policymakers could use the survey data to determine which digital technologies should be regulated in their respective areas of responsibility.

The purpose of our own work here has been to provide a broad overview of the adverse effects of digitalization. To this end, we drew on multiple sources, including academic literature, interviews with experts from various disciplines, feedback from other IS researchers, and journalistic articles from the United States and Germany. Those efforts of ensuring due diligence notwithstanding, we might have missed some other important RSED. After all, we only included journalistic articles from two western countries. Although both magazines also report on events in other regions of the world, this may have inadvertently created a cultural bias. To redress this, future researchers could look at the issue through a different cultural lens, the potential benefit being the identification of other important RSED.

A final observation to be made in this regard is that the breadth of our taxonomy, though intended for the aforementioned purpose of comprehensiveness, may be interpreted by some as having led to a lack of parsimony. To compensate for that, future research could develop more specific theories for the adverse effects of digitalization, for example by exploring their causal relation to specific technologies, affordances, or contexts.

5.2.2 Future research based on Chapter 3: antecedents of digitalization's negative consequences

The research articles included in Chapter 3 focus on the antecedents of the negative aspects of digitalization and, as such, they provide certain promising paths for future research. In Section 3.1, we identified 24 concerns related to the integration of automated decision-making into the lives of ordinary individuals. These concerns were identified by means of a thorough literature review and 13 semi-structured interviews. During the interviews, we presented five use cases of ADM, based on which the interviewees were asked to express their concerns. Some of those concerns are hardly unique to ADM but rather transferrable to other new technologies. Future research could, therefore, focus on users who are already using systems based on automated decision-making in order to identify any ADM-specific concerns this may cause.

Although our research focused on the concerns that individuals have about ADM, some of our interviewees named certain aspects that would mitigate their concerns. One of these aspects is *transparency*. We found that understanding how and why algorithms come to a decision could mitigate many of the concerns identified by our study. The research area of explainable AI focuses on this phenomenon, and while it does aim to create more transparent systems, more work has to be done. It remains to be said, then, that even though we have already identified these and other mitigating aspects, such as *trust*, future research on ADM could aim to identify enough of them to ensure the development of systems that address the concerns of individuals in a proactive rather than a reactive way.

Aside from these mitigating aspects, however, our interviewees also named numerous positive aspects of ADM, such as time savings, a reduced effort for individuals, less subjectivity and more fairness in decisions, variety and positive surprises through ADM, and lower error rate in decisions. Future research could investigate the relationship between the positive aspects of ADM, its mitigating features, and the concerns identified in this research article. Certain concerns may, after all, be mitigated rather well by certain positive aspects of automated decision-making. Such findings would be very useful for developers of systems that incorporate automated decisions.

As the assessment of new technologies and the intention to use them may be affected by the user's cultural background or other individual characteristics, future researchers could conduct large-scale studies with a wide range of participants. This would yield a detailed understanding of the incidence rate of certain concerns among specific user groups; something of enormous value in the development of services based on automated decision-making.

In section 3.2, we investigated how different mHealth app features are evaluated by potential users in Germany and Denmark. Our research focused exclusively on PHR as an example of mHealth apps. We identified the various PHR features by analyzing relevant academic literature, but due to the dynamic developments in this area, new PHR features are likely to present themselves before long, and these should promptly be added to the list. Moreover, further research could incorporate other types of mHealth apps in order to identify additional mHealth app features and achieve results that can be generalized to a higher degree. Besides, while we intentionally focused on how users perceive the PHR features, many other mHealth researchers focus on a clinical or organizational perspective. It would, therefore, be interesting to conduct complementary studies on PHR features to fully assess their clinical or organizational usefulness.

In the meantime, it bears repeating that an important purpose of this study was to identify potential reasons for the numerous differences in the feature evaluation. To do so, we examined four user characteristics, namely *privacy concerns*, *mHealth literacy*, *mHealth self-efficacy*, and *adult playfulness*. As we found, these do indeed account for several of the differences, but it is conceivable that the general experience of mHealth apps usage, or other aspects like time or support, might also explain some of those differences in evaluation, which is why they recommend themselves to future research.

Together, the participants of our study represent a broad section of sociodemographic characteristics, including different ages, educational backgrounds, and employment states. Nevertheless, the sample is not representative of Germany or Denmark. Due to the comparatively unbalanced sample in terms of German and Danish participants as well as the overall small sample size, the risk of a bias could not be completely excluded. Furthermore, most of the participants were not experienced in the use of mHealth apps. To account for these shortcomings and verify the general validity of our conclusions, future researchers are encouraged to conduct large-scale studies with people from different countries and different experience levels.

As the two articles included in Chapter 3 show, the *antecedents* that must be considered when investigating the negative consequences of digital technology use are complex. Section 3.1 shows that there may be as many as 10 reasons why individuals are concerned about automated decisions, and these concerns are likely related to the underlying *technology*, *data*, or the *decision* itself. Section 3.2 examines four individual user characteristics, one or indeed all of which may explain the differences in how particular mHealth app features are evaluated. These characteristics might, therefore, be seen as *antecedents* of *user dissatisfaction*, and our fellow researchers would do well to explore them further, along with the *antecedents* of the many as yet unfamiliar RSED, a more detailed understanding of which promises to help us identify particularly vulnerable user groups.

