December 2024

How Uncertainty and AI Reciprocity Shape Data Disclosure Decisions in AI Health Services

Alexander Zieglmeier
Professur für Digitale Services und Sustainability, Alexander.Zieglmeier@lmu.de

Johann Kranz
Ludwig-Maximilians-University Munich, kranz@lmu.de

Tawfiq Alashoor
IESE Business School, talashoor@iese.edu

How Uncertainty and AI Reciprocity Shape Data Disclosure Decisions in AI Health Services

Completed Research Paper

Alexander Zieglmeier
LMU Munich School of Management
Ludwigstraße 28, 80539 Munich
Ludwig-Maximilians-Universität
alexander.zieglmeier@lmu.de

Johann Kranz
LMU Munich School of Management
Ludwigstraße 28, 80539 Munich
Ludwig-Maximilians-Universität
kranz@lmu.de

Tawfiq Alashoor
IESE Business School
Av. de Pearson, 21, Les Corts, 08034 Barcelona
talashoor@iese.edu

Abstract

AI health services have become pervasive through advancements such as machine learning and increasing demands stemming from the needs of an aging society. This study explores the concept of "AI reciprocity" within commercial AI health services to examine prosocial data disclosure, wherein users contribute data to enhance service quality for all other users within a system. This study expands the literature on privacy calculus in the context of AI health services as it scrutinizes the impact of privacy uncertainty and AI reciprocity benefits on data disclosure. Conducting an online experiment, we found that privacy uncertainty is driven by transparency features and is associated negatively with data disclosure. Conversely, we find that AI reciprocity is positively associated with data disclosure. However, we could not find evidence that AI reciprocity can be influenced by manipulating the perceived social distance of the beneficiaries. Our findings suggest several avenues for future research.

Keywords: Artificial intelligence reciprocity, privacy calculus, prosocial data disclosure, privacy uncertainty, privacy transparency, social distance, construal level theory, AI health services

Introduction

AI services have spread ubiquitously across a diverse set of domains. Fueled by accompanying advances in machine learning and Internet of Things (IoT) technology, they have also enriched the landscape of smart health services. AI health services have been applied in areas such as caregiver robots, assisting self-diagnosis, or helping to prevent medication (Guerra & Johnson, 2023). Due to the aging of many societies, the relevance of AI health service systems will surge. Furthermore, healthcare companies are projected to more than triple their expenses on AI technology, reaching $47 bn by 2028 (The Economist, 2024).

AI health services differ from conventional mobile health service devices such as wearables or mobile health apps by being more intelligent and personalized (Liu & Tao, 2022). Driven by statistical learning processes, AI health services can adapt to individual customer needs based on their usage behavior. To detect patterns

in user behavior, AI health services demand a continuous supply of sensitive data to provide tailored recommendations. As a result, users are concerned about their privacy (Guo et al., 2016; Klossner et al., 2023). Consequently, a conflict arises in the customers' valuation of AI health services. While users appreciate additional personalization as a benefit, they seek to avoid the privacy risks associated with disclosing sensitive data. This trade-off is known as the personalization-privacy paradox (Guo et al., 2016; Liu & Tao, 2022). Moreover, whenever people deliberate on the disclosure of data in return for a reward, they engage in a cost-benefit analysis, known as the privacy calculus (Dinev & Hart, 2006; Smith et al., 2011).

An aspect so far rather overlooked in the literature on privacy and acceptance of AI health services is the fact that AI-based services are usually based on an AI platform (Raddatz et al., 2023). AI platforms help organizations access AI technology for developing or using AI applications by bringing together and coordinating different agents. This approach improves efficiency and allows for a flexible technological setup that enhances overall value (Geske et al., 2021). It entails that numerous service users contribute their data to the platform and individual personalization rewards are not the only outcome. Because of the generativity and convergence of AI-based services (Yoo et al., 2010; Zittrain, 2006), unbounded innovation occurs on AI platforms driven by diverse and uncoordinated actors. Hence, AI platforms are generative systems (Thomas & Tee, 2022) in which the sharing of data provides indivisible and collective value through data network effects (Gregory et al., 2021).

As the platform gathers and learns from user data, its value increases for each user (Gregory et al., 2021). In the case of AI-based services, additional user data enriches the database upon which algorithmic models are trained and make their decisions. Consequently, the quality of services for all other users within the system improves and may even trigger the innovation of new services. Hence, such services expose reciprocal benefits (Fox et al., 2021; Hamari & Koivisto, 2015), as sharing data mutually benefits the self and others using the service. In the domain of AI health services, this also implies that the well-being of all other users in the system is increased, as service innovation and increased service performance are facilitated by better and more data. These reciprocal benefits were, for instance, an important motivator regarding public COVID-19 tracing app acceptance (Fox et al., 2021). In the context of commercial AI services, the aspect of "AI reciprocity" has been vastly overlooked in the literature.

We address this shortcoming in a number of ways. First, research on other-focused data disclosure suggests that people share data not only for personal gains but also to assist others (Nabity-Grover et al., 2020; Wagner et al., 2018). That is particularly evident in studies on COVID-19 tracing apps that emphasize the importance of social benefit appeals to encourage adoption (Carlsson Hauff & Nilsson, 2023; Dooley et al., 2022; Trang et al., 2020). Nevertheless, there are inconsistencies concerning the importance of social benefit appeals, as several studies found no impact compared to personal benefit framings (Matt et al., 2022; Munzert et al., 2021; Seberger & Patil, 2021). Consequently, the question arises as to whether social benefit appeals also effectively influence data disclosure outside an extremely specific COVID-19 context. As recent research in the privacy literature shows (Butori & Miltgen, 2023; Clark et al., 2023), construal level theory (CLT) (Trope & Liberman, 2010; Trope et al., 2007) may explain people's assessments of benefits in the privacy calculus. According to CLT, individuals perceive events or concepts in decision-making as more concrete and relevant when they have a lower psychological distance from the event. In the context of prosocial data disclosure, this would imply that social benefit appeals gain importance if the beneficiary of the disclosure is perceived psychologically closer to the data provider.

Second, the privacy calculus assumes that people assess their privacy risk regarding privacy decision-making. However, consumers often struggle to adequately assess their privacy due to uncertainty about how a service uses and protects their data (Al-Natour et al., 2020). Despite that, there is only scarce literature on how companies can counteract the consequences of privacy uncertainty. Privacy transparency features are assumed to reduce information asymmetries and ambiguity (Fast, 2019; Karwatzki et al., 2017). Hence the provision of privacy transparency features seems an appropriate tool to increase the willingness to disclose data by reducing privacy uncertainty. However, the literature on privacy transparency (Betzing et al., 2020; Karwatzki et al., 2017; Wiencierz & Luenich, 2022) found inconclusive results on the effect of transparency features on data disclosure. Furthermore, besides the work of Al-Natour et al. (2020) in the context of mobile apps, there is also no indication of how transparency features influence privacy uncertainty in a prosocial context like AI health services. To investigate these shortcomings of the privacy calculus within the context of commercial AI health services we ask the following research question:

RQ: How do privacy transparency and social distance impact the privacy calculus for commercial AI health services?

To address the research question, we conducted an online experiment entailing a 2x2 full factorial between-subjects design. We observe that high levels of privacy transparency decrease privacy uncertainty compared to low levels. We also find that privacy uncertainty is associated negatively with the willingness to disclose data. Further, we discover that AI reciprocity benefits have a significant effect on the willingness to disclose data. However, we do not find a significant effect of social distance influencing AI reciprocity benefits. We contribute to the literature in the following ways. Firstly, we extend the literature on privacy transparency (Betzing et al., 2020; Karwatzki et al., 2017; Wiencierz & Luenich, 2022), as we show that higher levels of transparency are associated negatively with privacy uncertainty in the prosocial context of AI health services. Secondly, we contribute to the literature on uncertainty in privacy-related decision-making (Acquisti et al., 2015; Acquisti et al., 2007; Al-Natour et al., 2020) as we find supporting evidence that privacy uncertainty is negatively associated with prosocial data disclosure. Lastly, our findings extend the literature on other-focused data disclosure (Nabity-Grover et al., 2020; Wagner et al., 2018). Thus, we introduce and analyze the concept of prosocial data disclosure (Ghaffar & Widjaja, 2023; Skatova & Goulding, 2019; Thiebes et al., 2017; Trang et al., 2020) to the commercial context.

