Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2023 Research Papers | ECIS 2023 Proceedings

5-11-2023

Data as the New Currency - An Empirical Study Using Conjoint Analysis

Barbara Krumay
Johannes Kepler University Linz, barbara.krumay@jku.at

Stefan Koch
Johannes Kepler University, stefan.koch@jku.at

Follow this and additional works at: https://aisel.aisnet.org/ecis2023_rp

Recommended Citation

Krumay, Barbara and Koch, Stefan, "Data as the New Currency - An Empirical Study Using Conjoint Analysis" (2023). *ECIS 2023 Research Papers*. 259.
https://aisel.aisnet.org/ecis2023_rp/259

This material is brought to you by the ECIS 2023 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2023 Research Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

FDATA AS THE NEW CURRENCY—AN EMPIRICAL STUDY USING CONJOINT ANALYSIS

Research Paper

Barbara Krumay, Johannes Kepler University Linz, Austria, barbara.krumay@jku.at

Stefan Koch, Johannes Kepler University Linz, Austria stefan.koch@jku.at

Abstract

Since data and information are becoming important factors in competitiveness in the digital age, organisations tend to have an enormous appetite for data. However, users are becoming increasingly reluctant to provide their data without receiving some benefits. Therefore, it is necessary to identify the extent to which consumers are willing to protect their data by paying for the use of a service with money or with data. This study investigates willingness to pay for an online service by examining both money and data as currency (i.e. the users' privacy costs). Furthermore, this study is an empirical investigation that uses conjoint analysis to determine whether different service types show different preferences and which characteristics are decisive. The findings show that the online service used has an impact on whether people pay with money or their data.

Keywords: Privacy, Currency, Privacy Costs, Conjoint Analysis.

1 Introduction

Digitalisation and the use of information systems evoke the constant creation and use of data, including personal data left behind by people using information systems. Quite often, this private data is shared—wilfully or not—in exchange for some expected benefits, particularly when people use offerings over the internet, which is the backbone of many developments in the digital age. These benefits, including products and services, are expected to be free of charge (Dou, 2004). However, this is rarely the case (Dou, 2004), since people pay for them by sharing information about themselves when accessing a website or web shop. Clearly, businesses operating on the internet need to attract as many people as possible to leverage network effects (e.g., Church et al., 2008) and generate advertising revenue (Dou et al., 2016). While private data collected from users is valuable for all businesses, advertisers use it to create targeted ads (Malgieri and Custers, 2017). Since regular advertising revenues on websites are decreasing, internet businesses and content providers, such as online newspapers, have suffered from drops in revenue. The collection of private data and the selling thereof have become a business model that creates many privacy issues (Adkinson et al., 2002; Awad and Krishnan, 2006; Buchanan et al., 2007). Since users are becoming increasingly reluctant to share their private data (Acquisti et al., 2015; Benndorf and Normann, 2018), some businesses, such as content providers, offer paid services (e.g. *The New York Times* and the British Broadcasting Corporation [BBC] have introduced so-called paywall systems; (Cook and Attari, 2012; Dou, 2004). However, customers have not received this very well. For example, in 2010, when the BBC introduced a paywall system, a drastic drop in the number of visitors occurred (Dou, 2004). Only a quarter of regular users were willing to pay for an online newspaper (Dou, 2004). For content providers in particular, the dilemma is three-fold: first, users are increasingly reluctant to share their private data, particularly without directly benefitting from it (Acquisti et al., 2015; Benndorf and Normann, 2018); second, users expect that services on the internet are free of charge

(Rana and Weinman, 2015); third, users are becoming more and more annoyed by ads shown on websites (Goldstein et al., 2014). Therefore, businesses must attribute appropriate value to private data (i.e. monetising private data as important information for content providers to price their products and services accordingly). This valuation is influenced by the users' willingness to pay (WTP), either via a monetary payment or the monetisation of their private data (i.e. using private data as currency; (Gates and Matthews, 2014; Rana and Weinman, 2015; Schreiner and Hess, 2013). However, the willingness to share private data seems to be a function of the product (Phelps et al., 2000) as well as a part of the preference structure of buying decisions (Buck et al., 2017). In general, the willingness to share private data depends on various factors, ranging from trust or expected benefits (Dinev and Hart, 2006) to the type of information shared, the perceived control over data after sharing or the removal-request behaviour of a company (Buck et al., 2017; Culnan and Armstrong, 1999). Clearly, the willingness to share data in terms of using private data as currency (Benndorf and Normann, 2018; Norberg et al., 2007) shows similarities to WTP (Breidert et al., 2006; Goes et al., 2010). There have already been some attempts to identify the attributed value of private data as a currency, leading to versioning strategies of the same service (Meinert et al., 2006; Schreiner and Hess, 2013). However, few studies have focused on monetising the value of private data (e.g., Grossklags and Acquisti, 2007; Schreiner and Hess, 2013). One of these studies investigated the monetary value of users' WTP for protecting their private data and the price they would accept for selling their data (Grossklags and Acquisti, 2007). The authors concluded that users are willing to sell their private data only for a low sum (Grossklags and Acquisti, 2007). Another study focused on users' WTP for the protection of private data based on the idea of a freemium model (i.e. offering basic protection functionality to users for free but providing further protection for a specific monetary sum (Schreiner and Hess, 2013); Both studies showed that users are only willing to pay a very low amount of money to protect or their private data (e.g., Grossklags and Acquisti, 2007; Schreiner and Hess, 2013). However, at the intersection of customers' interest in protecting their private data (Acquisti, 2008) and data becoming a currency (e.g., Schwartz, 2003), it remains unclear how people monetise their privacy and the private data they are willing to share. Furthermore, some studies have assumed that this is hardly possible (Buck et al., 2017), as it is a highly complex situation to assess, even though both share characteristics of costs: monetary costs or costs of privacy (Grossklags and Acquisti, 2007). By contrast, companies, to a certain extent, may attribute the value of private data by accepting private data as currency based on the idea of WTP either with money or with private data (Benndorf and Normann, 2018; Hartmann et al., 2016; Rana and Weinman, 2015).

Since the attribution of value to private data shares characteristics with monetary WTP, we suppose WTP can be used as the basis for investigating users' assessment of data as currency (Benndorf and Normann, 2018; Hartmann et al., 2016; Rana and Weinman, 2015). As existing studies remain unclear or even contradictory (Buck et al., 2017), this study aimed at contributing to further developing this research topic, focusing on users' WTP in terms of money compared to bearing privacy costs (i.e. using data as currency). We further investigated the impact of service characteristics and user preferences by focusing on the variety in users' WTP across different service options. Therefore, we asked the following research question: To what extent are users willing to pay with money or bear privacy costs (i.e. using data as currency) for using a particular online service? To answer this research question, we adopted an empirical approach by conducting a survey of users and applying a conjoint analysis to the dataset. The remainder of the paper is organised as follows: First, a brief overview of the current academic discussion is provided that covers the main concepts and terms; next, the methodological approach is described, followed by the conjoint analysis; the paper concludes with a discussion and an outlook for future research.