5.2.3 Future research based on Chapter 4: mitigation mechanisms to cope with the negative consequences of digitalization

Based on the findings of the two research articles in Chapter 4, some interesting questions arise for future research. Section 4.1 identifies and evaluates specific data privacy measures in terms of their impact on customer satisfaction. Since we have identified 32 data privacy measures with a focus on Germany and wider Europe, future research could investigate whether different cultures or legal frameworks might produce or require other data privacy

measures. As part of this study, we conducted two online surveys concerning a flight booking scenario and an online shopping scenario so as to capture a greater range of experience and opinions, but since the participants of these surveys were predominantly students, our study cannot be deemed representative. Future research might focus on further scenarios and other customer groups to add to the results presented in this paper and test their general validity. Also worth considering in this context is the fact that our research neglected the potential impact of the device used to book a flight or make an online purchase. For instance, the privacy concerns that customers have when using a laptop might differ from those they contend with when using smartphones, tablets, or voice assistants. This could, therefore, be a fruitful field for future research.

This brings us to an important caveat. Empirical studies in the data protection context must keep in mind the privacy paradox, which is to say the discrepancy between how customers intend to protect their own privacy and how they actually behave (Acquisti & Grossklags, 2005; Norberg et al., 2007). Since our study focused on the former, future research could be done to test whether our results are verifiable in real-world situations.

Based on the results of our two empirical studies, we are confident to conclude that companies can increase customer satisfaction and so to speak "delight" customers by implementing specific data privacy measures. Nevertheless, the classification of certain measures as so-called delighters was less clear than that of basic needs. To address this issue, future research could focus on the question of whether particular data privacy measures might delight only specific customer groups. Based on these findings, companies could then think about giving their customers the choice of different levels of data protection, for instance, a basic offer at a low price and a premium offer at a higher price.

Section 4.2 presents the concept of a privacy bot, the purpose of which is to strengthen the digital sovereignty of its users. Since this is a practice-oriented research article, it has numerous limitations when viewed from an academic perspective. We discussed a versatile privacy bot that is able to automatically evaluate the privacy statements of various internet services. To illustrate these functions, we implemented a clickable prototype of the privacy bot. We also described numerous options for how the evaluation of privacy statements could be conducted. Nonetheless, this central part of the privacy bot has not yet been implemented. Therefore, design science researchers are encouraged to develop our theoretical concept into a user-friendly privacy bot.

We tested the usefulness of this concept with the help of an online survey of 78 internet users. Although the results from this initial survey were promising, the concept and various proposed privacy bot features would need to be evaluated again in more detail before the actual privacy bot could be developed successfully. Also, it would have to be determined whether certain of its functions have already been developed and gone to market in the meantime. For example, as a possible extension of the basic concept, we mentioned the use of the privacy bot during identification procedures. In one shape or another, however, this service is already being offered by numerous other companies.

Chapter 4 provides two examples of how suitable *mitigation mechanisms* can be found to deal with the negative consequences of digitalization. Both research articles focus on the field of data privacy (cf. RSED *loss of privacy*, Chapter 2.2). In view of the multitude of adverse effects caused by digitalization, future research on mitigation mechanisms for further RSEDs would appear to be advisable. The best and perhaps the only way to accomplish this task would appear to be through the interaction of various players. Already, companies that are developing digital technologies should ensure that they are as risk-free as possible, and this can be supported by collaborating with universities or other government-funded research institutions. Since policymakers should intervene where risky digital technologies affect particularly vulnerable user groups, such as children and young people, they ought to look at limiting the use of these digital technologies to user groups that can cope with the higher risk (e.g., adults). In addition, particularly vulnerable user groups should be made more aware of the risks and side effects of using digital technologies (e.g., in school lessons).

5.3 Conclusion

This dissertation contributes to the IS research on the dark side effects of using digital technologies. It provides a comprehensive taxonomy of RSEDs, many of which have not been adequately addressed in the IS research to date. Looking ahead, it is my hope that these pages contain numerous starting points for future research projects that could focus on, among other worthy subjects, the detailed analysis of individual RSEDs. Meanwhile, this dissertation also considers the antecedents of the adverse effects of digitalization, and indeed their appropriate mitigation mechanisms. More precisely, it provides two articles on antecedents and two concrete examples of the measures that can be taken to mitigate the risk of data privacy incidents.

Throughout, it has been my guiding intention to cast a spotlight on the negative aspects of digitalization without eclipsing its opportunities. For example, the mHealth apps discussed in

Section 3.2 have the potential to make life easier for countless people. The privacy bot, introduced in Section 4.2, offers the potential to increase the digital sovereignty of its users. Nevertheless, most digital technologies are beset by severe risks and side effects, which is why I wish to conclude on the same cautionary note that has run through this entire dissertation. It is incumbent upon each one of us to use digital technologies in a way that benefits us and others more than it causes harm. Further research will have to be done on the multiple risks and side effects of digitalization to ensure that policymakers can make informed decisions on which safeguards to place upon digital technologies. In the meantime, companies must also honor their responsibility to protect their customers, employees, and other stakeholders who use their digital technologies. Ultimately, however, it is up to everyone individually to take a critical look at the use of digital technologies. Only such a critical examination will make sure that the positives will outweigh the negatives in the use of digital technologies. Hopefully, this dissertation can make a small contribution towards tipping the scales the right way.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Bronfenbrenner, U. (1981). *Die Ökologie der menschlichen Entwicklung: Natürliche und geplante Experimente*. Klett-Cotta.

Costello, G. J., Donnellan, B., & Curley, M. (2013). A Theoretical Framework to Develop a Research Agenda for Information Systems Innovation. *Communications of the Association for Information Systems*, *33*(1), Article 26, 433–462.

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, *26*(6), 688–715. https://doi.org/10.1057/s41303-017-0064-z

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336–359. https://doi.org/10.1057/ejis.2012.26

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MISQ (MIS Quarterly)*, *20*(2), 167–196.