Theoretical Background: Privacy Calculus and Construal Level Theory

Privacy scholars conducted studies on a wide variety of technologies over the past years. These include online social networks (Krasnova et al., 2010), e-commerce (Dinev & Hart, 2006), and location-based services (Naous et al., 2019; Xu et al., 2009). Furthermore, they also examined digital health applications such as contact tracing apps (Hassandoust et al., 2021), and wearable devices (Dincelli & Zhou, 2017; Li et al., 2016). Among all those studies scholars applied the privacy calculus as the central concept to determine and understand the patterns of individual data disclosure. The privacy calculus is based on the conceptualization of privacy as a commodity which suggests that value judgments about privacy are subject to personal evaluation based on cost-benefit calculations (Smith et al., 2011). Further, the privacy calculus can be described as an adaption of rational choice theory in the context of information privacy. The theory assumes that individuals act rationally and are willing to accept certain information privacy risks in exchange for some perceived benefits (Dinev & Hart, 2006). These benefits usually encompass financial rewards, personalization, and social adjustment, whereas privacy risk mirrors the belief of an individual to incur potential cost due to the shared information (Smith et al., 2011)

Nevertheless, the privacy calculus has its limits, especially when it comes to explaining the privacy paradox. This phenomenon describes situations where users claim to be concerned about privacy but still decide to disclose large amounts of data for small rewards (Norberg et al., 2007). Responding to the limitations, another stream of privacy research has evolved criticizing the theoretical assumptions of the privacy calculus such as rationality (Acquisti & Grossklags, 2003; Acquisti et al., 2016). Recently, an increasing number of studies criticized the assumption that the benefits emerging from data disclosure solely refer to a self-focused or personal-only perspective (Ghaffar & Widjaja, 2023; Nabity-Grover et al., 2020; Rohunen & Markkula, 2019). In contrast to the rather self-centered characteristics of the privacy calculus, there is increasing evidence in the literature that people not only consider their personal benefits when making decisions on data disclosure. In the literature on social networks, this phenomenon is described as the social calculus (Nabity-Grover et al., 2020; Wagner et al., 2018). It assumes that people take an “other focus” considering others' perspectives in evaluating the costs and benefits of sharing information (Buller & Burgoon, 1996). Tightly related to the concept of other-focused data disclosure is the term prosocial data disclosure, which is defined by Ghaffar and Widjaja (2023, p. 3) “as a form of prosocial behavior where individuals disclose their data with the intention to benefit others”.

Various streams of research display the increasing relevance of prosocial data disclosure. In the field of data donation (Hillebrand et al., 2023; Pfiffner & Friemel, 2023; Skatova & Goulding, 2019) people are willing to share data to support others despite not receiving any objective personal benefit in return. Similarly in the context of COVID-19 tracing apps, many studies reveal that the benefits for society are an important driver for the adoption and intention to use the app (Carlsson Hauff & Nilsson, 2023; Dooley et al., 2022; Kuo, 2023; Trang et al., 2020) or the disclosure of an infection (Jörling et al., 2023). On the other hand, there are also studies in the tracing-app context that did not find evidence of the influence of social benefit appeals compared to individual motives (Matt et al., 2022; Munzert et al., 2021; Seberger & Patil, 2021).

Several questions arise from the current state of the literature on prosocial data disclosure. First, data donation and the tracing app context share the fact that the data-receiving entity is usually non-profit. Hence, it is unclear if social benefit appeals are also effective in commercial contexts as the potential to support others' well-being with data is not necessarily bound to non-profit institutions receiving the data. Second, in the previous studies, the social benefits materialized across large fractions of society if not even society as a whole due to being used by medical research or fighting COVID-19. Hence, it is unclear whether social benefit appeals are also relevant within smaller samples of society. Third, the tracing app context is very specific as many of these studies have been carried out during the covid-pandemic. Also, due to the mixed results in the tracing-app studies, there is no clear indication of how effective other-focused benefit appeals would be in terms of adoption or data disclosure when applied in other scenarios entailing personal as well as social benefits, such as AI health services.

Thus, not only does the aspect of perceived benefits in the privacy calculus deserve further attention, but also the perceived risks are considered a key factor in privacy decision-making and are weighed against perceived benefits in the privacy calculus. However, especially in the context of AI-based services users cannot evaluate their privacy risk as their privacy rather becomes an object of uncertainty (Al-Natour et al., 2020). While both concepts of risk and uncertainty deal with partial information, uncertainty denotes subjective probabilities whereas risk is estimated with a priori calculable probabilities (Dimoka et al., 2012). Driven by asymmetric information (Acquisti et al., 2015), uncertainty affects privacy-related information practices by the absence of information regarding the characteristics, usage, and protection of collected data (Al-Natour et al., 2020). As a result, customers lacking this information are not qualified enough to imagine an appropriate level of privacy risk. In conclusion, privacy uncertainty is not about consumers' risk assessment but rather their ability to accurately evaluate the privacy of their information (Acquisti et al., 2007). However, based on current research, it remains unclear whether uncertainty translates to positive or negative results regarding data disclosure. Some studies suggest that a lack of information negatively affects the willingness to disclose data (Acquisti et al., 2015; Acquisti et al., 2007) deducted from qualitative reasoning. Conversely, there is a scarcity of empirical studies testing this assumption. Pavlou et al. (2007) show in an experiment within a B2C e-commerce setting that perceived uncertainty decreases purchase intention. However, their focus is on the seller and product albeit not on privacy uncertainty regarding the data processed. Al-Natour et al. (2020) show that privacy uncertainty negatively affects perceived risk, intention to use an app, and even the willingness to pay for an app. However, to date, the literature does not provide a clear answer to the question of how privacy uncertainty influences the willingness to disclose data, particularly in the context of AI health services.

Intending to reduce information asymmetries and resolve ambiguity (Fast, 2019; Karwatzki et al., 2017), privacy transparency features qualify as an appropriate tool to mitigate privacy uncertainty. The concept of privacy transparency refers to how well service providers inform users about a firm's practices regarding the handling of data (Karwatzki et al., 2017). From the customers' perspective, transparency features differ from privacy policies in that they aim to provide a clear and accessible overview of what data is collected and how it may be used by organizations (Awad & Krishnan, 2006). The dimensions of privacy transparency usually encompass the information on the purpose for using the data, the scope of data collection as well as information on how the data will be shared, processed, and protected (Hashim & Wang, 2022). Hence the main purpose of privacy transparency features is to enable consumers to make well-informed and self-serving privacy decisions (Tsai et al., 2011). However, as current research shows, there are inconclusive results on the effectiveness of privacy transparency features. In essence, there are three different kinds of outcomes (Sleziona & Widjaja, 2022). The literature either shows positive effects on disclosure (Guo et al., 2022; Wiencierz & Luenich, 2022), no effects (Betzing et al., 2020; Karwatzki et al., 2017), or even negative effects on disclosure (Marreiros et al., 2017; Martin, 2016). Despite its conceptional connection to privacy uncertainty, the literature is scarce on whether privacy transparency features impact privacy uncertainty. To the best of our knowledge, only Al-Natour et al. (2020) find that information on the collection, use, and protection of data alleviates privacy uncertainty in the context of mobile apps. Hence, the question arises, whether this relationship also translates to the context of AI health services involving even more sensitive data requests.