2 Background Information

When Warren and Brandeis coined the term privacy as the 'right to be let alone' (Warren and Brandeis, 1890), they were influenced by a new technology at the time: photography. More than 50 years later, the UN declared privacy to be among the well-accepted human rights (United Nations, 1948). The internet as a general-purpose technology changed the value of data in general and private data in

particular (Gates and Matthews, 2014; Nolin, 2020), creating ethical and legal issues (Acquisti et al., 2015; Fernback and Papacharissi, 2007; Finn et al., 2012; Nissenbaum, 2020). The ongoing digitalisation further challenges the concept of privacy, as technologies, such as cloud computing or the Internet of Things, enable the automated collection of private data from various sources to gain an advantage (Akter and Wamba, 2016; Cichy et al., 2021; Günther et al., 2017; Meinert et al., 2006; Rana and Weinman, 2015). People using these offerings (e.g. on the internet) often assume that they are allegedly free of charge, yet the true currency is the private data collected while making use of the offers. In this regard, the general idea of privacy as a human right and the responsibility of companies to protect private data collected not only stands in stark contrast to the value private data has for businesses but also the value attributed to it from the customer's point of view (e.g., Culnan and Armstrong, 1999; Fernback and Papacharissi, 2007; Xu et al., 2011).

2.1 Privacy

Privacy as a concept has shown many different yet contradictory characteristics. Overall, privacy is the right of individuals and organisations to decide 'when, how and to what extent information about them is communicated to others' (Westin, 1968). This means that transferring private data is a decision to be made (Acquisti et al., 2015). People seem to be more and more reluctant to share private data (Acquisti et al., 2015), in particular sensitive data (Belanger et al., 2002). However, how people behave may differ from this observation. Different models have been developed to explain people's behaviour when sharing private data. One well-known approach is the privacy calculus model, which assumes that people calculate the value of their private data before giving it away (Culnan and Armstrong, 1999; Dinev and Hart, 2006; Laufer and Wolfe, 1977; Li et al., 2010). It has been stated that people are 'willing to disclose personal information in exchange for some economic or social benefit' (Culnan and Armstrong, 1999). However, research has shown different influencing factors (e.g. in the context of e-commerce (Dinev and Hart, 2006), regarding cultural differences (Trepte et al., 2017) and situational effects (Kehr et al., 2015; Li et al., 2010). Factors such as risk and moral attitudes, general privacy concerns, trust and the expected benefits influence not only the behaviour but also the value attributed to private data (Dinev and Hart, 2006; Kehr et al., 2015). However, not all people seem to follow this rational calculation, and it has been shown that some individuals show paradoxical behaviour. They express their reluctance to share private data (i.e. behavioural intention to share) yet act contradictory (i.e. disclosure behaviour), for example, by disclosing private data on the internet with almost no hesitation (Awad and Krishnan, 2006; Liang et al., 2017; Norberg et al., 2007). This so-called privacy paradox has been vividly discussed, showing that people are not acting purely rationally when it comes to sharing their private data (Awad and Krishnan, 2006; Kokolakis, 2017; Norberg et al., 2007). In this regard, trust seems to have a significant impact on private data disclosure, outperforming risk considerations that might negatively influence the behavioural intention to share data (Norberg et al., 2007; Schoenbachler and Gordon, 2002). Lately, some researchers have argued that concepts such as the Theory of Planned Behavior (Ajzen, 1991) would perfectly explain the phenomenon (Dienlin and Trepte, 2015). However, the privacy paradox might be a logical misconception, arguing that attitudes are stated more generally (i.e. the value of privacy in general) and that behaviour depends on the situation; thus, the two are different (Solove, 2021). In addition, the attitudes of users towards sharing their private data and ignoring any privacy concerns have been referred to as privacy cynicism (Choi and Jung, 2020; Hoffmann et al., 2016; van Ooijen et al., 2022). This phenomenon is seen as a mechanism for coping with ongoing privacy threats (Hoffmann et al., 2016). Privacy cynicism leads to ignorance of privacy threats and the lightheaded use of services on the internet (van Ooijen et al., 2022). However, raising privacy awareness might be a possibility to smooth the rather paradoxical situation (Correia and Compeau, 2017; Oetzel and Gonja, 2011; Pötzsch, 2008). Awareness, particularly information privacy awareness, impacts an individual's assessment and decision when sharing data is at stake (Avgerou and Stamatiou, 2015; Correia and Compeau, 2017). The above-mentioned models aimed at describing or explaining privacy behaviour also have an influence on the value attributed to private data, as further discussed below.

2.2 Attributing the Value of Private Data

The value of private data has been found to be influential when it comes to the decision whether to share data (Dinev and Hart, 2006; Li et al., 2010). The value of privacy is different from that of private data (Solove, 2021). Whereas the value of privacy is a more general concept (e.g. reflected by privacy concerns), the value of private data is directly related to the behaviour in a specific situation (Solove, 2021). As previously mentioned, some concepts assume that people are truly calculating or balancing the benefits of a service or product with their shared private data (Dinev and Hart, 2006). However, people are rarely able to express the value of their private data in monetary terms (i.e. monetising their personal data; (Schreiner and Hess, 2013). To assess the value of a product or service in general, WTP (i.e. the amount of money [or costs] one is willing to pay) has often been discussed (Breidert et al., 2006; Goes et al., 2010). Particularly in a network and platform economy, WTP plays an important role (Shapiro et al., 1998), as it allows companies to address different customer segments with different prices to increase profits (Chellappa et al., 2011; Stole, 2007; Varian, 1989). Based on the WTP of a user, companies disclose different prices (price discrimination) based on customers' characteristics, aiming to find the maximum price they are willing to pay (Varian, 1989). In addition to WTP, the willingness to accept (WTA) a price for a product sold has received some attention (e.g., Horowitz and McConnell, 2003; Simonson and Drolet, 2004). WTA directly focuses on individuals selling products and services (e.g. unused consumer goods; (Simonson and Drolet, 2004). However, WTA and WTP are the same when income effects are not important (Chapman et al., 2017). Since the assessment of the value of private data is not usually related to income effects (e.g. not the business of the individual), the price would be the same (Chapman et al., 2017; Horowitz and McConnell, 2003; Simonson and Drolet, 2004). When it comes to attributing the value of private data, the privacy calculus model seems promising (Dinev and Hart, 2006). However, attempts to calculate the amount of money attributed to private data have shown different results (Gates and Matthews, 2014; Grossklags and Acquisti, 2007; Schreiner and Hess, 2013). Whereas users seem to be not very keen on paying money for protecting their private data (Grossklags and Acquisti, 2007; Schreiner and Hess, 2013), they relate the money paid by companies to buy private data (e.g. name, address, phone, birthdate) to the values of private data (Gates and Matthews, 2014). Some approaches focus on the value of data in general on a specific market, attributing value based on the demand for the data in the market (Rana and Weinman, 2015). The value of private data has also been investigated in an experimental setting by focusing on willingness to sell data (Benndorf and Normann, 2018). The experiment showed that people were more reluctant to share personal information (e.g. birthday) or would at least sell it for a higher price (Benndorf and Normann, 2018). Although the attribution of value to private data seems to be complicated, WTP and using private data as currency (Benndorf and Normann, 2018; Norberg et al., 2007) show similarities (Breidert et al., 2006; Goes et al., 2010). However, existing attempts have not provided a clear picture of the relationship between WTP and the monetising of private data.