Besides the consumers' difficulties in fully recognizing the benefits and risks regarding data disclosure, another challenge for them is to weigh them appropriately. Construal level can be used as an indicator predicting the weight of benefits and risks in the decision-making process. As Solove (2021) argues people do not always engage in rational risk-benefit trade-offs but rather choose what is on the forefront of their

thoughts. In the special case of health services, this could mean that risks preponderate in relation to the benefits (Clark et al., 2023; Keith et al., 2022). Keith et al. (2022) explain this effect based on CLT which argues that the risks are often more concrete for people than the benefits. The CLT connects individuals' conceptualizations of the psychological distance of occurrences to their degrees of abstraction. Since individuals primarily encounter the present moment firsthand, they generate mental interpretations, the so-called construals, to depict entities and occurrences beyond immediate sensory access (Trope & Liberman, 2010; Trope et al., 2007). The construal level resembles whether an entity or occurrence is processed rather abstractly (high-level construal) or concretely (low-level construal). For instance, social distance describes the interpersonal closeness of events, implying that events further from the self are represented on a higher construal level.

Within the subject of privacy in data disclosure, there is a small yet growing fraction of the literature that has investigated the influence of construal levels. Bandara et al. (2017) argue that the privacy paradox might be explained by construal level theory as privacy values are more abstract yet psychologically distant than shopping benefits. Hallam and Zanella (2017) show that a privacy breach that is framed temporally more distant has a smaller impact on everyday choices. Furthermore, the construal-level theory has been applied to deliver explanations on the effectiveness of privacy statements and policies (Cowan et al., 2021; Zhang et al., 2020). Finally, Butori and Miltgen (2023) show that framing benefits and risks in terms of their construal level of concreteness affects disclosures. However, so far studies applying CLT in the privacy context concentrated on the self-focused data disclosure paradigm. According to Trope and Liberman (2010), psychological distance can have consequential implications also for prosocial behavior. Nevertheless, most contributions within the realm of privacy research apply CLT either as a theoretical framework or only manipulate the number of details associated with the variable of interest. Besides Hallam and Zanella (2017), there is a lack of actual empirical manipulation of construal level based on psychological distances. Further, the literature on prosocial behavior suggests that people are more likely to support those they perceive as similar to themselves (Touré-Tillery & Fishbach, 2017). However, the current privacy literature does not indicate whether the social proximity of the beneficiaries also facilitates prosocial data disclosure.

Research Model & Hypotheses

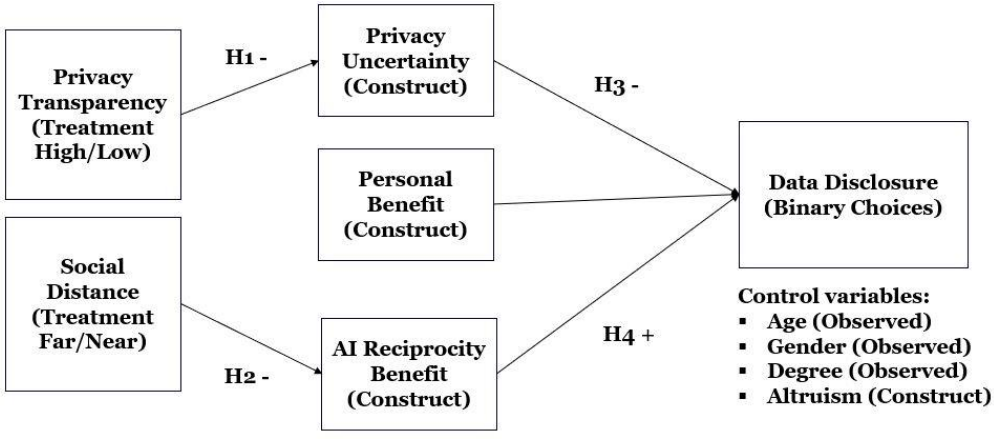

Figure 1. Research Model

Notes: We did not formulate a hypothesis for the positive impact of personal benefit on data disclosure since this relationship has been examined widely in various privacy studies.

Based on the above theoretical foundations we designed our research model as depicted in Figure 1. Accordingly, we expect transparency features to reduce privacy uncertainty. As outlined in the previous section we define privacy transparency features as information provided by the service provider on how the data will be shared, processed, and protected (Al-Natour et al., 2020; Hashim & Wang, 2022). Privacy uncertainty is described as the absence of information regarding the characteristics, usage, and protection of data (Al-Natour et al., 2020). Based on the conceptual relatedness, we propose that privacy transparency

features are a relevant predictor of privacy uncertainty. That argumentation is also supported by the fact that transparency features help to reduce information asymmetry and thereby mitigate ambiguity (Fast, 2019; Karwatzki et al., 2017) which are assumed drivers of privacy uncertainty (Al-Natour et al., 2020). Research in the context of mobile apps finds that the provision of transparency features has the potential to alleviate privacy uncertainty (Al-Natour et al., 2020). However, in the field of AI health services, the data requested are even more sensitive compared to a mobile app context. Thus, we argue that information asymmetry has an even larger impact on the decision-making of consumers in the domain of AI health services. Hence, transparency features are predicted to reduce privacy uncertainty in this context. Thus, we hypothesize the following:

> ***Hypothesis 1 (H1):*** *Privacy transparency features will have a negative impact on privacy uncertainty.*

Further, we expect that increasing social distance to the beneficiaries of data disclosure will negatively affect the perceived AI reciprocity benefit. We conceptualize AI reciprocity benefits as the mutual benefits all users of an AI service experience by disclosing their data. We derived the concept of AI reciprocity from the observation that AI services generate data network effects, driven by statistical learning processes (Gregory et al., 2021). As a result, the sharing of data increases the service quality for all users of such a service. In the specific context of AI health services, we argue that increased service quality also translates to increased well-being and health. This can be achieved by using a wider variety of data sources, allowing algorithms to detect health issues earlier and provide more accurate health recommendations. Another yet similar outcome could also be the development of new services due to insights from a more diverse dataset. In both cases these benefits spill over to all users of the service, resembling a social benefit. Hence, the concept of AI reciprocity entails personal as well as social benefits. As recent literature on CLT (Butori & Miltgen, 2023; Clark et al., 2023) has shown, the construal level influences the relevance of benefits and risks in the privacy calculus. Further Touré-Tillery and Fishbach (2017) conclude that people are more willing to help other people they perceive as socially close. This tendency can be explained from a construal level perspective as information is processed on a lower construal level for socially close instead of socially distant others (Trope & Liberman, 2010). Within the context of AI health services, we argue that the AI reciprocity benefit entails a prosocial component, as the sharing of data also benefits the health and well-being of other people in the system. Thus, we argue that not only in prosocial behavior but also in prosocial data disclosure, people perceive social benefits as less abstract for supporting close others compared to more distant others. Thereby, the AI reciprocity benefit gains more weight during decision-making. Hence, we hypothesize:

> ***Hypothesis 2 (H2):*** *Social distance will have a negative impact on the AI reciprocity benefit.*

Additionally, we expect privacy uncertainty to negatively affect the amount of data disclosure. In this context, we define the amount of data disclosure as the amount of data participants provide in our scenario. Privacy uncertainty has been shown to negatively influence perceived risk, intention to use an app, and willingness to pay for an app (Al-Natour et al., 2020). However, we argue that especially regarding AI health services dealing with substantial amounts of sensitive data, people's actions are even more dependent on their perceived privacy uncertainty compared to the context of mobile apps. As the intention to use a data-driven service encompasses the disclosure of data, we hypothesize:

> ***Hypothesis 3 (H3):*** *Privacy uncertainty will have a negative impact on the amount of data disclosure.*

Lastly, we expect that the AI reciprocity benefit will positively affect the amount of data disclosure. The literature streams on other-focused as well as prosocial data disclosure have shown that people do not only disclose data for their individual benefit (Carlsson Hauff & Nilsson, 2023; Nabity-Grover et al., 2020; Trang et al., 2020; Wagner et al., 2018). In the context of AI health services, we contend that AI reciprocity generates benefits that enhance the well-being of all users, thereby also benefiting other users within the system. In contrast to the current research stream on prosocial data disclosure, we do not assume that the appeal of disclosing data to benefit others depends on a non-profit organization receiving the data. It does also not depend on the reach of the benefit materialized. Instead, we argue that AI reciprocity facilitates data disclosure if people understand that disclosing their data indeed supports other users' well-being. By delivering an opportunity to generate personal as well as social benefits, AI reciprocity drives data disclosure among participants. Thus, we hypothesize:

Hypothesis 4 (H4): *The AI reciprocity benefit will have a positive impact on the amount of data disclosure.*

Methodology

Design and Procedure

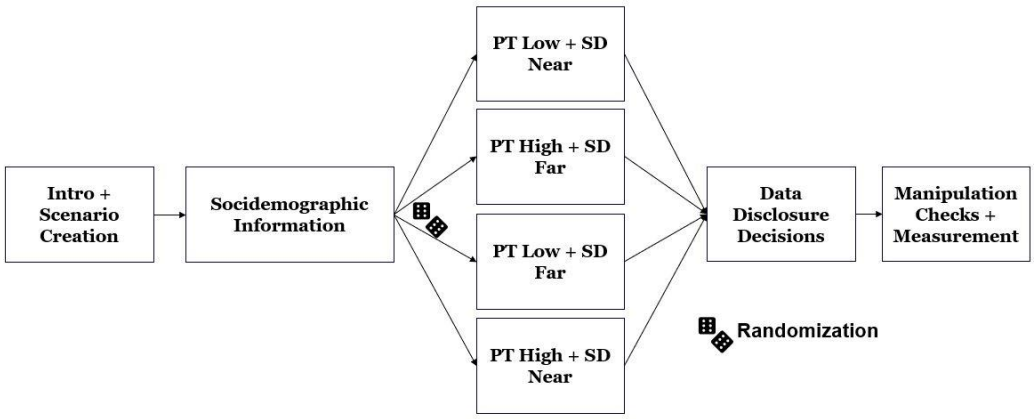

Figure 2. Experimental Flow

Notes: We also randomized the order of the Privacy Transparency (PT) and Social Distance (SD) treatments

To evaluate our research model, we designed a 2 (privacy transparency: high vs. low) x 2 (social distance of beneficiary: far vs. near) between-subject online experiment. Each participant was randomly assigned to one of the four treatment blocks as visualized in Figure 2. We collected data from 251 German participants via Prolific. Each participant earned 1.20 £, the mean age was 29.8, and 49 % were female. To create a realistic environment in which we could assess the willingness to disclose data for an AI health service, we chose the context of a market research study conducted by a startup called "SmartLifeAI" regarding the acceptance of smart services in apartments and created a corresponding cover story. This cover story included detailed information on how smart services use the data to create personalized health recommendations. Figure 2 depicts the experiment's sequence.

Following an introduction, including the scenario creation of a market research study on smart health services in apartments as well as questions on demographic information, the participants were randomly assigned to one of the four treatment blocks. After receiving the treatment, the participants were asked to make twelve binary decisions on whether they would share vs. not share the specified data when using the smart health service, as listed in Table 1. Lastly, we included a post-task questionnaire with manipulation and attention checks, as well as constructs to measure our model, followed by a debriefing.

Experimental Treatments

To incorporate the treatment of privacy transparency we draw on Al-Natour et al. (2020). Accordingly, we use similar dimensions referring to the collection, use, and protection of data, whereas we slightly adapted the detailed information regarding the usage of data to the context of the sensitive information requested in our study. In the condition of low privacy transparency, participants were only provided information on what data is used based on the twelve types of data disclosure outlined in Table 1. In contrast, participants in the privacy transparency high condition were shown additional information addressing the topics of how their data is used and protected by SmartLifeAI, and with whom their data is shared before we asked them to make their decisions on data disclosure To factor in the treatment of the social distance of the social benefit appeals following CLT, we used a "similar vs. dissimilar others" framing. We chose framings either stressing the social benefit of AI reciprocity to the well-being of dissimilar others (socially far) or the well-being of similar others (socially near).

Would you disclose the following information to use the SmartLifeAI services?	**Yes**	**No**
Heart rate via our wearable fitness tracker		
Sleeping patterns via our wearable fitness tracker		
Daily steps via our wearable fitness tracker		
Stress (breathing) via our wearable fitness tracker		
Movements in the living room via our floor sensors		
Movements in the bedroom via our floor sensors		
Movements in the bedroom via our cameras		
Movements in the living room via our cameras		
Nutritional data of your groceries via our smart refrigerator		
Body composition (weight, fat, muscle mass) via our smart scale		
Chronic diseases via our smartphone app		
Psychological health via our smartphone app		

Table 1. Binary Choices Regarding Data Disclosure

The sociodemographic attributes of age and gender are an established tool in the literature on interpersonal closeness (Liviatan et al., 2008). Hence, to achieve variations in perceived similarity we showed the participants pictures of another user they could support by disclosing their data. Depending on the condition, this person was either of similar age and identical gender (socially near) or differing age range and gender (socially far). We also added further descriptions to the pictures emphasizing either differences or similarities between the participant and other users portrayed in the picture such as lifestyle or health status.

Measurements

We measured the dependent variable of data disclosure by the amount of data the participant decided to share (0-12). To assess the effectiveness of the treatments, we also included manipulation checks based on a 7-point Likert-type scale ranging from 'strongly disagree' (1) to 'strongly agree' (7). To determine the effect of the treatment on privacy transparency, we asked the participants to evaluate whether the information given on how their data was protected was detailed and understandable to them. To assess the impact of the treatment regarding the social distance of the social benefit appeal we asked the participants whether they believed that people more similar to them would benefit more from their data than people dissimilar to them.

Further, we also collected information on several constructs relevant to our study drawing on previous research and also based on a 7-point Likert-type scale. Altruism was measured based on Anderson and Agarwal (2011), privacy uncertainty based on Al-Natour et al. (2020), and personal benefit based on Li et al. (2014). We slightly modified the construct of reciprocity used by Fox et al. (2021) to suit better the context of AI health services. Furthermore, we checked for the socio-demographic background of the participants (age, gender, education). Additionally, we also added a question on whether the participants would rather use the AI health services for the personal or societal benefits that are generated. We measured this tradeoff based on a 7-point Likert-type scale ranging from 'Only Social benefit' (1) to 'Only personal benefit' (7). We also added two attention checks to be able to screen for participants with insufficient levels of focus.

Analysis & Results

In this section, we detail the analysis as well as the data validation procedures undertaken to establish the construct validity and reliability of the measurement items applied. After establishing these necessary pre-conditions, we continued to evaluate the proposed model using structural equation modeling (SEM). All

data validation and model testing were completed in R (R Core Team, 2024) using the lavaan SEM package (Rosseel, 2012). Due to failed attention checks, our final sample was reduced to N = 240. For assessing the manipulation check of privacy transparency, we used a Welsh t-test, which revealed significant group differences in participants' perceived privacy transparency ($M_{lowPrivacyTransparency}$ = 3.71, $M_{highPrivacyTransparency}$ = 5.04, t (237) = -6.14, p < .001). For the manipulation analysis of the social distance, we also applied the Welch t-test, which revealed significant group differences in the participants' perceptions of the social distance of the beneficiary of data disclosure ($M_{farSocialDistance}$ = 3.89, $M_{nearSocialDistance}$ = 5.66, t (207) = -7.56, p < .001). However, there was no significant difference regarding the mean response to our tradeoff question between the importance of social vs. personal benefits regarding the services ($M_{farSocialDistance}$ = 4.88, $M_{nearSocialDistance}$ = 4.87, t (238) = .07, p = 0.530).