2.3 Use of Private Data

The possibility of using private data as currency is directly related to companies' approaches to using this data for their benefits, e.g. enable targeted marketing; (Acquisti et al., 2015; Castells, 2010). Companies need to collect valuable information from their customers to, for example, identify their WTP and customise offers for specific customer segments. Information about customers can be gained by collecting data (i.e. via cookies) or buying customer data (Benndorf and Normann, 2018). This information is used to either directly address the users' WTP or to form customer segments that can then be specifically addressed (Beales, 2010; Berger, 2010), for example, to offer premium products and services (Baker et al., 2001; Phillips, 2021). Price discrimination in general is commonly divided into three degrees: (1) individual price, (2) versioning and (3) customer segments (Acquisti, 2008; Shapiro et al., 1998; Stole, 2007). The first degree—individual price—means meeting exactly the individual's WTP, and it is mainly applied to expensive goods as it requires specific information regarding personal traits and behaviours (Acquisti, 2008). The second degree—versioning—allows a more anonymous form, as the individual person is not addressed; the buying intention determines the WTP, allowing

customers to choose between different versions, group discounts or the quantity of a service or product (Acquisti, 2008; Shapiro et al., 1998; Shivendu and Zhang, 2015; Stole, 2007). The third degree—customer segments—requires private data from customers to be aggregated to build customer segments; the offered price reflects the WTP of the segment, not the individual (Acquisti, 2008; Shapiro et al., 1998; Stole, 2007). The personal price offered to a user should match the WTP (Borgesius and Poort, 2017) and be based on the private data collected (e.g. from the browsing behaviour of an individual) and the analysis thereof (Akter and Wamba, 2016). Although companies' benefit from these mechanisms, this has been seen as an unfair practice (Turow et al., 2009) that may even negatively impact the relationship and trust between buyer and seller (Hinz et al., 2011; Odlyzko, 2009; Shapiro et al., 1998). In particular, the software industry has used these mechanisms broadly to skim the market, increase market share and benefit from positive network effects (Bhargava and Choudhary, 2008; Shivendu and Zhang, 2015). It has even been shown that the pricing of a commercial product (e.g. of a software) benefits from knowing the WTP of an according for-free product (e.g. open source software; (Raghu et al., 2009). To fully apply price discrimination, sufficient market share and mechanisms to hinder the resale of the product are needed (Borgesius and Poort, 2017; Hinz et al., 2011; Shapiro et al., 1998). Since the behaviour of people using the internet (e.g. browsing) is logged constantly without them being fully aware of it (Awad and Krishnan, 2006), users are hardly able to refrain from sharing their information. Data protection regulations exist to ensure that personal data is handled fairly, lawfully and transparently (Voss, 2014). Data protection focuses on protection against misuse in the form of loss or unauthorised use (Hsu et al., 2012) and on the consequences evolving from a misuse of private data (De Hert and Papakonstantinou, 2016). Different regulations and laws focus on the protection of private data, such as the General Data Protection Regulation (European Commission, 2016) valid in EU countries or the California Consumer Privacy Act (State of California, 2020), which has been adopted by other regions in the US (Goldman, 2020). For example, the rules foresee that companies provide privacy policies in an easy-to-read language, improving understanding and awareness (Krumay and Klar, 2020). In addition, clarification of data handling, in particular regarding sharing data with third parties, is required by law to influence their decision on sharing data (Urban et al., 2020). To achieve the goals of such regulations, a profound change in many data-based business models is required (Asdemir et al., 2012; Chen and Huang, 2016; Dou, 2004). The GDPR, for example, asks for privacy by default (i.e. preconfigured privacy preserving settings) and privacy by design (i.e. privacy preserving technologies). As data protection regulations are becoming stricter, services to handle data protection based on decentralised technologies, such as blockchains, have been applied in this regard (Alessi et al., 2018). In light of such regulations, data sharing and the value of private data may be influenced (e.g. by establishing trust and supporting privacy awareness among users; (Correia and Compeau, 2017; Pötzsch, 2008; Schoenbachler and Gordon, 2002).

3 Methodological Approach

As this research asks to what extent users are willing to pay with money compared to bearing privacy costs (i.e. private data as currency) for using a particular online service, we adopted an empirical approach based on a questionnaire and a binary choice-based conjoint (CBC) analysis (Eggers et al., 2018; Raghavarao et al., 2010). A conjoint analysis is often applied in market research (Eggers et al., 2018) to identify the benefits or values associated with individual product features by comparing two combinations of features with predefined properties (Chrzan and Orme, 2000; Eggers et al., 2018; Raghavarao et al., 2010). Choice-based means that the participants are asked to choose one of the combinations (i.e. offers); the choice made can be used to determine the significance of the respective properties on customers and their decisions (Raghavarao et al., 2010). CBC has many advantages compared to other, more traditional approaches (e.g. rating-based conjoint), as it allows a direct comparison between alternatives (choice sets, such as products or offers) to measure utility functions (Louviere and Woodworth, 1983; Raghavarao et al., 2010). In addition, CBC is expected to show higher validity (Eggers et al., 2018). As there are multiple choice sets, different combinations of the choice sets are exposed to the participants for comparison. This step is repeated until all meaningful combinations

are exposed (Eggers et al., 2018). The choice sets (or tasks) themselves are a combination of attributes on different levels developed from the research object. Participants choose the one choice set (among the sets simultaneously exposed), offering the highest individual utility (Eggers et al., 2018; Raghavarao et al., 2010). In conjoint analysis, several variables with different values can be used simultaneously. It is also usually possible that the respondent does not select any of the available combinations (Green and Rao, 1971; Raghavarao et al., 2010). To avoid fatigue in making choices and keeping the survey manageable, binary choices are used (i.e. only comparing two choice sets at the same time). The comparisons are displayed adaptively in a sequence based on the previously given answer; thus, there is no fixed order (Green and Rao, 1971).

Although CBC is often applied in an experimental setting (Eggers et al., 2018), there are studies that use questionnaires based on online survey tools to trigger the combination of different choice sets (Buck et al., 2017). One advantage of an online survey is reduced interviewer bias, as there is no interaction with the interviewer (self-administered). In addition, costs are—compared to telephone and face-to-face interviews—rather low, while the number of people who can be addressed simultaneously is high. Finally, the anonymity of the participants can easily be achieved, which is a precondition for surveys related to privacy to establish trust (Evans and Mathur, 2005; Ilieva et al., 2002; Wright, 2005). With the help of an online survey tool, the combination of questions (i.e. comparing two choice sets and exposing them at the same time for comparison) can easily be achieved. However, online surveys often suffer from a low response rate, a high rate of outliers and unverified respondents (Ilieva et al., 2002). To overcome problems due to participants misunderstanding the online survey (Ilieva et al., 2002), certain measures must be applied during the development of the questionnaire. These measures may include providing a solid base for the questionnaires, such as validated scales or questionnaires that have been used before, thorough pre-testing and revision based on it (Ilieva et al., 2002).

The questionnaire used in this study relied on questionnaires used in existing studies (DIVSI, 2014; VZBV, 2015) and was enriched by questions to collect demographic data. In addition to direct questions, the questionnaire included a comparison of choice sets. The first version of the questionnaire was pre-tested by seven people, leading to only minor changes (i.e. changing the order of the questions, adding more explanations). Thus, the revised version consists of 14 questions (see Table 1).