Construct Validity and Reliability

Construct Name	**CR**	**AVE**	**(1)**	**(2)**	**(3)**	**(4)**
1. Privacy Uncertainty	.925	.754	*.868*			
2. Personal Benefits	.940	.761	-.344***	*.872*		
3. Altruism	.835	.713	-.046	.214*	*.844*	
4. AI Reciprocity	.934	.873	-.351***	.728***	.193*	*.934*

Table 2. Construct Correlations, Reliabilities, and AVEs

Notes: N = 240; CR = Composite Reliability; AVE = Average Variance Extracted; Italicized values along the diagonal are the square root of the AVE; *** = significance at p < .001; ** = significance at p < .01; * = significance at p < .05

To ensure the validity and reliability of the measures used in our analysis, we initially conducted a factorial validation. Given that our model is built upon prior literature, encompassing constructs and relationships derived from established theories, we employed confirmatory factor analysis (CFA) to assess the measurement model. CFA is suitable in scenarios where existing theory indicates expected relationships among indicators and their corresponding factors (Brown, 2015), aligning with our research context. During model fitting, we removed items that exhibited weak loadings on their respective factors, enhancing the model's reliability. The refined model demonstrated a good fit to the data (Chi-sq = 85.68, df = 59, robustCFI = 1.00, robustRMSEA = 0.000) (Hair et al., 2010; Yuan et al., 2016).

With the model fitting the data well, we proceeded to calculate correlations, reliabilities, and AVE to reinforce factorial validity. These metrics are detailed in Table 2. To establish factorial validity, it is recommended that the AVE for each construct exceeds 0.5, indicating adequate convergent validity. Furthermore, discriminant validity is demonstrated when the square root of a construct's AVE is greater than the correlation between that construct and all other constructs in the model (Hair et al., 2010). As illustrated in Table 2, our model's constructs meet these criteria. Reliability is established through composite reliability values exceeding 0.7 (Fornell & Larcker, 1981). Accordingly, the reliability values presented in Table 2 demonstrate sufficient reliability for our constructs. Because all survey items were measured using the same method through an online experiment, the possibility exists that some of the spread variance among the constructs is due to a common method rather than the underlying relationships among the constructs. As a countermeasure, we randomized the order of items displayed to the participants. Accordingly, all correlations shown in Table 2 are below 0.90 implying that there is no significant indication of a common-method bias (Pavlou et al., 2007).

Model Testing Results

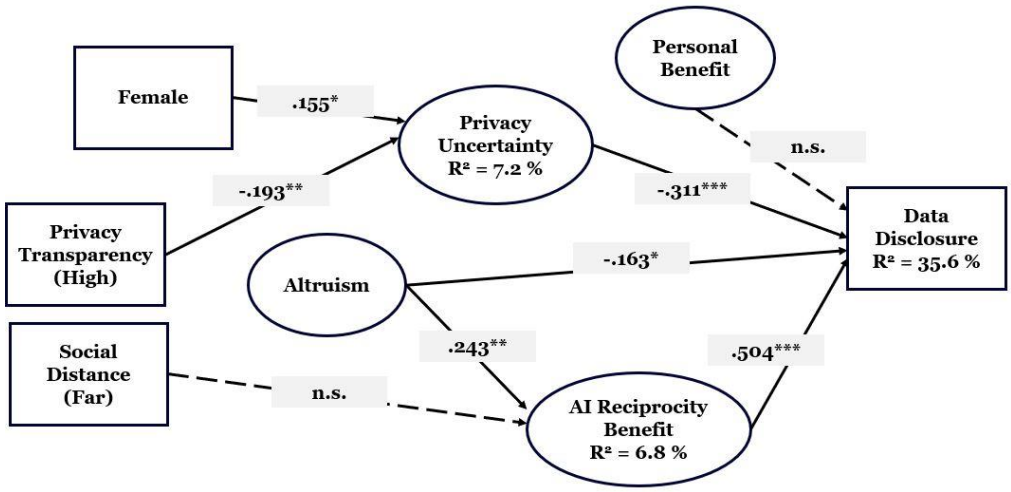

Figure 3. Research Model with SEM Results

Notes: *** = significance at p < .001; ** = significance at p < .01; * = significance at p < .05; Only those control variables having significant effects on the endogenous variables are included in the graph.

We tested the theoretical model shown in Figure 1 using covariance-based SEM with robust maximum likelihood estimation. Therefore, we included our treatment variables privacy transparency (high = 1) and social distance (far = 1) as dummy variables. In summary, we used altruism, age, gender, and academic degree as control variables for all the endogenous variables in the model. Consequently, we also dummy-coded gender (female = 1) and academic degree (yes = 1). The final model is shown in Figure 3 with model testing results, also portraying the significant effects of the control variables of gender and altruism on the respective endogenous variables. Fitting the structural model to the data produced fair indications of fit (Chi-sq = 338.84, df = 130, robustCFI = 0.93, robustRMSEA = 0.077) (Hair et al., 2010; Yuan et al., 2016). The tested hypotheses, along with their corresponding path estimates and significance levels, are summarized in Table 3. The testing results indicate general support for many of the relationships proposed in the model. These results are discussed in the context of their broader implications in the following section.

Discussion

Hypothesis	Path Est.	Supported
1. H1 Privacy Transparency -> (-) Privacy Uncertainty	-.193**	**Yes**
2. H2 Social Distance -> (-) AI Reciprocity Benefit	n.s.	No
3. H3 Privacy Uncertainty -> (-) Data Disclosure	-.311***	**Yes**
4. H4 AI Reciprocity Benefit -> (+) Data Disclosure	.504***	**Yes**

Table 3. Hypothesis Testing Results

Notes: *** p < .001; ** p < .01; * p < .05

This study was motivated by the need to gain a deeper understanding of the mechanisms that influence users' privacy-related decision-making regarding the context of commercial AI health services. The necessity to delve deeper into this topic stems from the fact that the general privacy calculus has several shortcomings to accurately map this process. This is the case due to two specific aspects of AI services. Firstly, we argue that driven by the characteristics of AI reciprocity, consumers do not exclusively build their disclosure decisions upon self-centered motives. Instead, they also factor in the prosocial component

related to AI health services entailing the potential to support other users in the system. Secondly, we propose that the data-intensive nature of AI health services highlights the uncertainty surrounding data collection, usage, and protection. Hence, in this context, perceived uncertainty is a more appropriate predictor for data disclosure than perceived privacy risks. Therefore, our research objective was to identify how privacy transparency and the social distance of the beneficiaries impact the privacy calculus for commercial AI health services. For this purpose, we introduced privacy uncertainty based on the definition of Al-Natour et al. (2020) and drew on the empirical studies on privacy transparency features (Betzing et al., 2020; Karwatzki et al., 2017; Wiencierz & Luenich, 2022).

Further, we deducted the construct of AI reciprocity from the concept of data network effects (Gregory et al., 2021) and derived a corresponding measure from the literature on reciprocal benefits (Fox et al., 2021; Hamari & Koivisto, 2015). We also introduced the concept of the CLT, drawing from its latest applications in the privacy literature (Butori & Miltgen, 2023; Clark et al., 2023). On top of that, we inferred from the literature on prosocial behavior (Touré-Tillery & Fishbach, 2017) how the social psychological distance might also influence prosocial data disclosure. Finally, we designed a randomized experiment and assessed our research model with 240 participants.

Our resulting model in Figure 3 outlines the high importance of AI reciprocity benefits concerning data disclosure in the context of AI health services. Despite being known as a strong predictor of data disclosure in privacy research (Dinev & Hart, 2006; Smith et al., 2011), the personal benefit construct becomes insignificant in our model when adding the AI reciprocity benefit. The concept of AI reciprocity also entails personal benefits to some extent, which explains their higher correlation compared to the other constructs in the model. Such a finding shows how AI reciprocity benefits overpowered personal benefits. Also, these outcomes show that people have a higher propensity towards sharing sensitive data when they perceive it as an act to support all users in the system instead of obtaining mere individual benefits. The relevance of the well-being of others in the participants' decisions is also mirrored in our tradeoff question regarding the importance of social vs. personal benefits of using health services. The results show that people consider both benefit types almost equally important. Therefore, our findings support the paradigm of other-focused data disclosure (Nabity-Grover et al., 2020; Wagner et al., 2018) also within a commercial context. In addition, our study confirms the importance of reciprocal benefits that Fox et al. (2021) found in the context of adopting COVID-19 tracing apps. Furthermore, this outcome is in line with the studies affirming that perceived social benefits positively affect data disclosure (Jörling et al., 2023; Rohunen & Markkula, 2019).

Despite our manipulation check being successful, the treatment of social distance failed to increase the gravity of the perceived AI reciprocity benefit. One conceivable explanation is, that AI reciprocity can be seen as a complex interplay of personal and social benefits. Accordingly, by not being entirely of a prosocial nature, this might have attenuated the effect of the social distance of the beneficiary. Another explanation could be that because our sample consists of relatively young individuals, the strategy of emphasizing social distance from older people might have had unintended consequences. Seeing images of elderly individuals possibly intensified feelings of needing assistance. An additional insight from our experiment is that the social distance treatment also failed to emphasize the strength of the social benefit in our tradeoff question. This result may also indicate that manipulations of social distance only work effectively in pure donation settings with the data receivers being even more severely in need, which deserves further attention in future research.

In contrast to our social distance manipulation, altruism is positively associated with AI reciprocity. This relationship is reasonable, as AI reciprocity can be considered a form of prosocial benefit. It follows that people exhibiting a high propensity to help others are also more inclined to perceive a higher AI reciprocity benefit. Counterintuitively, altruism also has a negative direct effect on data disclosure. One conceivable explanation is that the commercial context of our AI health service scenario led to a crowding-out effect on the altruistic motivation to share data. Nevertheless, this unexpected finding deserves further attention in future research. It also highlights the complexity of the construct of AI reciprocity in terms of balancing personal as well as prosocial benefits. As Figure 3 shows, our model empirically supports our hypothesis that privacy uncertainty is negatively associated with data disclosure. Responding to the scarcity in the empirical research domain of privacy uncertainty (Al-Natour et al., 2020; Pavlou et al., 2007), we extend these results by showing that privacy uncertainty is an important determinant of data disclosure within the prosocial context of AI health services. We also find empirical support that transparency features are associated negatively with privacy uncertainty. Thus, our findings extend existing literature (e.g., Al-Natour

et al. (2020)) by showing that transparency features also drive uncertainty in the context of AI health services. However, in contrast to the study of Al-Natour et al. (2020), the variance explained in privacy uncertainty by transparency features is rather low. One explanation is that we compared high vs. low transparency instead of full vs. none. However, the observation that gender had a significant impact on privacy uncertainty indicates that uncertainty may also largely be subject to personal attitudes and perceptions. Hence, the fact that privacy uncertainty is not primarily predicted by transparency features could provide an alternative explanation for the study results in the literature that downplay the impact of transparency on data disclosure (Betzing et al., 2020; Karwatzki et al., 2017).

Theoretical and Practical Implications

Our study makes several contributions to the works of literature on privacy and other-focused data disclosure (Nabity-Grover et al., 2020; Wagner et al., 2018). We argue that due to data network effects which are inherent to AI-based services, the individual disclosure of data not only yields self-centered benefits. It also yields benefits for other users because the service quality increases with each user disclosing data. A concept we refer to as "AI reciprocity". We also extend the literature on prosocial data disclosure (Ghaffar & Widjaja, 2023; Skatova & Goulding, 2019; Thiebes et al., 2017; Trang et al., 2020) as in the specific context of AI health services, we argue that increased service quality translates to increased well-being for the users. That is, the resulting health services deliver better performance thereby positively affecting the well-being and health of the users. Previous studies on prosocial data disclosure examined the donation of personal information for research purposes (Hillebrand et al., 2023; Pfiffner & Friemel, 2023; Skatova & Goulding, 2019) or the sharing of data in the context of a COVID-19 tracing app (Carlsson Hauff & Nilsson, 2023; Trang et al., 2020). These studies have in common that the data receiver is usually not a profit-oriented company, but a governmental or non-governmental organization. Also, they are often distinguished by the fact that the benefit created spills over to societies as a whole similar to a public good. Our study examines social benefit appeals in a commercial context where the social benefit is limited to the actual service users. The results of our study indicate that in the context of AI health services AI reciprocity benefits are a stronger predictor of data disclosure than personal health benefits.

Furthermore, we contribute to the literature on privacy uncertainty by providing empirical evidence of the negative relationship between privacy uncertainty and the willingness to disclose data (Acquisti et al., 2015; Acquisti et al., 2007; Al-Natour et al., 2020; Pavlou et al., 2007). Our contribution to this subject is twofold. On the one hand, we empirically apply the theoretical construct of privacy uncertainty (Al-Natour et al., 2020) to the context of AI health services and hence prosocial data disclosure. The previous literature only tested the effects of uncertainty in a self-focused setting (Al-Natour et al., 2020; Pavlou et al., 2007). Additionally, to the best of our knowledge, our study is the first that shows a significant impact of privacy uncertainty on the willingness to disclose data in the context of AI health services. As we also found an effect of gender on privacy uncertainty, our study sets the ground for future studies investigating more thoroughly what could be antecedents of privacy uncertainty besides transparency features. Lastly, we contribute to the research stream on privacy transparency (Betzing et al., 2020; Karwatzki et al., 2017; Wiencierz & Luenich, 2022) as our results show that transparency features are associated negatively with privacy uncertainty, also in a prosocial context like AI health services.

In conclusion, our findings challenge the relevance of the privacy calculus as a theoretical underpinning in the context of AI health services. Instead of being driven solely by perceived risks and personal benefits, we argue that data disclosure in such settings is also significantly shaped by privacy uncertainty and AI reciprocity benefits. Consequently, our results indicate that users disclose data not just for personal gain, but also for the collective gain driven by AI-based services and that privacy uncertainty serves as a significant barrier to sharing information. Our research also provides managerial implications. For companies in the AI health service industry, it might be promising to advertise the social benefits provided by the concept of AI reciprocity to potential users. Based on our findings, this should increase consumers' willingness to disclose data compared to a strategy solely emphasizing the personal health benefits generated. Further, our findings propose that providing transparency on the way data are collected and used seems like a reasonable approach to reducing privacy uncertainty.

Future Research & Conclusion

Our study is subject to some limitations. First, as we use a scenario-based approach, we can only ask for intentions to disclose data given our context instead of monitoring actual behavior. Nevertheless, using intentions to predict actual behavior is a well-established practice in privacy research (Alashoor et al., 2018; Dinev & Hart, 2006; Xu et al., 2009). However, future research should conduct studies involving the actual disclosure of health data suited to an AI health service context. Secondly, regarding the manipulation of the social distance, we strived to portray people similar to the participants based on age and gender in the socially close condition. The effect of the treatment regarding social distance would have arguably been stronger if we had created similar examples of peers based on more than those two characteristics. Therefore, we encourage future research to use examples of socially near and far people based on more than two features. In addition, our study opens new avenues for future research. It sets the base for finding further evidence on social benefits affecting data disclosures in commercial settings as well as determining their boundary conditions. Concerning our findings on privacy uncertainty, scholars could investigate in greater depth the antecedents of privacy uncertainty. Regarding privacy transparency, more invasive transparency messages could be evaluated to determine the specific effect of their content and form on data disclosure and privacy uncertainty. Future research could also assess whether social distance has an impact on purely prosocial data disclosure. We hope that our study will inspire more comprehensive efforts to address privacy uncertainty and AI reciprocity benefits to help users make decisions that are beneficial to themselves and others.