Topic	Direct Questions (Overview)
Demographic data	Q01: Gender Q02: Age in years Q03: Highest education completed Q04: Main occupation
Internet usage behaviour	Q05: Frequency of use Q06: Services used
WTP	Q07: Attitude towards paying for services
Data sharing	Q08: Influence on data sharing
Compensation	Q09: Knowledge about compensation possibilities Q10: Compensation possibilities used Q11: Consent to pay for not sharing data; Q11.1: reasons why
Personalised adds	Q12: Experiencing the use of data for targeted ads Q13: Attitude towards personalized ads
Privacy statements	Q14: Reading privacy statements before providing personal data

Table 1. Questionnaire overview

The questions were based on existing surveys in the native language of the respondents; thus, they have been translated for this study (DIVSI, 2014; VZBV, 2015). The demographic variables (Q01–Q04) were used to group respondents based on their characteristics (variables used in accordance with both reference surveys). Next, the variables addressing internet usage behaviour (Q05, Q06) were intended to determine whether people who are often online are more willing to pay for an online service or accept privacy costs. Analogously, the following question (Q07) asked whether people who were likelier to use free services were also likelier to share private data more easily (i.e. bear privacy costs). In addition, Q08 tried to assess how much influence the participants thought they had on the collection of their private data. The next three questions (Q09–Q11) were used to assess the respondents' attitudes towards free-of-charge services and how this influenced their privacy behaviours. The two questions on compensation possibilities (Q09, Q10) were meant to identify which compensation method was most commonly used for compensation and whether the respondents were even aware that they were compensating online services with their own data (privacy costs). In particular, the question about whether one would be willing to pay money for complete data protection (Q11) was used to assess basic attitudes about willingness to pay. If the answer to the previous question is no, the reasons for this are elicited (Q11.1). Questions on personalized advertising (Q12, Q13) are used to find out whether people who are more negative towards personalised advertising are also willing to pay for online services to a higher degree. The last direct question (Q14) was used to identify whether people who never read privacy statements were also likelier to share their data.

For the CBC applied, four different choice sets consisting of context and attributes on different levels (Eggers et al., 2018) were developed. The choice sets were attributed to different online services (contexts) showing different characteristics. The first context referred to a social media platform using extensive private data but not necessarily confidential data (in this case, Facebook). The second context referred to an unspecified online television broadcasting service (referred to as online TV), which did not require private data as it was broadcast to all. Finally, a service that needs and uses confidential data for fulfilling the required functionality was used as the third context (in this case, an unspecified telebanking service). Three different attributes have been defined for the choice sets: functionality (two levels), monetary payment (three levels) and privacy costs (two levels). Regarding functionality, two levels were defined: full functionality or reduced functionality. Based on the feedback from the pre-test, the reduced functionality was further explained to the participants by providing an example. For social media, the reduction was described in terms of a maximum of 15 messages per day. For online TV, the reduced service was described as a limited set of channels and no channel rating was provided. For telebanking, the reduced service was described in terms of a maximum of five outgoing payment transfers per month. The attribute monetary payment showed three different levels: low (free of charge), medium (€ 5 per month) or high (€ 20 per month). In terms of privacy costs, there were two different levels: low cost ('Private data will be protected and not used otherwise') and high cost ('Private data is reused and sold to other companies'). This resulted in four distinctive choice sets (Table 2) for all three services (context), which were paired in such a way that there was a distinctive difference in the pairings for the same service (e.g. pairing Offers 1 and 2 for Facebook). We refer to the choice set as 'offers', as they were presented to the participants as offers of service providers. Each respondent was adaptively exposed to at least nine and a maximum of 15 offer comparisons (in pairs of two offers), depending on the answer given in the previous comparison. There were two offers in each quadrilateral, and each respondent had to choose one of the two. Depending on the selected offer, one was led to two service offers.

Participants were invited via a mailing list at a university of about 500 subscribers, encouraging them to spread the invitation (snowball sampling). The online tool used for collecting data only processed fully filled-in questionnaires; thus, no partly filled-in questionnaires had to be excluded. Overall, 106 people responded to the questionnaire.

Choice set	Functionality	Monetary payment	Privacy costs
Offer 1	Full (F)	Medium fee (€ 5 per month) (MF)	Low privacy costs (LP)
Offer 2	Full (F)	No fee (NF)	High privacy costs (HP)
Offer 3	Full (F)	High fee (€ 20 per month) (HF)	Low privacy costs (LP)
Offer 4	Reduced (R)	No fee (NF)	Low privacy costs (LP)

Table 2. Offers used in the survey

4 Results

We provide a brief overview on the results from our survey. First, we describe the results regarding demographics. Out of the 106 respondents, 42% are female, and 58% male, one person did not specify (Q01). The age distribution of the respondents (Q02) showed that almost half of the survey participants were between 21 and 24 years old (more than 85% were between 18 and 35 years old). Regarding the highest education completed (Q03), more than half of the participants had completed secondary school (middle or high school). Slightly more than half (51%) of the respondents were students in a bachelor's or master's degree programme as their primary occupations. This is likely due, in part, to online distribution channels (i.e., mailing list at a university) being used to invite the participants. The remainder of the participants were divided into employed people, with almost 40%, as well as apprentices, high school students and self-employed people (in sum approximately 10%).

Next, we focus on the internet usage behaviour, including the respondents' attitude towards free services as well as control over private data on the internet. Regarding internet usage frequency (Q05), more than a third (37%) answered that they were online all day; likewise, more than half were online several times a day (52%) and 10% of the respondents were online at least once a day, summing up to overall 99% of the respondents being online at least once a day of more. Regarding the use of paid vs. free-of-charge services (Q06), almost two-thirds used mainly free-of-charge services, another third used both paid and free-of-charge services in roughly equal proportions and less than one percent of the respondents used mainly paid services ('exclusively paid services' was never selected). Interestingly, almost 90% did not regard paid services as being more reliable (Q07.a: 'Only online services that charge a fee are reliable'); thus, only 10% of respondents thought that only paid online services were reputable. However, 70% tended to agree with the statement that people pay for free-of-charge online services with their data (Q07.b 'If online services are free-of-charge, one usually pays with their data'). Around three-quarters of respondents agreed with the statement that online services that collect private data were using it (Q07.c 'Most online services that collect personal data from their users also do business with this data'), yet about 25% thought that this was not the case. When asked how they assess their influence on private data after sharing it on the internet (Q08: 'How much influence do internet users have on what happens to their data on the internet?'), most respondents thought that they had little to no influence. Only one person stated that having a lot of influence over one's own data was possible.

When it comes to knowledge regarding compensation possibilities (Q09), more than 80% stated, among other things, that they were aware of paid subscriptions as a compensation method; 75% knew about one-time payments when registering or purchasing as well as the compensation for services via providing personal data. In addition, 45% also knew about pay per use for a service. Additional possibilities mentioned were 'payment with other considerations (e.g. contribute to the server via hosting)' and 'microtransactions'. Regarding the compensation methods used (Q10), about two-thirds had paid at least once through a one-time payment when registering or making a purchase. Almost 60% of the respondents also used the input of personal data ('Entering my personal data and agreeing to use it') and paid subscription accounts at almost the same percentage. A third of the respondents applied pay-per-use strategies. Interestingly, 2% had never used any of these possibilities. When asked whether they would pay money to guarantee complete data protection (Q11 'Would you be willing to pay money to guarantee that your data will be used only the way you want it and not monetized in any other way

without your consent?'), the results were almost even: almost 51% would pay, while 49% would not. Women were more willing to pay for data privacy (61.4%), but a chi-squared test showed no statistical significance, with a p-value of 0.0982. Those who would not pay for data privacy were asked (in an open question) to provide reasons for their reluctance to pay (Q11.1). By far, the most frequently mentioned reason was that they did not trust the promises made (i.e., not using the private data for other reasons as specified). Also, half of them stated, among other things, that their own data were not that interesting to pay money for its protection. Almost a third (32%) thought that everything on the internet should be free and a fifth did not care what happened to their own private data. Significantly, more than half did not feel bothered by personalised advertising (Q12). Regarding the attitude towards personalised ads (Q13), almost 70% of the participants said that they simply ignored the advertising, and for 35%, it was usually not interesting. Just over 40% felt that the ads offered reflect a type of surveillance and 27% were concerned about the protection of their data. Slightly more than 15% experienced ads as positive, since they were made aware of other providers or offers. Almost 10% felt that the advertising corresponded to their interests. This question also gave respondents the opportunity to provide more information, and just a few participants (approximately 5%) stated that this issue did not affect them because they used software to block advertising. Even less participants stated that such advertising led to a purchase (1%), and another 1% found such advertising offensive. A large proportion of respondents did not read the privacy policy (Q14) when they chose an offer from an online service. In particular 45% answered that the do never read a privacy statement and 27% rarely reading it. Less than five percent always read the privacy statement.