Acknowledgements

This work is part-funded by the Foresight Next project sponsored by the German Federal Ministry for Economics and Climate Action.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & di Vimercati, S. (2007). What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *Digital privacy: Theory, Technologies, and Practices* (pp. 385-400). Auerbach Publications. https://doi.org/10.1201/9781420052183-29

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *Proceedings of the 2nd Annual Workshop on Economics and Information Security-WEIS*, *3*, 1-27.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442-492. https://doi.org/10.1257/jel.54.2.442

Al-Natour, S., Cavusoglu, H., Benbasat, I., & Aleem, U. (2020). An empirical investigation of the antecedents and consequences of privacy uncertainty in the context of mobile apps. *Information Systems Research*, *31*(4), 1037-1063. https://doi.org/10.1287/isre.2020.0931

Alashoor, T., Al-Maidani, N., & Al-Jabri, I. (2018). The Privacy Calculus under Positive and Negative Mood States. *Proceedings of the 39th International Conference on Information Systems*, 1-17. https://aisel.aisnet.org/icis2018/security/Presentations/6

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

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28. https://doi.org/10.2307/25148715

Bandara, R., Fernando, M., & Akter, S. (2017). The privacy paradox in the data-driven marketplace: the role of knowledge deficiency and psychological distance. *Procedia Computer Science*, *121*, 562-567. https://doi.org/10.1016/j.procs.2017.11.074

Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2020). The impact of transparency on mobile privacy decision making. *Electronic Markets*, *30*, 607-625. https://doi.org/10.1007/s12525-019-00332-3

Brown, T. A. (2015). *Confirmatory factor analysis for applied research* (2nd ed.). Guilford Press.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203-242. https://doi.org/10.1111/j.1468-2885.1996.tb00127.x

Butori, R., & Miltgen, C. L. (2023). A construal level theory approach to privacy protection: The conjoint impact of benefits and risks of information disclosure. *Journal of Business Research*, *168*, 1-15. https://doi.org/10.1016/j.jbusres.2023.114205

Carlsson Hauff, J., & Nilsson, J. (2023). Individual costs and societal benefits: the privacy calculus of contact-tracing apps. *Journal of Consumer Marketing*, *40*(2), 171-180. https://doi.org/10.1108/JCM-03-2021-4559

Clark, A., Keith, M. J., & Masters, T. (2023). Exploring Privacy Attitudes and Accurate Information Disclosure in Healthcare Contexts. *Proceedings of the 17th International Conference on Information Systems*, 1-17. https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/17

Cowan, K., Javornik, A., & Jiang, P. (2021). Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs. *Psychology & Marketing*, *38*(10), 1799-1813. https://doi.org/10.1002/mar.21576

Dimoka, A., Hong, Y., & Pavlou, P. A. (2012). On product uncertainty in online markets: Theory and evidence. *MIS Quarterly*, *36*(2), 395-426. https://doi.org/10.2307/41703461

Dincelli, E., & Zhou, X. (2017). Examining self-disclosure on wearable devices: The roles of benefit structure and privacy calculus. *Proceedings of the 35th Americas Conference on Information Systems*, 1-5. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/35

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Dooley, S., Turjeman, D., Dickerson, J. P., & Redmiles, E. M. (2022). Field evidence of the effects of pro-sociality and transparency on COVID-19 app attractiveness. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1-21. https://doi.org/10.31219/osf.io/gm6js

Fast, V. (2019). The role of transparency in privacy decision-making under uncertainty. *Proceedings of the 27th European Conference on Information Systems*, 1-12. https://aisel.aisnet.org/ecis2019_rip/32

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/10.1177/002224378101800104

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 1-15. https://doi.org/10.1016/j.chb.2021.106806

Geske, F., Hofmann, P., Lämmermann, L., Schlatt, V., & Urbach, N. (2021). Gateways to Artificial Intelligence: Developing a Taxonomy for AI Service Platforms. *Proceedings of the 29th European Conference on Information Systems*, 1-16. https://aisel.aisnet.org/ecis2021_rp/150

Ghaffar, A. M., & Widjaja, T. (2023). Towards a Theory to Explain Prosocial Data Disclosure-An Explorative Investigation of the Antecedents of Infection Disclosure. *Proceedings of the 44th International Conference on Information Systems*, 1-17. https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/4

Gregory, R. W., Henfridsson, O., Kaganer, E., & Kyriakou, H. (2021). The role of artificial intelligence and data network effects for creating user value. *Academy of Management Review*, *46*(3), 534-551. https://doi.org/10.5465/amr.2019.0178

Guerra, K., & Johnson, V. L. (2023). AI healthcare adoption: a privacy calculus model incorporating emotions and techno-social factors. *Proceedings of the 29th Americas Conference on Information Systems*, 1-6. https://aisel.aisnet.org/amcis2023/sig_adit/sig_adit/21

Guo, X., Zhang, X., & Sun, Y. (2016). The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, *16*, 55-65. https://doi.org/10.1016/j.elerap.2015.11.001

Guo, Y., Wang, X., & Wang, C. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern. *Journal of Enterprise Information Management*, *35*(3), 774-795. https://doi.org/10.1108/JEIM-12-2020-0481

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis: A Global Perspective* (7th ed.). Pearson Prentice Hall Publishing.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217-227. https://doi.org/10.1016/j.chb.2016.11.033

Hamari, J., & Koivisto, J. (2015). "Working out for likes": An empirical study on social influence in exercise gamification. *Computers in Human Behavior*, *50*, 333-347. https://doi.org/10.1016/j.chb.2015.04.018

Hashim, M. J., & Wang, Q. (2022). Using Active Privacy Transparency to Mitigate the Tension Between Data Access and Consumer Privacy. *Proceedings of the 44th International Conference on Information Systems*, 1-17. https://aisel.aisnet.org/icis2022/security/security/2

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), 463-471. https://doi.org/10.1093/jamia/ocaa240

Hillebrand, K., Hornuf, L., Müller, B., & Vrankar, D. (2023). The social dilemma of big data: Donating personal data to promote social welfare. *Information and Organization*, *33*(1), 1-25. https://doi.org/10.1016/j.infoandorg.2023.100452

Jörling, M., Eitze, S., Schmid, P., Betsch, C., Allen, J., & Böhm, R. (2023). To disclose or not to disclose? Factors related to the willingness to disclose information to a COVID-19 tracing app. *Information, Communication & Society*, *26*(10), 1954-1978. https://doi.org/10.1080/1369118X.2022.2050418

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369-400. https://doi.org/10.1080/07421222.2017.1334467

Keith, M., Clark, A., Masters, T., & Wigington, C. (2022). What Makes Health Data Privacy Calculus Unique? Separating Probability from Impact. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 1-10. https://doi.org/10.24251/hicss.2022.589

Klossner, S., Ghanbari, H., Rossi, M., & Sarv, L. (2023). Personalization-Privacy Paradox in Using Mobile Health Services. *Proceedings of the 31st European Conference on Information Systems*, 1-16. https://aisel.aisnet.org/ecis2023_rp/346

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109-125. https://doi.org/10.1057/jit.2010.6

Kuo, K.-M. (2023). Antecedents predicting digital contact tracing acceptance: a systematic review and meta-analysis. *BMC Medical Informatics and Decision Making*, *23*(1), 1-19. https://doi.org/10.1186/s12911-023-02313-1