In addition to the already described results, the results of the conjoint analysis are described based on their contexts (i.e. three different services—Facebook representing social media platforms, Online TV, Telebanking) used in the Offers. In the questionnaire, some pairings of choice sets (i.e. offers) were not disclosed to all participants. Furthermore, some pairings were not built, as the difference between them would have been difficult to grasp or even confusing. Tables 3 to 5 show the results in terms of pairings of offers, percentage of preferences per offer in the pairing, number of participants having been exposed to this pairing (n) and the p-value from the t-Test, to assess significance of the pairings.

The conjoint analysis applied on the pairings of offers in the context of a social media platform—in our case, Facebook – is shown in Table 3. The reduced functionality (SM Offer 4) is defined as a limitation related to private messages (i.e. sending a maximum of 15 private messages per day to other users), which was also explained in the questionnaire. Since we use here, the preferences always sum up to 100%.

Pairing	Choice set & Preference (%)	Choice set & Preference (%)	n	p-value (t-Test)
SM O1/SM O2	SM Offer 1 (F/MF/LC) 47.2%	SM Offer 2 (F/NF/HC) 52.8%	106	0.5625
SM O2/SM O3	SM Offer 2 (F/NF/HC) 56.0%	SM Offer 3 (F/HF/LC) 44.0%	50	0.4016
SM O2/SM O4	SM Offer 2 (F/NF/HC) 45.3%	SM Offer 4 (R/NF/LC) 54.7%	106	0.3338
SM O1/SM O4	SM Offer 1 (F/MF/LC) 44.3%	SM Offer 4 (R/NF/LC) 55.7%	106	0.2456
SM O3/SM O4	SM Offer 3 (F/HF/LC) 29.8%	SM Offer 4 (R/NF/LC) 70.2%	47	0.0043*

Table 3. Results of conjoint analysis for social media platform (SM) (F = Full functionality / R = Reduced functionality; NF = No fee / MF = Medium fee / HF = High fee; LC = Low privacy cost / HC = High privacy costs)

In the context of a social media platform, the preferences between the pairings where rather close for most of the pairings, indicating that among the participants no clear preference existed. Only the comparison between SM Offers 3 and 4 is on one hand very clear (SM Offer 4 is preferred by 70.2% of the participants) shows statistical significance (Table 3). This means that the respondents would rather accept a restriction of functionality than with money, keeping privacy costs at a low level in both offers

on a rather low level. However, it is important to know that this pairing (SM O3/SM O4) was only exposed to 47 of the participants.

The results shown in Table 4 represent the conjoint analysis in the context of online TV. Limited functionality is understood in terms of reduced number of channels (i.e., not all channels are available) and non-availability of channel ratings. This restricted functionality was explicitly provided as an example in the questionnaire.

Pairing	**Choice set & Preference (%)**	**Choice set & Preference (%)**	**n**	**p-value (t-Test)**
TV O1/TV O2	TV Offer 1 (F/MF/LC) 39.6%	TV Offer 2 (F/NF/HC) 60.4%	106	0.0320*
TV O2/TV O3	TV Offer 2 (F/NF/HC) 50.0%	TV Offer 3 (F/HF/LC) 50.0%	42	1
TV O2/TV O4	TV Offer 2 (F/NF/HC) 38.7%	TV Offer 4 (R/NF/LC) 61.3%	106	0.0190*
TV O1/TV O4	TV Offer 1 (F/MF/LC) 28.3%	TV Offer 4 (R/NF/LC) 71.7%	106	3.0160e-06*
TV O3/TV O4	TV Offer 3 (F/HF/LC) 20.0%	TV Offer 4 (R/NF/LC) 80.0%	30	0.0004*

Table 4. Results of conjoint analysis - context online TV (TV)
(F = Full functionality / R = Reduced functionality; NF = No fee / MF = Medium fee / HF = High fee; LC = Low privacy cost / HC = High privacy costs)

In the context of online TV, most pairings exposed to the participants showed a clear preference for one Offer over the other as well as statistical significance. This was identified in four of the five pairings – only pairing TV O2/TV O3 was evenly spread and not significant (p-value 1). This is interesting since TV O2 and TV O3 are similar in functionality (full functionality), but differ in fee (TV O2 – no fee; TV 03 – high fee) as well as privacy costs (TV O2 – high privacy costs; TV O3 – low privacy costs). However, it is important to mention that this pairing was only exposed to 42 of the participants. As already mentioned, the other four pairings showed a different result. Respondents were likelier to prefer the free offer (no fee) bearing high privacy costs than paying a medium fee per month (TV O1/TV O2). If the price rises to a high fee (€ 20) per month, this difference becomes even more pronounced (TV O3/TVO4). A comparison of TV Offers 2 and 4 also shows that the respondents would rather accept restriction of functionality than paying with their data (high privacy costs). Furthermore, there is statistical significance in the comparison between TV Offers 1 and 4, showing that people would rather pay with limited functionality than pay with actual money. If the amount to be paid increases from a medium to a high fee, the difference between the two offers increases.

Table 5 summarizes the results from the conjoint analysis in the context of a telebanking system (TB). Limited functionality is related to the number of outgoing payment transfers per month (i.e., a maximum of five outgoing payment transfers per month are available). This restricted functionality was explained and stated as an example in the questionnaire. In the context of the telebanking system, the results of the conjoint analysis are very different. Comparing TB Offers 1 and 2, there is statistical significance for a medium fee a month and low privacy costs compared with the free offer with high privacy costs. This pairing was exposed to all participants. Even with an increase to a high fee (i.e. € 20) a month, there is still statistical significance and a majority for the paid offer with low privacy costs (TB O2/TB O3). However, this pairing was exposed to 81 participants. A comparison between Offers 2 and 4 also shows a significant difference. The respondents would rather accept the restriction of functionality than privacy costs.

Pairing	Choice set & Preference (%)	Choice set & Preference (%)	n	p-value (t-Test)
TB O1/TB O2	TB Offer 1 (F/MF/LC) 76.4%	TB Offer 2 (F/NF/HC) 23.6%	106	4.9640e-09*
TB O2/TB O3	TB Offer 2 (F/NF/HC) 24.7%	TB Offer 3 (F/HF/LC) 75.3%	81	1.2260e-06*
TB O2/TB O4	TB Offer 2 (F/NF/HC) 22.6%	TB Offer 4 (R/NF/LC) 77.4%	106	1.0730e-09*
TB O1/TB O4	TB Offer 1 (F/MF/LC) 52.8%	TB Offer 4 (R/NF/LC) 47.2%	106	0.5625
TB O3/ TB O4	TB Offer 3 (F/HF/LC) 42.9%	TB Offer 4 (R/NF/LC) 57.1%	56	0.2891

Table 5. Results of conjoint analysis - context telebanking (TB)
(F = Full functionality / R = Reduced functionality; NF = No fee / MF = Medium fee / HF = High fee; LC = Low privacy cost / HC = High privacy costs)

A further analysis focused on the relationship between demographic characteristics and other questions. Comparing age (Q02) with reading data protection statements before providing personal data (Q14), a significant difference was found for almost all age groups. However, a vast majority of the participants in general stated they are not reading the privacy statements (never: 45%; rarely: 27%) and the results showed no correlation to age (chi-squared test). The results of the conjoint analysis also showed no correlation with age. Similarly, no significant influences were found with regard to gender and education. Therefore, we conclude that demographic variables (Q01: Gender, Q02: Age in years, Q03: Highest education completed) are not influencing the choice of the participants. However, there is a relationship between education and preference for monetary payment instead of bearing privacy costs ($p < 0.05$ for online TV; $p < 0.1$ for telebanking system). Individuals with apprenticeships had a stronger preference for monetary payment in this regard. Similarly, regarding employment ($p < 0.01$ for online TV, $p < 0.05$ for telebanking system), students tended to accept privacy costs more often. A significant correlation ($p < 0.001$) emerged for attitudes regarding personalised advertising. People who would not accept privacy costs were more likely to feel bothered by personalised advertising. This also remained significant in the context of social media platforms and online TV ($p < 0.001$).

5 Discussion

As companies rely on data for advertising and selling their products and services, data have become a currency in the internet economy. However, data as currency means privacy costs to users. With our study, we aimed at answering the following research question: To what extent are consumers willing to pay with money or bear privacy costs (i.e. data as currency) for a particular online service? Empirical data collected with the help of an online survey and a subsequent conjoint analysis supported us in answering this question. In particular, we found that only some demographic characteristics seem to have an influence on whether people are willing to pay with money, whereas other people are willingly bearing privacy costs, i.e use data as currency. Furthermore, is has been shown that the properties of the product might have some influence regarding the adoption of data as currency. Thus, our study contributes to research and businesses alike. We add some insights regarding privacy cynicism (Choi and Jung, 2020; Hoffmann et al., 2016; van Ooijen et al., 2022), a lately discussed phenomenon related to the discussion regarding the privacy calculus model and the privacy paradox (Dinev and Hart, 2006; Norberg et al., 2007; Solove, 2021). In addition, companies may benefit from our study, as it will help them understand which users will accept to pay for a service (paywall) and which will rather use their private data as currency. Furthermore, we identified that the WTP - attributed to the value of private data - of users differs depending on the service used. In short, users are likelier to pay with actual money when the service itself is already critical (e.g. telebanking) and will accept privacy costs when the service is not seen as critical.

The value of private data is hard to assess, especially for users on the internet. As already mentioned, there is an ongoing discussion regarding the privacy calculus vs. privacy paradox (Dinev and Hart, 2006; Norberg et al., 2007; Solove, 2021). The privacy calculus model seems to be the basic underlying concept allowing to attribute value to private data (Dinev and Hart, 2006). However, the true calculation process related to specific offers requiring users to share their private data remains unclear. As our study showed, there are clear preferences when it comes to payment with actual money vs. data as currency (i.e. privacy costs) vs. reduced functionality. In the context of specific offers users are not willing to pay actual money for data protection and are happy to pay privacy costs (i.e. use private data as currency) (van Ooijen et al., 2022). In the context of a social media platform, almost half of the people were willing to pay a medium fee (€ 5) for complete data protection. This value was lower for online TV, where only about 40% of the respondents would pay money for data protection. In contrast, more than three-quarters were willing to pay a medium fee for a telebanking service. A chi-squared test showed that the value of 9.806e-08* was statistically significant (i.e. relation between type of service in a specific context and with the value of data protection). The difference also remained significant for a payment of € 20 (i.e. a high fee, $p < 0.05$). In the case of social media platforms and online TV programmes, only half of those who were willing to pay a medium fee would also pay a high fee, while 75% would still pay a high fee for a telebanking system. For the full sample ($n = 106$), the percentage of those willing to pay a high fee for social media platforms was 20.8%, for online TV 19.8% and for a telebanking system 57.5%. However, for each service type, more than half of the respondents opted for limited functionality and data protection, as opposed to full functionality and no data protection. This means that individuals would rather pay with limited functionality than bear privacy costs. Again, the context (i.e. service type) remained significant ($p < 0.001$). We conclude that privacy cynicism is lower when there is more at stake (i.e. access to financial data). In addition, we propose that privacy cynicism is not only influenced by demographic factors but also by the characteristics and criticality of the service used. In particular, monetary payment and the costs of privacy are just two faces of the same coin, which are used differently depending on the context. However, people know that they can avoid monetary payments by paying with their data, but they would also accept a reduced service. In addition, the service showed that the influence of privacy awareness on the value attribution of private data remains unclear. Privacy awareness has been seen as a way out of the privacy paradox (Pötzsch, 2008), it is interesting that only a minor part of the participants (5%) reported that they always read privacy policies. In addition, only just over half of the participants were willing to pay money to secure the complete protection of their data, influenced by the lack of trust in the guarantee provided by companies. Thus, we assume that privacy awareness is not directly related to the value attribution of private data. This might even support the already expressed opinion, that privacy attitude (related to privacy awareness) and privacy behaviour (in a specific context) are not directly related (Solove, 2021). Even more interesting is the fact that many people did not care about what happened to their private data, assuming that their private data is of no use for other purposes (Q11.1). This fits the newly addressed privacy cynicism (Choi and Jung, 2020; Hoffmann et al., 2016; van Ooijen et al., 2022). As privacy cynicism has also been described as a mechanism to cope with privacy threats (Hoffmann et al., 2016), the following imprudent spread of private data by using online services (van Ooijen et al., 2022) contradicts the privacy calculus model (Dinev and Hart, 2006). Our study showed not only that people assume their private data being unimportant (Q11.1), but also refrain from protecting their data actively.

When it comes to practical implications, we provide some interesting discussion points. First, the above-mentioned knowledge about the value of private data for companies (as the opponent to privacy costs) gives people some power, particularly when the services are not very important to them. For companies, this means that they have to find the right balance between a fee and the data they would like to collect. As Offer 3 (full functionality, high fee, low privacy costs) seems to be only a possibility for a sensible service like telebanking, even offering a medium fee while providing full functionality seems not as attractive as one might assume. Although the fee in our case was not very high, the type of service and other factors seemed to be more influential. As mentioned earlier, content providers (e.g. newspapers) are particularly interested in identifying the WTP—either monetary payment or with data—of their customers, and content (such as news) is perceived as a free good on the internet, whereas for its non-

digital counterpart (the actual newspaper), people are still paying on a regular basis. As we did not specifically address this industry in our study, we think that some research should be conducted in this area to identify the correct balance.

Overall, it can be said that there were participants who would rather pay money instead of bearing privacy costs (i.e. to protect their private data). However, this depended on context (i.e. the service type). At a medium fee, this willingness ranged from 40–76%, and at a high fee, it was naturally at lower but also non-negligible rates of 20–58%. This also shows that price elasticity depends on the service type (context) and is the lowest for a telebanking system. For each service type, reduced functionality would be favoured over bearing privacy costs. Therefore, the protection of data is more important to the respondents than functionality. Thus, privacy costs, or the reluctance to bear privacy costs, should be considered when developing different versions of the same service. In addition, users expect to have some fair conditions (i.e. that their private data is protected or at least not collected) when they are willing to pay for a service.