Li, H., Gupta, A., Zhang, J., & Sarathy, R. (2014). Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision Support Systems*, *57*, 376-386. https://doi.org/10.1016/j.dss.2012.10.043

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8-17. https://doi.org/10.1016/j.ijmedinf.2015.12.010

Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, *127*, 1-11. https://doi.org/10.1016/j.chb.2021.107026

Liviatan, I., Trope, Y., & Liberman, N. (2008). Interpersonal similarity as a social distance dimension: Implications for perception of others' actions. *Journal of Experimental Social Psychology*, *44*(5), 1256-1269. https://doi.org/10.1016/j.jesp.2008.04.007

Marreiros, H., Tonin, M., Vlassopoulos, M., & Schraefel, M. (2017). "Now that you mention it": A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization*, *140*, 1-17. https://doi.org/10.1016/j.jebo.2017.03.024

Martin, K. (2016). Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online. *The Journal of Legal Studies*, *45*(2), 191-215. https://doi.org/10.1086/688488

Matt, C., Teebken, M., & Özcan, B. (2022). How the introduction of the COVID-19 tracing apps affects future tracking technology adoption. *Digital Transformation and Society*, *1*(1), 95-114. https://doi.org/10.1108/DTS-05-2022-0015

Munzert, S., Selb, P., Gohdes, A., Stoetzer, L. F., & Lowe, W. (2021). Tracking and promoting the usage of a COVID-19 contact tracing app. *Nature Human Behaviour*, *5*(2), 247-255. https://doi.org/10.1038/s41562-020-01044-x

Nabity-Grover, T., Cheung, C. M., & Thatcher, J. B. (2020). Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media. *International Journal of Information Management*, *55*, 1-5. https://doi.org/10.1016/j.ijinfomgt.2020.102188

Naous, D., Kulkarni, V., Legner, C., & Garbinato, B. (2019). Information Disclosure in Location-based Services: An Extended Privacy Calculus Model. *Proceedings of the 40th International Conference on Information Systems*, 1-17. https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/4

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105-136. https://doi.org/10.2307/25148783

Pfiffner, N., & Friemel, T. N. (2023). Leveraging Data Donations for Communication Research: Exploring Drivers Behind the Willingness to Donate. *Communication Methods and Measures*, *17*(3), 227-249. https://doi.org/10.1080/19312458.2023.2176474

R Core Team. (2024). *R: A Language and Environment for Statistical Computing*. In R Foundation for Statistical Computing.

Raddatz, N., Kettinger, W. J., & Coyne, J. (2023). Giving to Get Well: Patients' Willingness to Manage and Share Health Information on AI-Driven Platforms. *Communications of the Association for Information Systems*, *52*(1), 1017-1049. https://doi.org/10.17705/1CAIS.05247

Rohunen, A., & Markkula, J. (2019). On the road–listening to data subjects' personal mobility data privacy concerns. *Behaviour & Information Technology*, *38*(5), 486-502. https://doi.org/10.1080/0144929X.2018.1540658

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(2), 1-36. https://doi.org/10.18637/jss.v048.i02

Seberger, J. S., & Patil, S. (2021). Us and Them (and It): Social Orientation, Privacy Concerns, and Expected Use of Pandemic-Tracking Apps in the United States. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-19. https://doi.org/10.1145/3411764.3445485

Skatova, A., & Goulding, J. (2019). Psychology of personal data donation. *PLOS ONE*, *14*(11), 1-20. https://doi.org/10.1371/journal.pone.0224240

Sleziona, P., & Widjaja, T. (2022). Transparency in the Privacy Context: A Structured Literature Review. *Proceedings of the 30th European Conference on Information Systems*, 1-16. https://doi.org/aisel.aisnet.org/ecis2022_rp/124

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015. https://doi.org/10.2307/41409970

Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review*, *89*(1), 1-51. https://doi.org/10.2139/ssrn.3536265

The Economist. (2024). AIs will make health care safer and better. Retrieved 01.04.2024, from https://www.economist.com/technology-quarterly/2024/03/27/ais-will-make-health-care-safer-and-better

Thiebes, S., Lyytinen, K., & Sunyaev, A. (2017). Sharing is About Caring? Motivating and Discouraging Factors in Sharing Individual Genomic Data. *Proceedings of the 38th Conference on Information Systems*, 1-20. https://aisel.aisnet.org/icis2017/IT-and-Healthcare/Presentations/15

Thomas, L. D., & Tee, R. (2022). Generativity: A systematic review and conceptual framework. *International Journal of Management Reviews*, *24*(2), 255-278. https://doi.org/ 10.1111/ijmr.12277

Touré-Tillery, M., & Fishbach, A. (2017). Too far to help: The effect of perceived distance on the expected impact and likelihood of charitable action. *Journal of Personality and Social Psychology*, *112*(6), 860-876. https://doi.org/10.1037/pspi0000089

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, M., & Cheung, C. M. (2020). One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, *29*(4), 415-428. https://doi.org/10.1080/0960085X.2020.1784046

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, *117*(2), 440-463. https://doi.org/10.1037/a0020319

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology*, *17*(2), 83-95. https://doi.org/10.1016/S1057-7408(07)70013-X

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268. https://doi.org/10.1287/isre.1090.0260

Wagner, A., Krasnova, H., Abramova, O., Buxmann, P., & Benbasat, I. (2018). From 'Privacy Calculus' to 'Social Calculus': Understanding self-disclosure on social networking sites. *Proceedings of the 39th International Conference on Information Systems*, 1-17. https://aisel.aisnet.org/icis2018/social/Presentations/20

Wiencierz, C., & Luenich, M. (2022). Trust in open data applications through transparency. *New Media & Society*, *24*(8), 1751-1770. https://doi.org/10.1177/146144482097

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, *26*(3), 135-174. https://doi.org/10.2753/MIS0742-1222260305

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. *Information Systems Research*, *21*(4), 724-735. https://doi.org/10.1287/isre.1100.0322

Yuan, K.-H., Chan, W., Marcoulides, G. A., & Bentler, P. M. (2016). Assessing structural equation models by equivalence testing with adjusted fit indexes. *Structural Equation Modeling: A Multidisciplinary Journal*, *23*(3), 319-330. https://doi.org/10.1080/10705511.2015.1065414

Zhang, Y., Wang, T., & Hsu, C. (2020). The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust. *Journal of Intellectual Capital*, *21*(2), 145-163. https://doi.org/10.1108/JIC-05-2019-0113

Zittrain, J. L. (2006). The generative internet. *Harvard Law Review*, *119*(7), 1974-2040.

Appendix A: Measurement Scales

Construct	Items	Cronbach's Alpha
Privacy Uncertainty (Al Natour et al., 2020)	Overall, I am unsure if SmartLifeAI will safeguard my privacy. Overall, I am uncertain if SmartlifeAI will be good at managing my private information. Overall, I am worried if my information will be safe with SmartLifeAI. Overall, I am concerned that SmartLifeAI may breach formal or informal privacy agreements.	0.924
Personal health benefits (Li et al., 2014)	Using the SmartLifeAI services would improve my access to my health information. Using the SmartLifeAI services would improve my ability to manage my health. Using the SmartLifeAI services would help me to become more informed. Using the SmartLifeAI services would improve the quality of healthcare. I would manage my health more effectively using SmartLifeAI services.	0.940
Altruism (Anderson & Agarwal, 2011)	Helping others is one of the most important aspects of life. I enjoy working for the welfare of others	0.826
AI reciprocity benefit (adapted based on Fox et al., 2021)	I believe that disclosing my data to use the SmartLifeAI services could be mutually helpful to myself and other users. I believe that my participation in SmartLifeAI services could be advantageous to me and other users.	0.932

Table A.1. Measurement Scales and Cronbach's Alpha