6 Conclusion, Limitations and Further Research

Companies collect and use data to address potential customers via personalised ads. This annoys or harasses users, making them reluctant to share private data. However, research has shown that not all users are aware of privacy costs. This leads to an unbalanced situation, leaving both service providers and users unsatisfied. Since not all users have shown coping mechanisms, such as privacy cynicism (van Ooijen et al., 2022), our study showed that users are only willing to bear privacy costs (i.e., use private data as currency) to a certain extent. They would rather accept reduced functionality instead of bearing privacy costs (i.e. sharing private data). For companies, particularly service providers, it is important to realise that this very much depends on the service itself and how critical it is seen to be. In addition, there are some interesting demographical characteristics (e.g. occupation status) that may contribute to providing the most fitting version to users. Clearly, this research has several limitations, which can also provide impetus for future research. First, the sampling method did not consider representativeness, which may have led to bias due to a superior number of students. In general, the survey would benefit from more participants. Next, the questions used in the questionnaire were not academically validated. Finally, the conjoint analysis could also be further extended, particularly by adding more attributes and levels or different services (e.g. online content providers) that are in reality directly impacted by this issue. Regarding the level of the attributes, it might make sense to differentiate privacy costs in the choice sets (e.g. by adding a medium level, such as sharing only necessary data).

Acknowledgement

We would like to thank Martin Haider for supporting this research, in particular his support in terms of data collection and analysis.

References

Acquisti, A., 2008. Identity management, privacy, and price discrimination. IEEE Security & Privacy 6, 46–50.

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347, 509–514.

Adkinson, W.F., Eisenach, J.A., Lenard, T.M., 2002. Privacy online: A report on the information practices and policies of commercial web sites. Progress and Freedom Foundation, Washington DC.

Ajzen, I., 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes, Theories of Cognitive Self-Regulation 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Akter, S., Wamba, S.F., 2016. Big data analytics in E-commerce: a systematic review and agenda for future research. Electron Markets 26, 173–194. https://doi.org/10.1007/s12525-016-0219-0

Alessi, M., Camillo, A., Giangreco, E., Matera, M., Pino, S., Storelli, D., 2018. Make users own their data: A decentralized personal data store prototype based on ethereum and ipfs, in: 2018 3rd International Conference on Smart and Sustainable Technologies (SpliTech). IEEE, pp. 1–7.

Asdemir, K., Kumar, N., Jacob, V.S., 2012. Pricing Models for Online Advertising: CPM vs. CPC. Information Systems Research 23, 804–822. https://doi.org/10.1287/isre.1110.0391

Avgerou, A.D., Stamatiou, Y.C., 2015. Privacy awareness diffusion in social networks. IEEE Security & Privacy 13, 44–50.

Awad, Krishnan, 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Quarterly 30, 13. https://doi.org/10.2307/25148715

Baker, W., Marn, M., Zawada, C., 2001. Price smarter on the net. Harvard business review 79, 122–7.

Beales, H., 2010. The value of behavioral targeting. Network Advertising Initiative 1, 2010.

Belanger, F., Hiller, J.S., Smith, W.J., 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The journal of strategic Information Systems 11, 245–270.

Benndorf, V., Normann, H.-T., 2018. The Willingness to Sell Personal Data. The Scandinavian Journal of Economics 120, 1260–1278. https://doi.org/10.1111/sjoe.12247

Berger, D.D., 2010. Balancing consumer privacy with behavioral targeting. Santa Clara Computer & High Tech. LJ 27, 3.

Bhargava, H.K., Choudhary, V., 2008. Research note—when is versioning optimal for information goods? Management Science 54, 1029–1035.

Borgesius, F.Z., Poort, J., 2017. Online price discrimination and EU data privacy law. Journal of consumer policy 40, 347–366.

Breidert, C., Hahsler, M., Reutterer, T., 2006. A review of methods for measuring willingness-to-pay. Innovative marketing 2.

Buchanan, T., Paine, C., Joinson, A.N., Reips, U.-D., 2007. Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology 58, 157–165. https://doi.org/10.1002/asi.20459

Buck, C., Stadler, F., Suckau, K., Eymann, T., 2017. Privacy as a part of the preference structure of users app buying decision, in: : : Proceedings Der 13. Internationalen Tagung Wirtschaftsinformatik (WI2017). Presented at the WI2017, pp. 792–806.

Castells, M., 2010. The Rise of the Network Society, 2nd ed. John Wiley & Sons Ltd, Chichester, West Sussex, PO19 8SQ, United Kingdom. https://doi.org/10.1002/9781444319514

Chapman, J., Dean, M., Ortoleva, P., Snowberg, E., Camerer, C., 2017. Willingness to Pay and Willingness to Accept are Probably Less Correlated Than You Think. Working Paper Series. https://doi.org/10.3386/w23954

Chellappa, R.K., Sin, R.G., Siddarth, S., 2011. Price Formats as a Source of Price Dispersion: A Study of Online and Offline Prices in the Domestic U.S. Airline Markets. Information Systems Research 22, 83–98. https://doi.org/10.1287/isre.1090.0264

Chen, Y.-J., Huang, K.-W., 2016. Pricing Data Services: Pricing by Minutes, by Gigs, or by Megabytes per Second? Information Systems Research 27, 596–617. https://doi.org/10.1287/isre.2016.0651

Choi, H., Jung, Y., 2020. Online Users' Cynical Attitudes towards Privacy Protection: Examining Privacy Cynicism. Asia Pacific Journal of Information Systems 30, 547–567.

Chrzan, K., Orme, B., 2000. An overview and comparison of design strategies for choice-based conjoint analysis. Sawtooth software research paper series 98382, 360.

Church, J., Gandal, N., Krause, D., 2008. Indirect network effects and adoption externalities. Review of Network Economics 7.

Cichy, P., Salge, T.O., Kohli, R., 2021. Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. MIS Quarterly 45, 1863–1891. https://doi.org/10.25300/MISQ/2021/14165

Cook, J.E., Attari, S.Z., 2012. Paying for what was free: Lessons from the New York Times paywall. Cyberpsychology, behavior, and social networking 15, 682–687.

Correia, J., Compeau, D., 2017. Information privacy awareness (IPA): a review of the use, definition and measurement of IPA, in: Proceedings of the 50th Hawaii International Conference on System Sciences.

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science 10, 104–115.

De Hert, P., Papakonstantinou, V., 2016. The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer law & security review 32, 179–194.

Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology 45, 285–297. https://doi.org/10.1002/ejsp.2049

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

DIVSI, 2014. Daten – Ware und Währung. Deutsches Institut für Vertrauen und Sicherheit im Internet., Hamburg, Germany.

Dou, G., He, P., Xu, X., 2016. One-side value-added service investment and pricing strategies for a two-sided platform. International Journal of Production Research 54, 3808–3821.

Dou, W., 2004. Will internet users pay for online content? Journal of Advertising Research 44, 349–359.

Eggers, F., Sattler, H., Teichert, T., Völckner, F., 2018. Choice-Based conjoint analysis. Handbook of market research 1–39.

European Commission, 2016. GDPR, 2016/679.

Evans, J.R., Mathur, A., 2005. The value of online surveys. Internet research.

Fernback, J., Papacharissi, Z., 2007. Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. New Media & Society 9, 715–734.

Finn, R.L., Wright, D., Friedewald, M., 2012. Seven Types of Privacy, in: European Data Protection: Coming of Age, European Data Protection: Coming of Age. Springer, pp. 3–32.

Gates, C., Matthews, P., 2014. Data is the new currency, in: Proceedings of the 2014 New Security Paradigms Workshop. pp. 105–116.

Goes, P.B., Karuga, G.G., Tripathi, A.K., 2010. Understanding Willingness-to-Pay Formation of Repeat Bidders in Sequential Online Auctions. Information Systems Research 21, 907–924. https://doi.org/10.1287/isre.1080.0216

Goldman, E., 2020. An introduction to the california consumer privacy act (CCPA). Santa Clara Univ. Legal Studies Research Paper.

Goldstein, D.G., Suri, S., McAfee, R.P., Ekstrand-Abueg, M., Diaz, F., 2014. The Economic and Cognitive Costs of Annoying Display Advertisements. Journal of Marketing Research 51, 742–752. https://doi.org/10.1509/jmr.13.0439

Green, P.E., Rao, V.R., 1971. Conjoint measurement-for quantifying judgmental data. Journal of Marketing research 8, 355–363.

Grossklags, J., Acquisti, A., 2007. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information., in: WEIS. Citeseer.

Günther, W.A., Mehrizi, M.H.R., Huysman, M., Feldberg, F., 2017. Debating big data: A literature review on realizing value from big data. The Journal of Strategic Information Systems 26, 191–209.

Hartmann, P.M., Zaki, M., Feldmann, N., Neely, A., 2016. Capturing value from big data – a taxonomy of data-driven business models used by start-up firms. IJOPM 36, 1382–1406. https://doi.org/10.1108/IJOPM-02-2014-0098

Hinz, O., Hann, I.-H., Spann, M., 2011. Price discrimination in e-commerce? An examination of dynamic pricing in name-your-own price markets. Mis quarterly 81–98.

Hoffmann, C.P., Lutz, C., Ranzini, G., 2016. Privacy cynicism: A new approach to the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 10.

Horowitz, J.K., McConnell, K.E., 2003. Willingness to accept, willingness to pay and the income effect. Journal of Economic Behavior & Organization 51, 537–545. https://doi.org/10.1016/S0167-2681(02)00216-0

Hsu, C., Lee, J.-N., Straub, D.W., 2012. Institutional Influences on Information Systems Security Innovations. Information Systems Research 23, 918–939. https://doi.org/10.1287/isre.1110.0393

Ilieva, J., Baron, S., Healey, N.M., 2002. Online surveys in marketing research. International Journal of Market Research 44, 1–14.

Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal 25, 607–635.

Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Krumay, B., Klar, J., 2020. Readability of Privacy Policies, in: IFIP Annual Conference on Data and Applications Security and Privacy. Springer, pp. 388–399.

Laufer, R.S., Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of social Issues 33, 22–42.

Li, H., Sarathy, R., Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. Journal of Computer Information Systems 51, 62–71.

Liang, H., Wang, N., Xue, Y., Ge, S., 2017. Unraveling the Alignment Paradox: How Does Business—IT Alignment Shape Organizational Agility? Information Systems Research 28, 863–879. https://doi.org/10.1287/isre.2017.0711

Louviere, J.J., Woodworth, G., 1983. Design and analysis of simulated consumer choice or allocation experiments: an approach based on aggregate data. Journal of marketing research 20, 350–367.

Malgieri, G., Custers, B., 2017. Pricing Privacy – The Right to Know the Value of Your Personal Data (SSRN Scholarly Paper No. ID 3047257). Social Science Research Network, Rochester, NY.

Meinert, D.B., Peterson, D.K., Criswell, J.R., Crossland, M.D., 2006. Privacy policy statements and consumer willingness to provide personal information. Journal of Electronic Commerce in Organizations (JECO) 4, 1–17.

Nissenbaum, H., 2020. Protecting privacy in an information age: The problem of privacy in public, in: The Ethics of Information Technologies. Routledge, pp. 141–178.

Nolin, J.M., 2020. Data as oil, infrastructure or asset? Three metaphors of data as economic value. Journal of Information, Communication and Ethics in Society 18, 28–43.

Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs 41, 100–126.

Odlyzko, A., 2009. Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets. Review of Network Economics 8.

Oetzel, M.C., Gonja, T., 2011. The online privacy paradox: a social representations perspective, in: CHI'11 Extended Abstracts on Human Factors in Computing Systems. pp. 2107–2112.

Phelps, J., Nowak, G., Ferrell, E., 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing 19, 27–41.

Phillips, R.L., 2021. Pricing and revenue optimization, in: Pricing and Revenue Optimization. Stanford university press.

Pötzsch, S., 2008. Privacy awareness: A means to solve the privacy paradox?, in: IFIP Summer School on the Future of Identity in the Information Society. Springer, pp. 226–236.

Raghavarao, D., Wiley, J.B., Chitturi, P., 2010. Choice-based conjoint analysis: models and designs. Chapman and Hall/CRC.

Raghu, T.S., Sinha, R., Vinze, A., Burton, O., 2009. Willingness to Pay in an Open Source Software Environment. Information Systems Research 20, 218–236. https://doi.org/10.1287/isre.1080.0176

Rana, O., Weinman, J., 2015. Data as a Currency and Cloud-Based Data Lockers. IEEE Cloud Computing 2, 16–20. https://doi.org/10.1109/MCC.2015.46

Schoenbachler, D.D., Gordon, G.L., 2002. Trust and customer willingness to provide information in databasle-driven relationship marketing. Journal of Interactive Marketing 16, 2–16.

Schreiner, M., Hess, T., 2013. On the willingness to pay for privacy as a freemium model: First empirical evidence, in: ECIS 2013 Resarch in Progress. Presented at the European Conference on Information Systems, AIS, Utrecht, Netherlands.

Schwartz, P.M., 2003. Property, privacy, and personal data. Harv. L. Rev. 117, 2056.
Shapiro, C., Varian, H.R., Carl, S., 1998. Information rules: A strategic guide to the network economy. Harvard Business Press.
Shivendu, S., Zhang, Z. (James), 2015. Versioning in the Software Industry: Heterogeneous Disutility from Underprovisioning of Functionality. Information Systems Research 26, 731–753. https://doi.org/10.1287/isre.2015.0597
Simonson, I., Drolet, A., 2004. Anchoring Effects on Consumers' Willingness-to-Pay and Willingness-to-Accept. Journal of Consumer Research 31, 681–690. https://doi.org/10.1086/425103
Solove, D.J., 2021. The Myth of the Privacy Paradox. Geo. Wash. L. Rev. 89, 1–51.
State of California, 2020. CCPA.
Stole, L.A., 2007. Price discrimination and competition. Handbook of industrial organization 3, 2221–2299.
Trepte, S., Reinecke, L., Ellison, N.B., Quiring, O., Yao, M.Z., Ziegele, M., 2017. A cross-cultural perspective on the privacy calculus. Social Media+ Society 3, 2056305116688035.
Turow, J., King, J., Hoofnagle, C.J., Bleakley, A., Hennessy, M., 2009. Americans reject tailored advertising and three activities that enable it. Available at SSRN 1478214.
United Nations, 1948. Universal Declaration of Human Rights.
Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N., 2020. Measuring the impact of the gdpr on data sharing in ad networks, in: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. pp. 222–235.
van Ooijen, I., Segijn, C.M., Opree, S.J., 2022. Privacy Cynicism and its Role in Privacy Decision-Making. Communication Research 00936502211060984.
Varian, H.R., 1989. Price discrimination. Handbook of industrial organization 1, 597–654.
Voss, W.G., 2014. Looking at European Union data protection law reform through a different prism: The proposed EU General Data Protection Regulation two years later. Journal of Internet Law 17.
VZBV, 2015. Datenschutz – Die Sicht der Verbraucherinnen und Verbraucher in Deutschland. Verbraucherzentrale Bundesverband.
Warren, S.D., Brandeis, L.D., 1890. The Right to Privacy. Harvard Law Review 15.
Westin, A.F., 1968. Privacy and freedom. Washington and Lee Law Review 25, 166.
Wright, K.B., 2005. Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. Journal of computer-mediated communication 10, JCMC1034.
Xu, H., Dinev, T., Smith, J., Hart, P., 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. JAIS 12, 798–824. https://doi.org/10.17705/1jais.00281